UNIVERSIDADE FEDERAL DA PARAIBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

JOSIVAN DE OLIVEIRA FERREIRA

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

João Pessoa
2013

JOSIVAN DE OLIVEIRA FERREIRA

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

Dissertação apresentada ao Curso de Mestrado em Ciência da Informação, do Programa de Pós-graduação em Ciência da Informação, da Universidade Federal da Paraíba (PPGCI/UFPB), como requisito parcial para a obtenção do título de Mestre.

Área de concentração: Informação, conhecimento e sociedade

Linha de pesquisa: Ética, Gestão e Políticas de Informação

Orientador: Prof. Dr. Wagner Junqueira de Araújo

João Pessoa

2013

F383a Ferreira, Josivan de Oliveira.
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.-- João Pessoa, 2013.
123f. : il.
Orientador: Wagner Junqueira de Araújo
Dissertação (Mestrado) – UFPB/CCSA
1. Ciência da informação. 2. Gestão da segurança da informação. 3. Política de segurança da informação. 4. Análise de risco. 5. Sistema de concessão - diárias e passagens.

UFPB/BC CDU: 02:681.3(043)

JOSIVAN DE OLIVEIRA FERREIRA

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

Aprovado em: 27 / 03 /2013

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Informação da UFPB, na linha de pesquisa Ética, Gestão e Políticas de Informação, em cumprimento às exigências para a obtenção do título de mestre em Ciência da Informação.

BANCA EXAMINADORA

_____

Prof. Dr. Wagner Junqueira de Araújo - Orientador – PPGCI/UFPB

_____

Prof. Dr. Guilherme Ataíde Dias – Examinador Interno - PPGCI/UFPB

_____

Prof. Dr. Miguel Maurício Isoni – Examinador Externo – MPGOA/UFPB

Dedico

A minha mãe, ***in memoriam***, pelo esforço, durante toda a sua vida, em demonstrar a importância da educação;

Ao meu pai, pela dedicação à família;

A minha irmã, que sempre acreditou no meu potencial e pelo apoio para a realização dos meus objetivos;

A minha família de coração, pela força e pelo incentivo em todas as horas: amigos e amigas.

Agradeço

Primeiramente, a DEUS, pela vida e pelo modo como acredito em suas bênçãos;

A todos os que me apoiaram e me incentivaram para a realização deste trabalho, especialmente Suzana, que foi a primeira a fazer com que eu me interessasse pela área;

Ao Professor Wagner Junqueira de Araújo, em quem encontrei amizade, dedicação, apoio e orientação em todos os passos desse trabalho;

Aos Professores Guilherme Ataíde Dias e Ed Porto Bezerra, por aceitarem participar da Banca examinadora e pelos valiosos contributos para o aprimoramento deste trabalho, assim como o Professor Markson, que participou como suplente da Banca e que nos enviou suas contribuições;

A todos os professores do PPGCI, em especial, a Gustavo Freire, Joana Coeli Garcia, Marckson Sousa, Carlos Xavier, Edvaldo Alves, Isa Freire e Wagner Junqueira de Araújo;

A todos os colegas da turma de Mestrado 2011, pelas amizades, pelas experiências trocadas, pelos momentos vividos e pelas lições aprendidas na convivência em sala de aula e fora dela.

O conhecimento é o processo de acumular informações;
a Sabedoria reside na sua simplificação.
MARTIN H. FISCHER

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 mitigar 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.

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: Management of information security. Information Science. Policy information security. Risk analysis. Sistema de Concessão de Diárias e Passagens.

LISTA DE FIGURAS

.

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CE	Centro de Educação
CB	Centro de Biotecnologia
CCS	Centro de Ciências da Saúde
CCEN	Centro de Ciências Exatas e da Natureza
CCHLA	Centro de Ciências Humanas, Letras e Artes
CCM	Centro de Ciências Médicas
CCSA	Centro de Ciências Sociais e Aplicadas
CCTA	Centro de Comunicação, Turismo e Artes
CCEAR	Centro de Energias Alternativas e Renováveis
CT	Centro de Tecnologia
CTDR	Centro de Tecnologia e Desenvolvimento Regional
CCJ	Centro de Ciências Jurídicas
CI	Ciência da Informação
CCF	Coordenação de Contabilidade e Finanças
DSIC	Departamento de Segurança da Informação e Comunicações
FRAAP	Facilitated Risk Analysis and Assessment Process
GSI	Gestão de Segurança da Informação
GSIPR	Gabinete de Segurança Institucional da Presidência da República
GOV-BR	Governo Eletrônico
GRSIC	Gestão de Risco de Segurança da Informação e Comunicações
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Standartization Organization
MPOG	Ministério do Planejamento, Orçamento e Gestão
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
PSI	Política de Segurança da Informação
PRA	Pró-reitoria Administrativa
PRAPE	Pró-reitoria de Assistência e Promoção ao Estudante

RMF	Risk Management Framework
SERPRO	Serviço Federal de Processamento de Dados
SIBC	Sistema de Informação Baseado em Computador
TI	Tecnologia da Informação

SUMÁRIO

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.

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. A vida é intrinsecamente cheia de perigos, reais ou percebidos. Aviões podem explodir em pleno ar por causa de atividades terroristas; uma usina nuclear pode liberar substâncias radioativas na atmosfera; uma indústria química pode liberar gases tóxicos; um desastre natural pode atingir a área em que as pessoas vivem, e uma infinidade de incidentes pode ser ocasionada devido a violações de regras de segurança. Quando alguém atravessa a rua ou faz um investimento, está fazendo com base numa avaliação de riscos e benefícios que certa atividade traria. Com o uso da informação, isso não é diferente, principalmente quando se relaciona com os sistemas informatizados.

As ameaças são intensas porquanto a informação compreende 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.

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

[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.

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).

Assim, este estudo se justifica porque ainda são escassas as pesquisas realizadas em Setores de Atividade-meio das Instituições de Ensino Superior no Brasil, notadamente nas IFES públicas, e objetiva evidenciar, nas importantes atividades do SCDP, como estão fazendo uso das políticas de segurança da informação nos seus setores contábeis. Além disso, a motivação de ordem pessoal, em razão do cargo de técnico em Contabilidade na instituição, contribuiu para o desenvolvimento desse assunto relevante e deu a oportunidade de oferecer resultados práticos à universidade para ajudar seu posicionamento estratégico e a continuidade dos seus serviços.

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 procura responder ao seguinte questionamento: **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?**

A presente dissertação está estruturada em seis capítulos; no segundo capítulo, são feitas considerações sobre os pressupostos teóricos que nortearam a pesquisa, o poder da informação na história, a Ciência da Informação, os sistemas de informação, a segurança da informação e a análise de risco; o terceiro traz uma abordagem a respeito da segurança na Ciência da Informação, através de um levantamento dos trabalhos na área da segurança da informação entre 2007 e 2011; o quarto capítulo apresenta os procedimentos metodológicos, o tipo de pesquisa, o método escolhido, a caracterização da pesquisa, o campo de pesquisa e os instrumentos de coleta de dados. O quinto capítulo diz respeito aos resultados encontrados através da coleta realizada com a aplicação dos instrumentos de pesquisa, bem como o tratamento estatístico aplicado. Demonstra também a análise dos resultados encontrados. Finalmente, são apresentadas as considerações finais, com os aspectos conclusivos da pesquisa e propostas de ações sugeridas.

1.1 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.

1.1.1 Objetivos específicos

a) Descrever o SCDP, conforme visão do público escolhido;
b) Mapear o fluxo informacional do SCDP;
c) Identificar quais os níveis hierárquicos dos usuários responsáveis pela tomada de decisão;

d) Identificar os elementos de segurança do sistema em estudo;
e) Efetuar análise de risco com foco na segurança da informação nos documentos em seus diferentes suportes utilizados pelo SCDP.

2 FUNDAMENTOS TEÓRICOS DA INFORMAÇÃO

2.1 O PODER DA INFORMAÇÃO NA HISTÓRIA

Com o passar das décadas, a informação vem se tornando a força necessária para o crescimento e a criação de riquezas. No mundo capitalista, o auge do desenvolvimento é determinado pelo que se sabe, e não, pelo que se possui, o que resulta na transição de uma economia industrial para uma economia da informação.

A concorrência numa economia da informação está representada na capacidade que as empresas têm de conseguir, organizar, entender e usar a informação da melhor forma possível. Portanto, a fim de liderar a concorrência, as organizações investem pesadamente na tecnologia de informática e comunicação, implantando sistemas de processamento de dados sofisticados e específicos para sua atividade empresarial. No entanto, o braço forte de todo o desempenho satisfatório que possa acontecer desprende-se do aparato tecnológico, porque ele não representa o principal aspecto que leva a tamanha vantagem. Isso, realmente, determina o progresso econômico e financeiro de uma entidade e está alocado na informação que esses sistemas sofisticados possibilitam manusear para atingir seus objetivos. Como argumenta McGee (1994, p.5), “a Informação é dinâmica, capaz de criar grande valor, e é o elemento que mantém as organizações unificadas”. A Tecnologia da Informação pode ser um fator importante no aperfeiçoamento do uso da informação, mas facilmente poderá se transformar inútil sem a informação e os humanos como usuários.

Como usuários da informação, os humanos determinam outro fator bastante relevante no desenvolvimento do mundo econômico e financeiro que, nesse caso, está agregado ao resultado dos dados processados pelos sistemas informacionais. Esse resultado, proveniente da coleta e do tratamento dos dados, chama-se conhecimento. No entanto, o conhecimento, além da informação, é peça fundamental para haver força competitiva que seja capaz de reformular conceitos e determinar diretrizes para se atingir o sucesso.

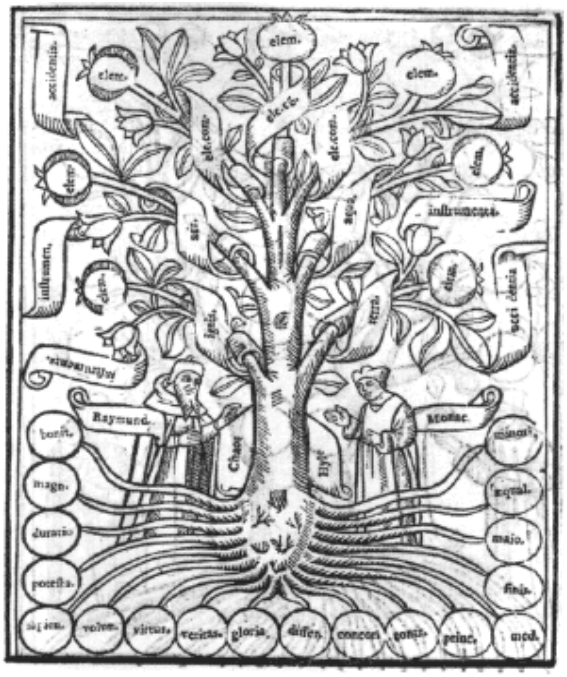
A base do nosso momento está atrelada ao passado. Todo resultado de uma vida humana é fruto de um trabalho construído continuamente desde o nascimento. Esse princípio básico está associado a tudo o que podemos imaginar, como:

acontecimentos, objetos, obras de arte, carreira, empresas e outros. Portanto, convém salientar a importância que devemos atribuir aos acontecimentos do passado que contribuíram para disseminar a informação, nos dias atuais, e ao conhecimento gerado por elas.

2.1.1 Idade Média e Moderna

O sistema de conhecimento, entre o Século XVI e a Idade Média, era visualizado através de uma grande árvore. Nessa representação, era possível associar o tronco e os galhos ao dominante e ao subordinado. Segundo Burke (2003, p. 82), “a imagem da árvore ilustra um fenômeno central em história cultural, a naturalização do convencional, ou a apresentação da cultura como se fosse natureza, da invenção, como se fosse descoberta”.

Figura 1 – Árvore do conhecimento



Fonte: BURKE (2003)

Nesse caso, existia um conhecimento dominante, concentrado no centro da árvore, cuja informação era disseminada para vários outros conhecimentos considerados menos importantes na época (BURKE, 2003, p. 82). Podemos observar, na concepção da árvore, que era necessário sistematizar o conhecimento, para que se pudessem executar ações, com eficácia e de forma ordenada, através

do uso da informação. Por isso, a partir do Século XVII, em lugar da “árvore”, o termo “sistema”, considerado até mais abstrato, começou a entrar em uso a fim de designar a organização do conhecimento (BURKE, 2003, p. 83). É bem provável que os primórdios dos sistemas, utilizados frequentemente, hoje, pelas grandes corporações, tenham surgido nessa época, quando os estudiosos sentiam, através do conhecimento, a necessidade de ordenar o que já havia sido construído.

O Renascimento foi um período marcado por grandes transformações em muitas áreas da vida humana, que assinalou a transição da Idade Medieval para a Idade Moderna. Nesse momento, o homem passou de mero observador da Criação Divina para ser a peça central, e o mundo passou a ser pensado como uma realidade a ser compreendida cientificamente, e não, apenas, admirada. Esse novo pensamento contrariava a Igreja medieval, que se tornou extremamente grandiosa por conciliar o racionalismo com a fé cristã.

A Igreja tinha o monopólio do conhecimento, era pioneira em diversas áreas avançadas, como a de arquivo e finanças. Na Europa, todos os professores universitários eram membros do clero. A informação que a burocracia papal detinha fez dela uma instituição mais grandiosa do que qualquer monarquia europeia, pois o conhecimento gerado representava muito poder, capaz de regular e manipular grupos fechados ou mesmo gerações inteiras de pessoas.

O poder da informação também pode ser demonstrado quando, no decorrer da história, surgiu o chamado “Orientalismo”, ou seja, o sistema ocidental de representação e dominação. Nesse caso, havia uma coleta sistemática de conhecimento pelas grandes potências europeias através das informações adquiridas nas viagens para as Índias ou para a África. Os registros do que tinha se tornado conhecido eram armazenados em documentos oficiais e guardados em locais especiais, pois seriam usados para dominar outras partes do mundo (BURKE, 2003, p.117).

Em meio a tantas informações que transitavam com constante intensidade pelos governos do passado, muitas delas eram consideradas altamente sigilosas. Por essa razão, estava em operação um sistema de controle ou censura. Em Veneza, por exemplo, o acesso aos arquivos era estritamente controlado, pois o próprio dirigente máximo da República não era autorizado a entrar sozinho nos arquivos. Portanto, apenas os membros do Senado tinham essa permissão, e os membros do “Collegio” podiam remover os documentos. É curioso saber que o

zelador do arquivo tinha que ser analfabeto para não correr o risco de ser tentado a ler os papéis sob sua guarda (BURKE, 2003, p. 125).

Os Estados dos primórdios da Europa moderna, com medo de haver motim, ou melhor, crimes contra a segurança do Estado, organizaram sistemas de censura para a imprensa. Veneza, a República Holandesa e a Inglaterra colocavam certos limites à liberdade de comunicação. Por exemplo, na Inglaterra, a Rainha Elizabeth limitou apenas a Londres, Oxford e Cambridge as impressões a fim de manter eficazmente sua supervisão (BURKE, 2003, p. 131).

Outra preocupação que levava à censura no governo era o temor à publicação de informação confidencial. Em Portugal, o conhecimento das Índias e da África era tratado como segredo de Estado e levava o Rei Manuel a proibir os cartógrafos de representarem a costa africana situada além do Congo. Em 1711, um tratado sobre a economia brasileira, chamado de Cultura de opulência do Brasil, imediatamente foi censurado, pois se temia que os estrangeiros pudessem aprender as rotas para as minas de ouro do Brasil. Todavia, algumas informações precisavam ser tornadas públicas a fim de o governo atingir seus objetivos. É o caso das leis e dos decretos que eram constantemente proclamados em voz alta além de impressos e afixados em locais públicos. No entanto, era necessário manter o equilíbrio entre dar ao público informação de menos, situação que incentivaria os rumores mais exagerados, e dar-lhe informação demais, o que incentivaria as pessoas comuns a se pronunciarem sobre questões do Estado (BURKE, 2003, p.133).

2.1.2 Pós-modernidade e suas implicações na segurança da informação

A quebra das fronteiras, devido à globalização, contribuiu muito para o fortalecimento da disseminação da informação no mundo, como argumenta Stuart Hall (2001, p. 67):

> [...] a “globalização” se refere àqueles processos, atuantes numa escala global, que atravessam fronteiras nacionais, integrando e conectando comunidades e organizações em novas combinações de espaço-tempo, tornando o mundo, em realidade e experiência, mais interconectado.

Atualmente, é inegável que os processos caracterizados pela globalização se intensificaram, gerando diversos traços marcantes para a história. Dentre esses, pode-se destacar “a revolução das comunicações que fizeram reduzir a muito pouco o privilégio que o Estado detinha sobre a moeda e a comunicação, consideradas atributos da soberania e vistos como peças estratégicas da segurança nacional” (SANTOS, 1997, p. 291).

No mercado, a cada dia, é visível a facilidade de comunicação, transmissão e de processamento de informações, além da mobilidade internacional de capital. No plano econômico, a globalização caracteriza-se pela desnacionalização financeira. No plano político, o maior desafio refere-se à perda de autonomia do estado nacional, na medida em que existe uma concentração significativa do poder econômico nas mãos de um pequeno grupo de grandes empresas transnacionais e instituições econômicas mundiais, conforme salientou Santos (1997, p. 291):

> Por outro lado, as multinacionais, dotadas de um poder de intervenção global e se beneficiando da mobilidade crescente dos processos de produção podem facilmente pôr em concorrência dois ou mais Estados ou duas ou mais regiões dentro do mesmo Estado sobre as condições que decidirão da localização do investimento por parte da empresa multinacional.

A relação que existe entre a informação e o mundo globalizado enfatiza a importância de haver mais consciência quanto à segurança dos dados que são diariamente processados por organizações, governos e indivíduos. A internet, basicamente, é responsável pela transmissão dessas informações, visto que, por meio dela, é possível armazenar grande quantidade de documentos que ficam dispostos para consulta em toda parte do Planeta. Segundo Lafer (2011, p. 12), a facilidade de acesso e de pesquisa na Internet já é maior que a busca de informações em documentos impressos. Sejam essas consultas efetuadas por autoridades públicas, empresariais, bibliotecas ou outros porta-vozes de qualquer natureza. No entanto, esse cruzamento de informações digitalmente armazenadas tem como consequência a crescente dificuldade de deixá-las sigilosas, ao passo que, na transmissão dessas informações, existe o anonimato na rede, ou melhor, a ausência de características que permitam a identificação de autoria das ações executadas nela. No ambiente virtual, a pessoa pode facilmente se passar por outra, independentemente de etnia, gênero ou grupo social, desde que tenha acesso aos

recursos computacionais para essa tarefa. Essa é uma situação crítica, que leva a relatos contemporâneos, como o devassamento da vida privada, o roubo em contas bancárias, a quebra de segredo profissional, o vazamento de informações diplomáticas e outros.

Nos Estados Unidos, em novembro de 2010, houve a maior quebra de segurança digital da história do país, quando o WikiLeaks, site especializado em divulgar informações confidenciais, publicou telegramas diplomáticos que continham dados sobre as opiniões do governo estadunidense e suas relações com o mundo exterior. Esse acontecimento tem sua raiz no embate acirrado pelo acesso à informação governamental que acresceu no início deste Século XXI (LAFER, 2011, p. 20).

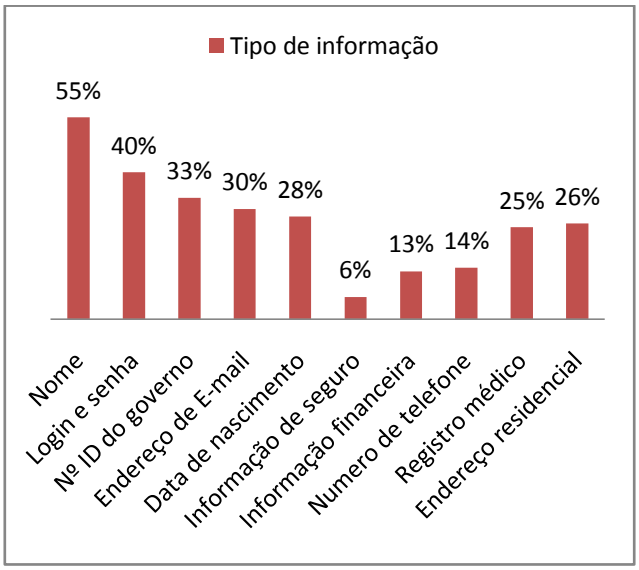
Em 22 de junho de 2011, o Brasil sofreu sua terceira tentativa de invasão por hackers aos sites da Presidência da Republica, do Portal Brasil e da Receita Federal. Nesse ato hostil, foi registrado cerca de dois bilhões de acessos num horário em que, normalmente, eles são praticamente nulos. Conforme relatou o diretor superintendente do Serviço de Processamento de Dados (Serpro), Gilberto Paganotto, o objetivo, em geral, desses ataques é fazer pichações ou conseguir dados após os tumultos de acessos.[2] Consequentemente a esses ataques e atribuindo atenção à preservação da vida privada, o Código Penal brasileiro foi alterado através da Lei 12.737, publicada no Diário Oficial da União, em 11 de novembro de 2012, e estabelece punição aos crimes de invasão nos dispositivos eletrônicos, como celulares, notebooks, desktops, *tablets* ou caixas eletrônicos para adulterar dados ou obter vantagens ilícitas. As invasões procuram interceptar informações sensíveis, tais como número de identidade, seguro social, data de nascimento e outras informações pessoais que podem ser utilizadas para roubo de identidade e outras fraudes (WORKMAN, 2008, p. 663, tradução nossa).

Os ataques à informação, através da internet, multiplicam-se consideravelmente a cada dia. O gráfico a seguir demonstra as informações que mais sofrem violação de dados, conforme relatório da Symantec, acumulado entre janeiro e novembro de 2012:

---

[2] "Governo bloqueia tentativa de invasão a sites". Disponível em: http://www.clicrbs.com.br/jsc/sc/impressa/4,181,3362044,17386. Acessado em 20 de setembro de 2011.

Gráfico 1 – Percentual de exposição por violação de dados



Fonte: Relatório Symantec (2012)

De acordo com o gráfico, o nome pessoal é o componente mais comum a ser roubado em uma violação de dados, em que se obtiveram 55% do tempo de análise. Isso supera até *login* e senhas, comumente usados para identidades on-line, que aparecem dentro de 40% de todas as violações de dados. Observa-se também que as informações financeiras, relativas a cartão de crédito, salários e conta-corrente, só aparecem em 13% de todas as violações de dados. Isso pode ser devido às restrições mais pesadas sobre a forma como a informação financeira é recolhida, confirmada e armazenada.

Em contrapartida, mais de 80% das violações de dados ocorreram em 2012 com organizações cuja presença na Internet é secundária à sua atividade principal, tais como os setores de saúde e educação, onde o acesso para a execução dos serviços é, muitas vezes, realizado como meio de conveniência em vez de uma frente de negócios[3]

[3] Symantec Intelligence Report: Novembro 2012. Estados Unidos, 2012, p. 3. Disponível em: http://www.symantec.com/pt/br/theme.jsp?themeid=gin. Acesso em: 22/12/2012

2.2 CIÊNCIA DA INFORMAÇÃO

Após a primeira década do Século XX, depois da segunda revolução científica, diversas pessoas ligadas à área do conhecimento, como cientistas, filósofos, reformadores sociais e outros, desejaram intensamente condensar, num único corpo, os crescentes milhares de documentos científicos espalhados pelo mundo, os quais poderiam se coletados para o progresso social e intelectual. Essa síntese única seria estabelecida por intermédio da documentação, como destacou Otlet:

> [...] uma ciência geral, uma filosofia da ciência, uma enciclopédia são necessários para unificar todas as ciências particulares, até que todas as suas conexões fragmentárias sejam removidas, e todos seus princípios, métodos e programas de desenvolvimento e sucesso sejam revelados pela simplificação de suas concepções e exposições (OTLET, 1935, p. 360 – Tradução nossa).

Otlet tinha certeza de que um sistema único garantiria uma descrição e classificação simplificada da realidade mundial, determinando, nesse caso, para uma estabilidade e paz social no mundo. Para ele, o conceito de documento consistia em toda gama de produtos de informação que surgem e se expandem com a revolução industrial: artigos, relatórios científicos e técnicos, desenhos industriais, patentes, cartões-postais, fotografias (FREIRE, 2006. p.16). Nesse caso, era apropriado organizar toda essa documentação de uma forma que o conhecimento registrado estivesse disponível para quem tivesse a necessidade de obtê-lo.

Portanto, a maneira utópica de pensar de Otlet, em relação ao valor e à universalidade da documentação, pode ser encarada como origem para a Ciência da Informação, pois o usuário, gradativamente, deixa de permanecer na periferia para o centro do processo de comunicação da informação, que passa a representar como um campo de atividade científica (FREIRE, 2006, p. 9 e 10).

A história intelectual de uma disciplina científica deve focar sua busca na fundamentação teórica. Em 1964, foi dada uma consideração formal para os fundamentos da Ciência da Informação. Por essa altura, um número considerável de intelectuais passou a discutir o assunto na literatura (SHERA, 1977, p. 260). Foi nesse cenário que Borko (1968, p. 3) definiu:

> Ciência da Informação é a que investiga as propriedades e o comportamento da informação, as forças que regem o fluxo de

> informações e os meios de processamento da informação para torná-la acessível e usual. Preocupa-se com o corpo de conhecimentos relacionados com a origem, coleta, organização, transformação e utilização da informação. Isto inclui a investigação de diligências de informação em ambos os sistemas naturais e artificiais, o uso de códigos para transmissão eficiente de mensagens, bem como o estudo dos dispositivos de informação e as técnicas de processamento, tais como computadores e sistemas de programação.

A Ciência da Informação tem duas raízes: uma é o estudo dos problemas relacionados à transmissão de mensagens, e a outra, a computação digital. Na primeira raiz, as origens estão relacionadas à sociedade humana, com suas redes de relacionamento baseadas na linguagem, ligadas a todos os aspectos sociais e culturais próprios do ser humano. Todavia, na outra raiz, a tecnologia recente se refere ao impacto da computação nos processos de produção, coleta, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação (CAPURRO, 2003, p.7). Esse impacto é bem representado pelo uso dos sistemas de informação utilizados pelas organizações nesse mundo globalizado.

2.3 SISTEMA DE INFORMAÇÃO

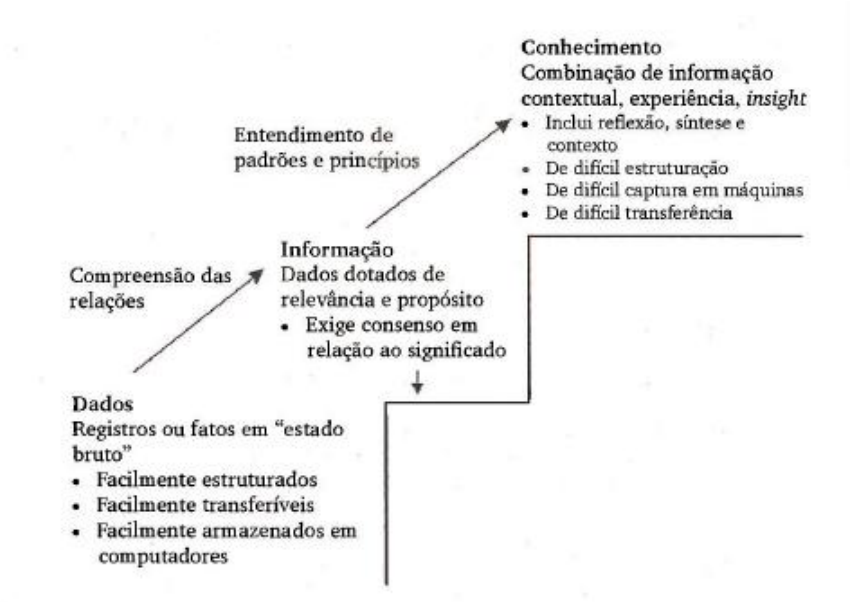
Sistema de informação é “um conjunto organizado de pessoas, hardware, software, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações de uma organização” (O’BRIEN, 2004, p.6). Para Turban et al. (2005, p. 40), “um sistema de informação (SI) coleta, armazena, analisa e dissemina informações para finalidade específica”. Stair et al. (2006, p. 12) definem o sistema de informação como “ um conjunto de elementos ou componentes inter-relacionados que coletam (entrada), manipulam (processo) e disseminam (saída) dados e informações e oferecem um mecanismo de realimentação para atingir um objetivo”.

Nos conceitos anteriores, observam-se dois elementos do sistema de informação que podem parecer intercambiáveis: os dados e a informação. Entretanto, segundo O’Brien (2004. p. 13), “é melhor encarar os dados como recursos de matéria-prima que são processados em produtos acabados de informação”. Ou seja, dados são elementos que, submetidos a um processo de organização, manipulação, análise e avaliação, passam a ter valores para um contexto adequado aos usuários finais específicos. Logo, a informação representa uma coleta de dados organizada e

orientada para atribuir um significado que muda o modo de pensar do destinatário. A mudança proveniente desse processo gera um terceiro e importante elemento, chamado de conhecimento, pois, de acordo com Davenport (1998, p. 18), “é a informação mais valiosa (...) é valiosa precisamente porque alguém deu à informação um contexto, um significado, uma interpretação (...).”

Nos sistemas de informação, dado, informação e conhecimento são fundamentais para o sucesso ou o fracasso das organizações. Na maioria das vezes, o resultado depende de se saber qual deles precisou, com qual deles contamos e o que podemos ou não fazer com cada um deles, pois entender o que são esses três elementos e como passar de um para o outro é essencial para a realização bem-sucedida dos sistemas empresariais (DAVENPORT, 2003, p. 13). Para Angeloni (2003), eles formam um sistema com hierarquia difícil de delimitar na medida em que os conceitos variam de acordo com o entendimento de cada indivíduo. A figura 2 apresenta a estrutura dessa hierarquia e suas particularidades:

Figura 2 – A hierarquia da informação



Fonte: Beal (2011, p. 12)

Considerando que os dados constituem elementos em estado bruto, caso não sejam de qualidade, as decisões organizacionais também seguirão essa mesma natureza (ANGELONI, 2003, p. 18). Além do mais, a ação decisória para os gestores organizacionais é um grande desafio, quando há necessidade de transformar dados

em informação e informação em conhecimento, tentando diminuir as interferências pessoais que ocorrem nesse processo. É por isso que as empresas precisam de diferentes tipos de sistemas de informação para apoiar a tomada de decisões e as atividades de trabalho nos vários níveis e funções organizacionais.

A figura 3 apresenta, de forma concisa, os principais elementos do sistema de informação.

Figura 3 – Componentes de um sistema de informação

Fonte: STAIR et al. (2006, p. 12)

Os sistemas de informação são partes integrantes das organizações, inclusive, para algumas, sua ausência acarretaria na extinção do negócio. De acordo com a figura 3, a entrada, o processamento, a saída e a realimentação são os componentes que formam um sistema de informação. A entrada busca coletar dados em estado bruto que podem proceder de dentro da organização ou de seu ambiente externo. O processamento faz a conversão dos dados brutos em uma forma mais significativa para a empresa. A saída se encarrega de transmitir as informações que foram processadas aos usuários ou às funções que serão empregadas. Logo após a execução dos três elementos, temos a realimentação no sistema de informações provenientes da avaliação e como forma de corrigir o seu funcionamento (LAUREANO, 2005, p. 6).

Antes do surgimento dos sistemas de informação, as organizações se baseavam através do uso de técnicas de arquivamento e recuperação da informação mediante grande volume de documentos. Existia uma pessoa responsável para organizar, registrar, catalogar e recuperar os dados, chamada de “arquivador”. Esse método, aparentemente simples, exigia um grande esforço para

atualizar e recuperar a informação. Com o procedimento manual, era praticamente impossível fazer o cruzamento e a análise dos dados.

Em meados da década de 1930, a documentação tomou um rumo diferente devido ao desenvolvimento do filme fotográfico e das câmeras de miniatura. Essa nova tecnologia, emprestada da indústria do cinema, tornou possível o uso da microfotografia em bibliotecas. Havia previsões de que os microfilmes suplantariam os livros convencionais e que os cartões de catálogo seriam substituídos por microfilmes de textos. No entanto, embora toda essa nova descoberta possibilitasse ao estudioso dar-se ao luxo de manter sua própria microrreprodução, não era, ainda, a base para um sistema de informação (SHERA, 1977, p. 252).

A base histórica para um sistema de informação surgiu em 1945, com a publicação de "*As we may think*", de Vannevar Bush, que incendiou a imaginação do público em geral e abriu caminho para uma nova era da documentação e da Ciência da Informação (SHERA, Ibidem, p. 255). Nesse ensaio, Bush enfatizava que o homem deveria posicionar esforços científicos para tornar o conhecimento humano coletado mais acessível e apresentou um aparelho chamado de memex.

> Considere um dispositivo futurista e para uso individual, que é uma espécie de biblioteca com arquivo mecânico. Ele precisa de um nome, e esse é "memex". Memex é um dispositivo no qual o indivíduo armazena todos os seus livros, registros e comunicações, e sendo mecanizado, proporciona uma consulta com extrema velocidade e flexibilidade. É um suplemento íntimo alargado à sua memória (BUSH, 1945 – Tradução nossa[4]).

Armazenar e recuperar documentos ligados por associações, como sugere Vannevar Bush, é semelhante a alguns dos recursos básicos desempenhados por um Sistema de Informação Baseado em Computador (SIBC). O'Brien (2004, p. 10) enumera cinco dos recursos principais que podem ser aplicados a todos os tipos de SIBC, a saber: pessoas, hardware, software, dados e redes. O SCDP é um exemplo desse tipo de sistema, por meio do qual se aplicam os cinco recursos usados para coletar, manipular, armazenar e processar as informações, pertinentes à concessão de diárias e passagens pela UFPB. Com base nisso, apresenta-se, no quadro 1, a definição desses recursos e suas aplicações no SCDP:

---

[4]"As we may think". Disponível em: http://www.ps.uni-saarland.de/~duchier/pub/vbush/vbush-all.shtml. Acessado em 08 de agosto de 2011.

Quadro 1 – Recursos principais de SIBC e o SCDP

RECURSO	DEFINIÇÃO	APLICAÇÃO NO SCDP
Pessoas	Elemento mais importante, pois inclui todos aqueles que gerenciam, usam, programam e mantêm o sistema em funcionamento (STAIR et. al., 2006, p. 15).	O grupo é formado por servidores com ou sem cargo de direção, fornecedores licitados (agências de viagem) e servidores externos de suporte técnico da Serpro.
Hardware	Compreendemtodos dos dipositivos físicos e equipamentos usados no processamento de informações, incluindo mídias de dados, desde folhas de papel a pen drives (O'BRIEN, 2004, p. 11)	Computador com requisitos mínimos de memória em 128 MB ou superior e processador Pentium de 233 MHz; conector USB tipo A (Universal Serial Bus) 1.0 compatível com 2.0; monitor de vídeo; impressora; scanner; token (USB ePass2000 e ePass2000NG) e formulário de papel.
Software	É um conjunto de programas que permitem que o hardware processe dados (TURBAN et. al., 2005, p. 41). Incluem-se os procedimentos utilizados para instruir as pessoas que manuseiam o SIBC (O'BRIEN, op. cit., p.12).	São requisitos mínimos: sistemas operacionais - Windons 98/SE, 2000, ME, XP, 2003, MacDos e Linux e drives para instalação do token. Arquivos com informações para implantação e uso do sistema, disponíveis na Internet.
Dados	Formam os meios físicos de armazenagem e os programas que comandam e organizam a coleção de arquivos relacionados (LAUDON et. al., 2004, p.13).	Os dados processados incluem informação de contato, históricos pessoais, registros financeiros e identificadores oficiais, tais como números de CPF, Identidade e outros.
Redes	É um sistema de conexão (com ou sem fio) que proporciona o compartilhamento de recursos por vários computadores (TURBAN, et. al., 2005, p. 41).	Dispositvo para acesso à internet; navegador Internet Explorer 5.5 ou Netscape 7.0 ou Mozilla 1.5 ou superior; programa Java Virtual Machine 1.4.2 ou superior; cadeias de certificação do Serpro.

Fonte: Elaborado pelo autor (2013)

As aplicações dispostas no quadro 1 referem-se aos elementos que estão presentes no SCDP, caracterizando-o como um sistema de informação baseado em computador. O recurso de rede pela Internet, mencionado na última linha do quadro, representa uma economia para as organizações, pois o uso dessa tecnologia permite aplicações menos dispendiosas em termos de desenvolvimento, operação e manutenção (O'BRIEN, Ibidem, p. 171). Entre os serviços oferecidos pela Internet, estão: descoberta, comunicação, colaboração e demais serviços Web. Esse último representa um sistema com padrões aceitos universalmente para armazenar, recuperar, formatar e apresentar informações utilizando uma arquitetura cliente/servidor. Além do mais, lida com todos os tipos de informações digitais, incluindo texto, hipermídia, gráficos, som e usa interfaces gráficas do usuário, de modo que é muito fácil de utilizá-la (TURBAN et al., Ibidem, p. 567). São

características apropriadas para a tramitação eletrônica de documentos no SCDP, necessárias para justificar as solicitações de diárias e as passagens dos servidores no sistema. São exemplos desses documentos: formulário de autorização, convite, programação, folder, memorando ou ofício, e-mail e outros.

O uso dos sistemas de informação contribui para a aplicação do Programa de Governo Eletrônico do Estado brasileiro, criado para dar uma nova gestão pública que seja capaz de tornar eficientes as funções governamentais, universalizar o acesso aos serviços e promover a transparência de suas ações (BRASIL, 2000). No entanto, proporcionais ao aumento da eficácia dos serviços públicos são os ataques à rede por pessoas que a usam a fim de compartilhar e distribuir programas mal intencionados. Nesse caso, as vulnerabilidades já inerentes aos sistemas de informação e às oriundas da internet forçam as organizações a tratarem seus sistemas com políticas de gestão da segurança da informação.

2.4 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Existem inúmeros argumentos que consolidam a importância das informações para o setor empresarial. No entanto, não basta estar ciente desse valor e utilizar a informação como ferramenta para atingir os objetivos empresariais, é necessário criar mecanismos que façam garantir o seu fluxo ininterrupto. Albertin (2010, p. 4) argumenta que, “quanto mais complexo é o ambiente computacional, quanto mais recursos são disponibilizados aos usuários, e quanto mais informação é requerida, mais difícil se torna garantir a confidencialidade e integridade das informações”. Observa-se, nesse caso, a importância que as organizações devem atribuir a esse assunto, procurando criar mecanismos ou políticas internas que garantam a segurança das informações manuseadas nos setores.

A Segurança da Informação (SI) é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003, p.43). Segundo o Governo Federal Brasileiro, ela é definida como

> a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a

> segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000)

Para Beal (2011, p. 52), “a segurança é uma área da gestão da informação que diz respeito a todas as etapas do fluxo informacional cujo objetivo é garantir a proteção da informação de acordo com os requisitos de sigilo, integridade, autenticidade, disponibilidade e irretratabilidade da comunicação”. O requisito referente ao sigilo procura proteger a informação contra a divulgação indevida que, acrescentado ao da integridade, evita a modificação não autorizada. Com respeito ao requisito da autenticidade, a informação tem garantia de ser proveniente de uma fonte verdadeira e fica disponível aos usuários com a garantia do requisito da disponibilidade. Por fim, de acordo com Beal (Ibidem, p. 52), o requisito da irretratabilidade protege contra a alegação por um dos integrantes da comunicação de que ela não aconteceu.

Outros conceitos relativos à confidencialidade, integridade e disponibilidade encontram-se na NBR ISO/IEC 27001:

> a) disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
> b) confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
> c) integridade: propriedade de salvaguarda da exatidão e completeza de ativos (ABNT, NBR ISSO/IEC 27001, 2006)

A NBR ISO/IEC 27001 representa a segunda parte da ISO/IEC 1799 e foi implantada no país em 2006. “Essa Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)” (ABNT NBR ISO/IEC 27001, 2006, p. 5). O SGSI tem a função de “assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas” (ABNT NBR ISO/IEC 27001, p. 5). Pretende-se que os requisitos dessa norma sejam aplicáveis a todas as organizações sem determinação de tipo, tamanho e natureza.

As normas são documentos orientadores com regras mínimas de segurança e qualidade para se produzir algo ou realizar determinado serviço. A Associação Brasileira de Normas Técnicas (ABNT), junto com o Comitê Brasileiro de Computadores e Processamento de Dados e com a Comissão de Estudo de Segurança Física em Instalações de Informática, elaborou a ABNT ISO/IEC 27000 e séries, de origem britânica e publicada internacionalmente pela *International Organization for Standartization* (ISO). São elas:

ISO/IEC 27001:2005 – publicada em 30/04/2006, tem como títulos Tecnologia da Informação, Técnica de Segurança e Sistemas de Gestão de Segurança da Informação;

ISO/IEC 27002:2005 – passou a ser válida a partir de 30/09/2005 e tem como título diferenciado o Código de prática para a gestão de segurança da informação. Ela estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação. Os objetivos definidos nela provêm diretrizes gerais sobre as metas geralmente aceitas para SGSI;

ISO/IEC 27003:2010 – publicada em 04/11/2011, tem os seguintes tópicos: Tecnologia da Informação, Técnicas de segurança e Diretrizes para implantação de um SGSI.

ISO/IEC 27004:2009 – foi publicada em 01/04/2010 e acrescenta os títulos Gestão da segurança da informação e a Medição;

ISO/IEC 27005:2008 – publicada em 07/07/2008 e validada um mês depois, acrescenta em seus títulos a questão da Gestão de riscos de segurança da informação;

ISO/IEC 27011:2008 – foi validada em 11/12/2009 e tem como objetivo fornecer diretrizes para a gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.

Além das normas de origem internacional que garantem a certificação ISO para as empresas, temos outros dispositivos legais, de caráter federal, relacionados à segurança da informação. É o caso da Constituição Federal (1988), das Leis, dos

Decretos e das Instruções Normativas. De acordo com Araújo (2009, p. 41), “a segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software”.

Nesse contexto, é importante que a gestão de segurança da informação esteja associada a uma prática administrativa utilizada por todos os membros de uma organização, e para sua eficácia é necessária uma estrutura organizacional capaz de planejar e implementar os controles desejados (MENEZES, 2006).

Beal (2005) aponta que, nas organizações, há uma tendência a se atribuir as atividades e as responsabilidades de segurança à unidade de tecnologia da informação. Isso acontece porque a maioria dos problemas de segurança tem relação com os diferentes suportes que a informática proporciona ao meio informacional. Nesse caso, percebe-se que os aspectos físicos, humanos e de gestão de processos são colocados fora do contexto operacional, e isso prejudica a qualidade da segurança alcançada (ALVES, 2006).

Outro fator relevante para melhorar a qualidade da segurança da informação é o envolvimento da cúpula estratégica da organização no processo. Sobre esse aspecto, Fugini e Bellettini (2004) salientam:

> [...] a segurança da informação exige uma abordagem em nível estratégico plenamente integrado ao negócio da organização. Sem isso, será sempre uma área com pouca importância, reativa, passiva, atuando somente quando os problemas ocorrerem. Infelizmente, a tendência de não implantação de procedimentos de segurança até que ocorra algum problema é bastante comum na literatura [...]

A identificação dos controles a serem implantados num sistema de segurança da informação requer um planejamento cuidadoso, muita atenção aos detalhes em toda a organização e, consequentemente, a participação de todos os indivíduos que fazem parte dela (ARAÚJO, 2009, p. 41). O patrocínio da alta administração para incorporar um comportamento de proteção às informações é de fundamental importância, principalmente pelo fato de essas práticas serem complexas e exigirem dinheiro e tempo para serem implantadas. Além do mais, esse envolvimento da cúpula estimula os gestores e os colaboradores da organização, independentemente da área em que atuam. Contudo, fatores como tempo e curso

impedem que toda e qualquer informação que tramite em uma organização seja protegida. Para oferecer os níveis de proteção adequados a cada tipo de informação, é necessário classificá-la.

2.4.1 Classificação da informação quanto à segurança

Algumas informações, por sua natureza, devem ter seu sigilo preservado. Além das razões de interesse estratégico, a informação pode exigir tratamento confidencial por outros motivos, entre os quais, destaca-se a necessidade de preservar a privacidade dos dados pessoais coletados.

Existem diversas formas de classificar a informação. O decreto nº 4.553/2002 classifica os dados ou informações quanto ao grau de sigilo. Seu detalhamento é apresentado no quadro abaixo:

Quadro 2 – Classificação da informação quanto aos requisitos de sigilo

ULTRASSECRETOS	SECRETOS	CONFIDENCIAIS	RESERVADOS
• Aqueles cuja revelação não autorizada acarrete dano excepcionalmente grave à segurança da sociedade e do Estado. Exemplo: planos e operações militares	• Aqueles cuja revelação não autorizada acarrete dano grave à segurança da sociedade e do Estado. Exemplo: Assuntos diplomáticos	• Aqueles que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e, se revelados sem autorização, frustre os objetivos ou acarrete dano à sociedade e ao Estado.	• Sua divulgação não autorizada compromete planos, operações e objetivos neles previstos.

Fonte: (BRASIL, 2002- Adaptado pelo autor).

Embora a Legislação Federal mencione apenas a classificação relativa ao sigilo da informação, é importante para qualquer organização, seja ela pública ou privada, estabelecer também classificações para a informação relativas aos seus requisitos de disponibilidade, integridade e autenticidade (BEAL, 2011, p. 60).

Classificar a informação quanto aos requisitos de proteção é uma das medidas elencadas para incorporar a política de segurança da informação numa entidade. Essa política é de extrema importância para que haja uma boa comunicação

entre os integrantes da organização com respeito às responsabilidades atribuídas e ao comportamento esperado em relação à informação.

2.4.2 Política de Segurança da Informação

Uma política de segurança da informação (PSI) é formada por diretrizes, regras e princípios corporativos, destinados a governar a proteção dos ativos de informação e orientar os seus participantes (CARUSO et. al., 1999, p. 367). A norma ABNT NBR ISSO/IEC 27001 (2006, p. 2) define o ativo como “qualquer coisa que tenha valor para a organização”, portanto, uma PSI deve ser encarada como um ponto de forte importância e impacto na organização, representando o mais alto nível de documentação da segurança da informação. Embora os padrões, os procedimentos e os guias estejam num nível mais baixo, isso não quer dizer que eles sejam menos importantes. Segundo o Ministério do Planejamento Orçamento e Gestão, “as políticas superiores devem ser definidas como em primeiro lugar por questões estratégicas, enquanto os outros documentos seguem como elementos táticos” (BRASIL, 2005, p. 4).

A fim de estabelecer diretrizes relativas à política de Segurança da Informação e Comunicações (SIC), nas entidades da Administração Pública Federal, o Decreto nº 3.505, de 13 de junho de 2000, tem como pressupostos básicos:

> a) assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
> b) proteção de assuntos que mereçam tratamento especial;
> c) capacitação dos segmentos das tecnologias sensíveis;
> d) uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
> e) criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
> f) capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado;
> g) conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade. (BRASIL, 2000)

Os elementos normalmente encontrados em uma política de segurança de informação incluem:

- Identificar, em todos os níveis da organização, quem é o responsável e presta contas pela informação, bem como, as linhas hierárquicas para essas funções;
- Classificar as informações analisando o valor que elas representam para a instituição e o custo dela;
- Estabelecer o padrão mínimo de segurança para aplicação em todos os sistemas corporativos e orientar a encontrar, mediante análise de risco, os pontos que merecem medição extra de proteção;
- Reconhecer que a proteção efetiva deverá estar sempre presente em todo o desenvolvimento do sistema ao invés de ser adicionada num momento posterior;
- Implementar a segurança da informação nos procedimentos operacionais, estabelecendo controles de acesso e auditoria interna;
- Determinar a política de segurança de pessoal e treinamento;
- Atentar para os procedimentos de controle de material proprietário e de licenças de uso de software e fazer as adaptações necessárias para garantir adequação à legislação aplicável;
- Criar uma política quanto ao relatório e investigação de incidentes de segurança, bem como requisitos de planejamento para continuidade do serviço;
- Estabelecer uma política de segurança da informação que responda às mudanças da organização de acordo com as suas necessidades, pois, desse modo, ela não ficará estática (BEAL, 2011, p. 55).

Um programa de gestão em segurança da informação deve estabelecer uma política bem estruturada e que seja baseada em evidências que permitam conferir à empresa o nível pretendido pela Administração. Esse processo é composto por uma sequência de fases, em que os riscos devem ser determinados e classificados. Conforme Silva at. al. (2003, p. 34), a análise de riscos garante um conjunto de medidas de segurança que permitirão reduzir ou eliminar os riscos a que a empresa está sujeita.

2.5 ANÁLISE DE RISCO COM FOCO NA SEGURANÇA DA INFORMAÇÃO

Os riscos sempre farão parte dos sistemas de informação, afinal, embora o seu significado tenha mudado, não é um novo problema ou uma nova terminologia, e os seres humanos sempre tiveram de enfrentá-los no ambiente em que vivem (LAUREANO, 2005, p. 70). Os riscos representam a “probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios” (SÊMOLA, 2003, p. 50). Os autores Silva, Carvalho e Torres (2003, p. 253) são mais objetivos na definição de risco quando o apontam como “exposição a determinada ameaça”.

Em razão de sua importância para os negócios em geral, os riscos, em tecnologia da informação, devem ser tratados de modo semelhante aos outros principais riscos, tais como: risco estratégico, ambiental, de mercado, de crédito, operacional, ou seja, todos aqueles que resultem na incapacidade de alcançar os objetivos da organização (ISACA, 2009, p. 11). Além disso, entender os riscos envolvidos e aplicar um processo de acordo com o negócio da empresa garantirá que os gastos estejam entre aqueles que realmente são necessários (PELTIER, 2005, p. 3).

O sucesso de uma gestão de risco depende da capacidade de quantificar esses riscos e de decidir quais deles estão dispostos a ocorrer. Portanto, gestão de risco é o processo que permite aos gerentes de Tecnologia da Informação (TI) equilibrarem o funcionamento e os custos econômicos referentes às medidas de proteção, obtendo ganhos na missão de proteger sistemas e dados organizacionais (STONEBURNER at al, 2002, p.4). É o “uso sistemático de informações para identificar fontes e estimar o risco” (ABNT NBR ISO/IEC 27001:2006). O gerenciamento de riscos não é “uma ciência exata, ele reúne os melhores julgamentos coletivos de indivíduos e grupos responsáveis pelo planejamento estratégico, supervisão, gerenciamento e operação das organizações” (NIST, 2011, p. 1, tradução nossa). Além do mais, permite que uma empresa assuma o controle de seu próprio destino em que apenas os métodos e as garantias que são realmente necessários serão utilizados (PELTIER, 2005, p. 3).

Vários termos e definições são adotados nos processos de gestão de risco que necessitam de entendimento. Nesse caso, o quadro 3 relaciona os termos dessa gestão de segurança.

Quadro 3 – Termos relacionados à gestão de risco

Termo	Descrição	Autor
Ameaça	A presença de todo evento potencial que causar um impacto indesejável na organização é chamada de ameaça. Pode ser provocada ou natural, ter um efeito pequeno ou grande na segurança ou na viabilidade de uma companhia.	Krutz e Vines (2001, p. 19-20)
Ativo	É um recurso, processo, produto, ou infra-estrutura, e assim por diante, que uma organização determinou que deve ser protegido. A perda desse recurso poderia afetar a confidencialidade, integridade ou disponibilidade. Pode ser tangível ou intangível, podendo afetar a continuidade do negócio de uma organização. O valor de um ativo é composto de todos os elementos que são relacionados a esse recurso: sua criação, desenvolvimento, sustentação, reposição, credibilidade, custos considerados e valor de aquisição.	Krutz e Vines (2001, p. 19-20)
Brecha	É quando um mecanismo da segurança pode ser contornado por uma ameaça. Quando uma brecha é combinada com um ataque, pode resultar em uma invasão.	Tittel et al. (2003, p. 181)
Exposição	Suscetibilidade para perda de um ativo devido a uma ameaça; há possibilidade que uma vulnerabilidade seja explorada por um agente ou por um evento da ameaça. A exposição não significa que um evento de perda esteja ocorrendo realmente. Significa que, se houver uma vulnerabilidade e uma ameaça que possam ser exploradas, existe a possibilidade de ocorrer uma exposição.	Tittel et al. (2003, p. 180)
Invasão	É quando um agente da ameaça ganha o acesso à infraestrutura de uma organização com a subversão dos controles de segurança e pode infringir danos diretamente aos ativos.	Tittel et al. (2003, p. 181)
Proteção	É um controle ou as contramedidas empregadas para reduzir o risco associado a uma ameaça específica, ou o grupo de ameaças.	Krutz e Vines (2001, p. 19-20)
Risco	É a possibilidade de que uma ameaça específica venha explorar uma vulnerabilidade específica e causar dano a um ativo.	Tittel et al. (2003, p. 180)
Vulnerabilidade	É a ausência ou a fraqueza de uma proteção. Uma ameaça mínima tem o potencial de transformar-se em grande ameaça, ou em ameaça mais frequente, por causa de uma vulnerabilidade.	Krutz e Vines (2001, p. 19)

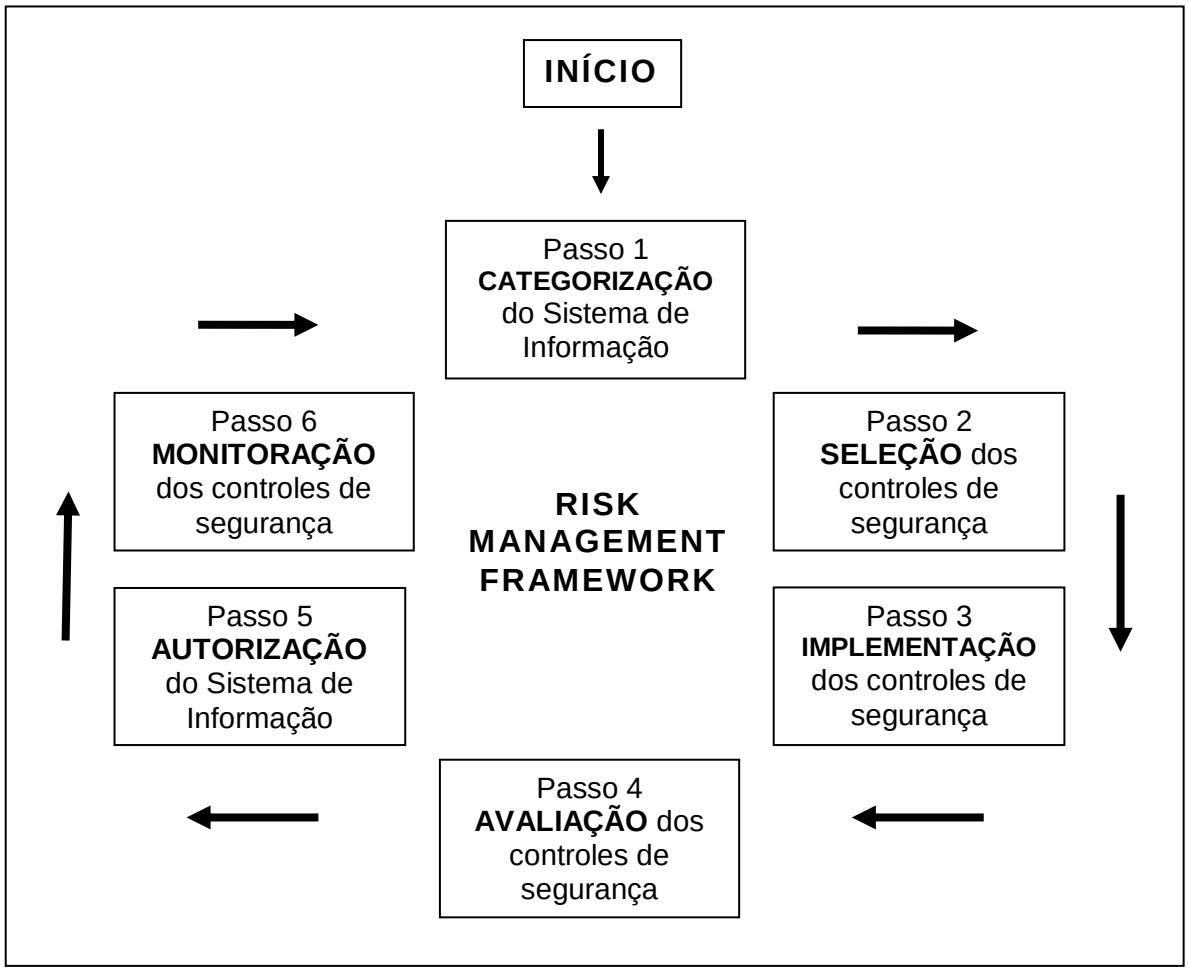
Fonte: ARAÚJO (2009), p. 51.

2.5.1 Métodos: RMF, GRSIC e FRAAP

O *National Institute of Standards and Technology* (NIST) é uma agência governamental não regulatória do Departamento de Comércio dos Estados Unidos que, entre suas responsabilidades, desenvolve padrões, normas e orientações de segurança para os sistemas de informação federais (NIST, 2010, p. 1). Em razão

dessa diretriz, o NIST publicou o método *Risk Management Framework (RMF*), que “fornece um processo disciplinado e estruturado que integra as atividades de gerenciamento de informações de segurança e de risco no ciclo de vida do sistema em desenvolvimento” (NIST, 2010, p. 7, tradução nossa). A figura 4 demonstra, de forma abrangente, esse procedimento.

Figura 4 – Processo RMF



Fonte: NIST (2010)

A estrutura da gestão de risco RMF, ilustrada na figura 4, inclui os seguintes passos:

- **Categorizar** o sistema de informação e as informações processadas, armazenadas e transmitidas através de uma análise de impacto;
- **Selecionar** um conjunto inicial de controles de segurança de linha de base para o sistema de informação mediante a categorização da

> informação e, se necessário, através de uma avaliação organizacional de risco e de condições locais;
>
> - **Avaliar** os controles de segurança usando os procedimentos adequados para determinar o grau correto de adequação e funcionamento, a fim de produzir o resultado desejado em relação ao cumprimento dos requisitos de segurança do sistema;
> - **Autorizar** o funcionamento do sistema de informação com base na determinação do risco para as operações organizacionais, ativos, indivíduos, governo, resultante da operação do sistema de informação e da decisão de que esse risco é aceitável;
> - **Monitorar** os controles de segurança do sistema de informação de forma contínua, incluindo a avaliação de sua eficácia, documentando as mudanças no ambiente de operação e relatando o diagnóstico para os funcionários envolvidos (NIST, 2010, p. 7,8, tradução nossa).

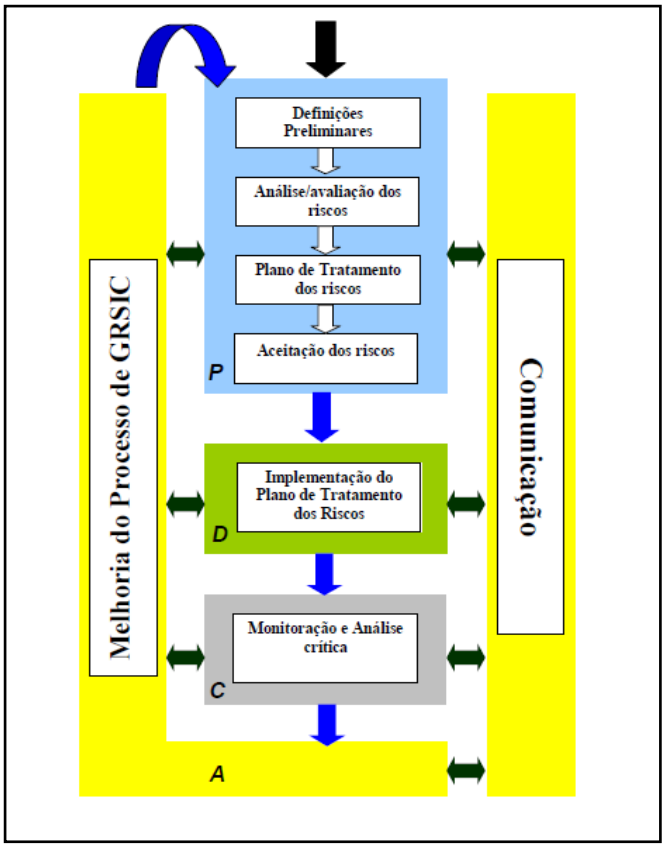
O governo brasileiro, também preocupado com a segurança das informações de seus sistemas federais, estabeleceu junto com o Departamento de Segurança da Informação e Comunicações (DSIC), a Instrução Normativa nº 04/IN01/DSIC/GSIPR, emitida em 14/08/2009, estabelecendo diretrizes para o processo de GRSIC (Gestão de Riscos de Segurança da Informação e Comunicações) nos órgãos ou entidades da Administração Pública Federal, direta e indireta. Salienta-se que a referida instrução normativa recebeu sua primeira revisão e sua emissão procedeu a partir de 15 de fevereiro de 2013.

Primeiramente, o processo GRSIC baseia-se no ciclo PDCA (*Plan-Do-Check-Act* / Planejar-Fazer-Verificar-Agir), uma sequência de passos utilizados para controlar qualquer processo definido. O uso dos ciclos pode ser assim relatado: 1 – planejar envolve definir como será feito (quem, o que, quando, onde, como) e as metas e os métodos para se atingir o objetivo; 2 – fazer significa tomar a iniciativa, educar, treinar, implementar, executar o planejado conforme as metas e os métodos definidos; 3 – verificar consiste em checar os resultados que estão sendo obtidos e de forma contínua, garantindo a execução dos trabalhos programados; 4 – agir determina fazer as correções necessárias através de ações corretivas ou melhorias.

Através da figura 4, observa-se que o processo de GRSIC é formado pelas fases de “definições preliminares, análise/avaliação dos riscos, plano de tratamento

dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração, análise crítica, melhoria do processo de Gestão de Riscos de Segurança da Informação e Comunicações e comunicação do risco" (04/IN/DSIC/GSI/PR, 2013, p. 5).

Figura 5 – Processo de GRSIC



Fonte: BRASIL, 2013 (Anexo A).

Nesse contexto, e de acordo com a Instrução Normativa 04/IN01/DSIC/GSI/PR, revisada em 15/08/2013, as etapas do GRSIC são assim definidas:

- **Definições preliminares** - nessa etapa, analisa-se a organização, a fim de estruturar o processo de GRSIC, considerando-se as características do órgão e as restrições a que estão sujeitas. Nesse caso, define-se o escopo que pode abranger o órgão como um todo, um segmento, um processo, um sistema, um recurso ou um ativo da informação. É importante que o GRSIC atenda aos objetivos gerais e ao escopo definido, contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.

- **Análise/avaliação dos riscos** - nesse momento, identificam-se os ativos e seus respectivos responsáveis dentro do escopo estabelecido; apuram-se os riscos levando em consideração as ameaças, as vulnerabilidades e as ações já existentes de segurança da informação; estimam-se os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados; avaliam-se os riscos, determinando se são aceitáveis ou se requerem tratamento; relacionam-se os riscos que necessitam de tratamento, priorizando-os de acordo com os critérios determinados pelo órgão.
- **Plano de tratamento dos riscos** – a partir daqui, as formas de tratamento dos riscos serão determinadas considerando-se as opções de reduzir, evitar, transferir ou reter o risco; atentando para a eficácia das ações de segurança já existentes, tendo em vista as restrições organizacionais, técnicas e estruturais, os requisitos legais e a análise de custo/benefício.
- **Aceitação do risco** – nessa quarta etapa, os resultados dos processos anteriores serão verificados de acordo com o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.
- **Implementação do Plano de Tratamento dos Riscos** – é a execução das ações de Segurança da Informação e do Plano de Tratamento dos Riscos aprovado.
- **Monitoração e análise crítica** - essa etapa apresenta as seguintes ações: detectar possíveis falhas nos resultados, monitorar os riscos e as ações de segurança da informação e checar a eficácia do processo de GRSIC.
- **Melhoria do processo de GRSIC** – cabe, nessa fase, propor à autoridade decisória do órgão a necessidade de implementar as melhorias identificadas na etapa anterior e, depois de aprovadas, executá-las, assegurando que as melhorais atinjam os objetivos desejados.

- **Comunicação do Risco** - procura manter as instâncias superiores informadas sobre todas as fases da gestão do risco, compartilhando as informações entre a autoridade decisória e as demais partes envolvidas e interessadas (BRASIL, 2009, p. 4, 5).

O último passo da sequência de processos para análise de risco abordados nesta pesquisa é o Facilitated Risk Analysis and Assessment Process (FRAAP). 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 4, abaixo, demonstra-se as semelhanças e as diferenças entre os dois tipos de análise.

Quadro 4 – Análise de risco quantitativa e qualitativa

Propriedade	Quantitativa	Qualitativa	Autor
Análise custo/benefício	sim	não	(KRUTZ e VINES, 2001, p. 23) TITTEL et al., (2003, p. 188)
Cálculos complexos	sim	não	(KRUTZ e VINES, 2001, p. 23) TITTEL et al., (2003, p. 188)
Custos financeiros	sim	não	(KRUTZ e VINES, 2001, p. 23)
É objetiva	sim	não	TITTEL et al., (2003, p. 188)
Envolve suposições	baixa	alta	(KRUTZ e VINES, 2001, p. 23) TITTEL et al., (2003, p. 188)
Envolve tempo/trabalho	alta	baixa	KRUTZ e VINES, (2001, p. 23) TITTEL et al., (2003, p. 188)
Fácil comunicação	alta	baixa	KRUTZ e VINES, (2001, p. 23)
Oferece resultados úteis e significativos	sim	sim	TITTEL et al., (2003, p. 188)
Pode ser automatizada	sim	não	KRUTZ e VINES, (2001, p. 23) TITTEL et al., (2003, p. 188)
Requer grande volume de informações	alta	baixa	KRUTZ e VINES, (2001, p. 23) TITTEL et al., (2003, p. 188)
Resulta em valores específicos	sim	não	TITTEL et al., (2003, p. 188)
Usa opiniões	não	sim	TITTEL et al., (2003, p. 188)

Fonte: 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).

2.5.2 Ameaças

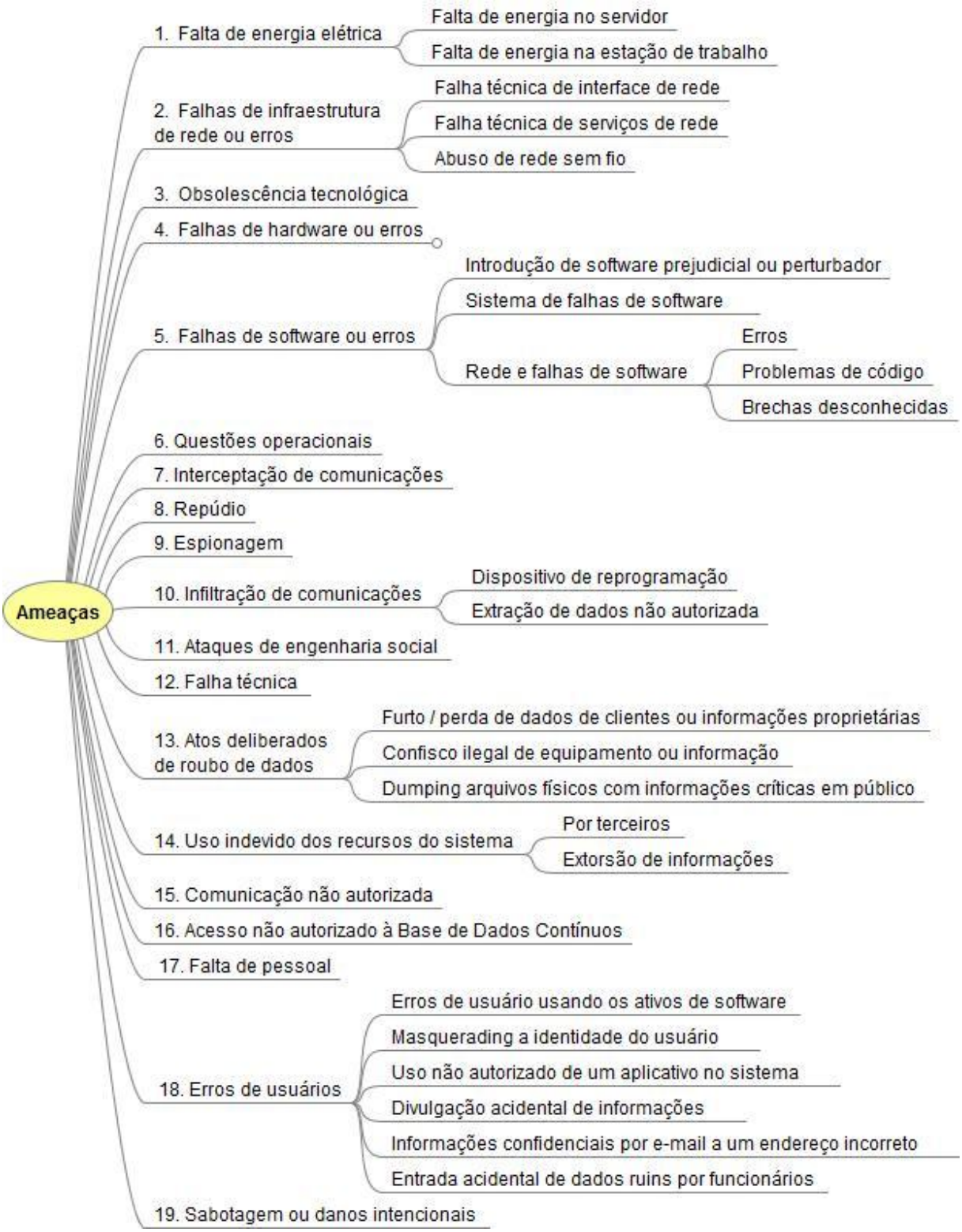
Quanto a sua intencionalidade, as ameaças são classificadas de acordo com os seguintes grupos:

> **Naturais** – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.
> **Involuntárias** – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.
> **Voluntárias** – Ameaças propositais causadas por agentes humanos como *hacker*s, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários (SÊMOLA, 2003, p. 47, 48).

Uma lista de ameaças é importante, porém, deve ser usada adequadamente para não causar impacto negativo no fluxo de ideias e informações. Deverá ser usada para garantir que tudo seja coberto ou identificado, todavia, não há determinação de que todo o processo de avaliação de risco esteja completo (PELTIER, 2009, p. 18).

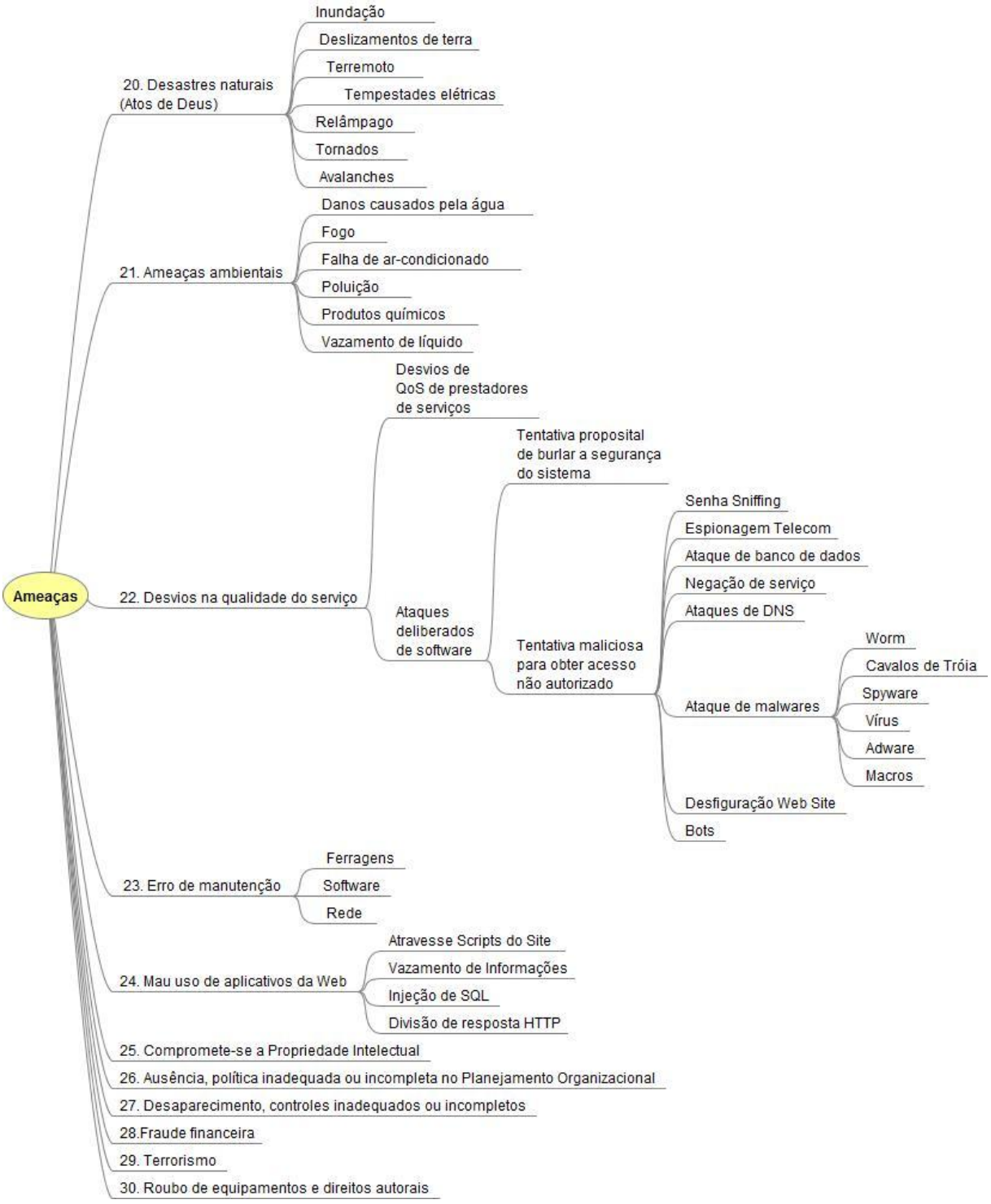
Para classificar as ameaças, é possível criar uma “árvore” cujos ramos correspondam aos tipos de ameaça, e as folhas, às ameaças em si. O quadro 5 demonstra esse arranjo:

Figura 6 – Árvore de ameaças para prestadores de serviços, itens 01 a 19



Fonte: Shahri et. al. (2012, p. 173, tradução nossa, elaborada pelo Freemind)

Figura 7 – Árvore de ameaças para prestadores de serviço, itens 20 a 30



Fonte: Shahri et. al. (2012, p. 173, tradução nossa, elaborada pelo Freemind)

A árvore poderá ser criada pelo responsável em segurança, através da investigação do tipo e da quantidade de ameaças que ocorrem anualmente. A dimensão e a composição dela dependem de fatores organizacionais relacionados ao setor de atividade, à dispersão geográfica, à dimensão e ao tipo de atividade desenvolvida (SILVA, 2003, p. 36).

Entre as ameaças demonstradas no quadro 5, o ataque de *malwares* demonstrou ter um crescimento significativo em 2012. Segundo o Cert.Br[5], só em uma categoria dessa ameaça, chamada de *worm*, houve 38.466 ocorrências no ano passado, ou seja, um crescimento de 43% em relação a 2011. *Malware* é um termo genérico empregado para designar todos os tipos de softwares indesejados, por exemplo: vírus, *worms*, cavalos de Tróia, *Spyware* e *Adware*. Esses códigos maliciosos podem infectar ou comprometer o computador de várias maneiras, entre elas: a) explorando vulnerabilidades encontradas nos programas instalados; b) executando arquivos infectados que o usuário adquire através de e-mails, mídias removíveis ou em páginas maliciosas da web; c) invadindo diretamente o computador do usuário e implantando o arquivo com os códigos maliciosos; d) através da autoexecução de mídias removíveis infectadas, tipo *pen-drives*. Depois de instalados, os *malwares* acessam os dados do computador e podem executar ações em nome do usuário, de acordo com as permissões que ele executa no sistema (VLACHOS et. al., 2007, p. 298).

Os principais tipos de *malwares* são:

a) Vírus

É um programa ou parte dele que se "espalha através de arquivos infectados, páginas que exploram vulnerabilidades no navegador, e-mails, e assim por diante, geralmente utilizando alguma técnica de engenharia social que leve o usuário a clicar em um link ou executar um arquivo" (MORIMOTO, 2010, p. 389).

b) Worms

São diferentes pela forma como infectam as máquinas, pois não dependem do usuário para executar o arquivo infectado e se replicam diretamente explorando

[5] "Análise de alguns fatos de interesse observados nesse período". Núcleo de Informação e Coordenação do Ponto BR. Disponível em: < http://www.cert.br/stats/incidentes/2012-jan-dec/analise.html> Acesso em: 12 de dezembro de 2012.

vulnerabilidades de segurança nas máquinas em rede. *Os worms* consomem muitos recursos do sistema devido a sua grande quantidade de propagação, causando diminuição no desempenho de redes e de computadores (TURBAN et. al., 2005, p. 449).

c) Cavalos de Troia (*Trojans*)

São similares aos vírus, mas seu objetivo principal é de abrir portas e oferecer alguma forma de acesso remoto à máquina infectada. Eles são muitos discretos, criados de uma forma que o usuário não perceba que seu computador está infectado. Essa situação “permite que o invasor roube senhas, use a conexão para enviar spam, procure informações valiosas no HD, ou mesmo use máquinas sob seu controle para executar ataques diversos em outros computadores” (MORIMOTO, 2010, p. 389).

d) Spyware

Tipo de programa que monitora as atividades de um sistema e envia as informações a terceiros. O seu uso pode ser legítimo quando o usuário consente que seu equipamento seja varrido e se verifique se outras pessoas o estão utilizando abusivamente, ou malicioso, quando a monitoração compromete a privacidade do usuário, deixando o computador vulnerável à capitação de dados sobre sua navegação ou inseridos em outros programas, como conta de usuário e senha.

d) Adware

Pode ser considerado como um subgrupo do spyware devido à semelhança quanto à forma de infecção e desinstalação. Trata-se de programas que expõem propagandas indesejadas, direcionadas de acordo com a navegação do usuário para efetuar monitoramento invisível e indevido.

Outra ameaça que ataca sistemas conectados à Internet é o *Scan.* É uma técnica utilizada para varreduras em redes de computadores, objetivando identificar os equipamentos ativos e quais serviços estão sendo disponibilizados por eles.

Segundo o Cert.Br[6], esse mecanismo é amplamente utilizado por atacantes que desejam identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador. A quebra de segurança é consumada quando, nos negócios e seus processos, compostos por ativos físicos, tecnológicos e humanos, são alvo de investidas, que buscam identificar um ponto fraco compatível, ou seja, uma vulnerabilidade capaz de potencializar uma ação (SÊMOLA, 2003, p. 18).

2.5.3 Vulnerabilidades e controles

A vulnerabilidade é "a suscetibilidade do sistema ao dano causado pela ameaça" (TURBAN et. al., 2005, p. 446). Identificar pontos vulneráveis no sistema é um aspecto importante na formulação de medidas adequadas de segurança, pois eles estão presentes no dia a dia das empresas e se apresentam nas mais diversas áreas de uma organização (LAUREANO, 2005, p. 17). Sobre isso, Turban et. al. (2005, p. 445) abordam:

> Teoricamente, existem centenas de pontos em um sistema de informação corporativo que podem estar sujeitos a alguma ameaça. E, na realidade, existem milhares de formas diferentes em que os sistemas de informação podem ser atacados ou danificados (TURBAN et. al., 2005, p. 445).

As redes de telecomunicação exigem arranjos mais complexos e diversos de hardware, software, pessoais e organizacionais, que ajudam na criação de novas vulnerabilidades. Muitas dessas oportunidades de ação para as ameaças são exemplificadas por Sêmola (2005, p. 49):

> **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, riscos de explosões, vazamentos ou incêndio.
> **Naturais** – Computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura etc.

---

[6] "Incidentes Reportados ao CERT.br". Núcleo de Informação e Coordenação do Ponto BR. Disponível em: < http://www.cert.br/stats/incidentes/2012-jan-dec/tipos-ataque.html>. Acesso em: 12 dezembro 2012.

> **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. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
> **Comunicação** – Acessos não autorizados ou perda de comunicação.
> **Humanas** – Falta de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras.

Logo após o conhecimento dos riscos acarretados numa organização, é preciso definir as medidas que serão capazes de aumentar a sua segurança. Nesse momento, é necessário identificar e selecionar os controles que irão salvaguardar os sistemas de informação e assegurar que eles funcionem segundo os padrões administrativos.

De acordo com Laudon et. al. (2004, p. 467),

> os controles consistem, portanto, em todos os métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e confiabilidade de seus registros e a adesão operacional aos padrões administrativos.

Os controles nos sistemas de informação são desenvolvidos para monitorar e manter a qualidade e a segurança das atividades de entrada, processamento, saída e armazenamento de informações. O quadro 6 mostra os vários tipos de controle:

Quadro 5 – Controles gerais e de aplicação para os sistemas de informação

TIPO			FINALIDADE	AUTOR
Controles Gerais	Físicos		Proteger fisicamente os recursos de computação e detectar eventual mau funcionamento.	TURBAN et al., 2005, p. 452) e LAUDON e LAUDON, 2004, p. 469.
	De acesso		Restringir o acesso de usuários não autorizados aos recursos de computação: ênfase na identificação do usuário através de senha, cartão inteligente, ficha e biometria.	TURBAN et al., 2005, p. 452)
	De segurança de dados		Proteger valiosos arquivos de dados empresariais em disco ou fita de acesso não autorizado, alteração ou destruição enquanto eles estão em uso ou armazenados.	LAUDON e LAUDON, 2004, p. 469.
	Administrativos		Padronizar regras, procedimentos e disciplinas de controles formalizados, destinados a garantir que os controles gerais e de aplicação da organização sejam executados e impostos adequadamente.	LAUDON e LAUDON, 2004, p. 469.
	De comunicações (rede)	Segurança de fronteira	Controlar o acesso ao sistema.	TURBAN et al., 2005, p. 452)
		Firewalls	Impor política de controle de acesso entre duas redes.	TURBAN et al., 2005, p. 452)
		Controles de vírus	Utilizar software antivírus	TURBAN et al., 2005, p. 452)
		Detecção de intrusão	Detectar acesso não autorizado à rede.	TURBAN et al., 2005, p. 452)
		Rede privada virtual	Usar a internet para transportar informações dentro de uma empresa e entre parceiros comerciais, mas com segurança reforçada pelo uso de criptografia, autenticação e controle de acesso.	TURBAN et al., 2005, p. 452)
	Autenticação		Tem como objetivo a prova de identidade.	TURBAN et al., 2005, p. 452)
	Autorização		Conceder permissão a pessoas e grupos para certas atividades com recursos de informação, com base na identidade verificada.	TURBAN et al., 2005, p. 452)
Controles de aplicação	Físicos		Programar rotinas que podem ser executadas para editar erros em dados de entrada antes de seu processamento.	LAUDON e LAUDON, 2004, p. 469.
	De processamento		Assegurar que os dados estejam completos, válidos e exatos, quando estiverem sendo processados, e que os programas estejam sendo corretamente executados.	TURBAN et al., 2005, p. 452)
	De saída		Confirmar se os resultados do processamento sejam exatos, válidos, completos e consistentes.	TURBAN et al., 2005, p. 452)

Fonte: Elaborado pelo autor (2012)

Os controles gerais estruturam o projeto, a segurança e o uso dos sistemas de informação, bem como a segurança dos arquivos de dados em geral, em toda a infraestrutura de tecnologia da informação. De modo geral, representam uma combinação de hardware, software e procedimentos manuais que garantem um ambiente de controle total nas organizações (LAUDON et. al., 2004, p. 468). Todavia, quanto aos controles de aplicação, são determinados para a área específica da empresa em um sistema particular e de procedimentos programados.

Para garantir a segurança nos sistemas de informação, as organizações podem usar intensamente os mecanismos de controle previamente identificados. No entanto, utilizar todas as opções disponíveis pode ser muito complicado e ter um custo excessivamente elevado de forma que o sistema se torne econômico e operacionalmente inviável. Nesse caso, “é preciso fazer certa análise custo/benefício para determinar quais mecanismos de controle oferecem as salvaguardas mais eficientes sem sacrificar a eficiência operacional ou de custo” (LAUDON et. al, op. cit., p. 468). Uma boa regra é não implantar um controle que custe mais do que o ativo a proteger, pois, caso contrário, o retorno sobre o investimento será baixo (PELTIER, 2009, p. 27).

Ao selecionar qualquer tipo de controle, será necessário medir o impacto operacional que, de alguma maneira, ele trará para a organização. Esse impacto poderá surgir com base na despesa de implantação, na produtividade, no tempo de resposta e, até mesmo, no efeito sobre a equipe organizacional. Sobre seleção de controles, Laudon et. al (op. cit., p. 477) descrevem:

> Para decidir quais controles usar, os desenvolvedores de SI devem examinar varias técnicas de controle, comparando suas respectivas efetividades em custo. Uma deficiência de controle em algum ponto pode ser compensada por um forte controle em outro. Talvez não seja eficiente em custo instalar controles rígidos em todos os pontos de ciclo de processamento, se as áreas de maiores riscos já estiverem seguras ou se existirem controles compensatórios em outro lugar. A combinação de todos os controles desenvolvidos para uma aplicação particular determinará sua estrutura geral de controle.

Uma equipe de gestão de risco não deseja implantar um controle que coloque a empresa em um risco maior. Portanto, para um bom gerenciamento de riscos, é necessário encontrar os problemas, detectar as ameaças para priorizar as

vulnerabilidades, identificar e selecionar o nível adequado de controle, a fim de que, dependendo do caso, o risco seja eliminado ou reduzido a um nível aceitável.

3 A SEGURANÇA DA INFORMAÇÃO SOB A ÓTICA DA CIÊNCIA DA INFORMAÇÃO

A segurança da informação tornou-se um assunto importante no meio organizacional, pois, à medida que a tecnologia avança, mais dados e informações passam a ser armazenados em grande escala e levados a qualquer lugar do planeta de forma rápida e eficiente. A Internet é fator fundamental nesse mundo digital globalizado, porque contribui para o crescimento contínuo de transações eletrônicas, que incluem correspondências particulares, operações comerciais, bancárias, entre outras. É nesse cenário que as empresas investem em segurança da informação (SI), uma vez que procura assegurar a continuidade e a estabilidade do negócio e permitir que os usuários e os bens estejam seguros em relação às ameaças e aos perigos.

Através de uma revisão de literatura, na Biblioteca Digital de Teses e Dissertações (BDTD), cuja busca teve como termo o assunto “segurança da informação”, conseguiu-se um diagnóstico do que vem sendo estudado, em termos de trabalhos acadêmicos apresentados, durante o período de 2007 a 2011.

De acordo com os parâmetros disponíveis no portal da BDTD para a busca de documentos – assunto, objetivo e título - constatou-se que há um total de 56 (cinquenta e seis) teses e dissertações depositadas no país. Esses trabalhos estão distribuídos de acordo com a tabela 1:

Tabela 1 – Quantidade de teses e dissertações entre 2007 e 2011

Nível	**2007**	**2008**	**2009**	**2010**	**2011**	**TOTAL**
Tese	1	1	4	0	3	**9**
Dissertação	7	14	9	10	7	**47**
TOTAL	**8**	**15**	**13**	**11**	**10**	**56**

Fonte: BDTD. Disponível em bdtd.ibict.br, acesso em 29/05/2012.

O total da tabela 1 sofreu algumas exclusões, pois, na análise, constatou-se que o assunto objetivado pelos autores não condizem com a SI. Caso de uma tese

no ano de 2011 e de três dissertações - uma em 2008 e duas em 2010. Diante disso, o total de documentos que antes representava cinquenta e seis passou para cinquenta e duas unidades. Mesmo com a exclusão da dissertação de um trabalho em 2008, esse continuou sendo o ano com o maior número de obras produzidas sobre o tema “segurança da informação”.

Para classificar as teses encontradas, foram agrupados oito trabalhos de acordo com alguns temas relativos à SI. O quadro 7, abaixo, apresenta essa classificação:

Quadro 6 – Classificação das teses entre 2007 e 2011

Quant.	Tema	Autor
2	Autenticação	Silva, D. (2007); Wong (2011).
1	Gestão de Segurança da Informação	Alexandria (2009)
1	Medidas de segurança	Ferreira (2009)
1	Métricas/Métodos	Santos (2009).
2	Modelos teóricos	Albuquerque (2008); Shimanuki (2011).
1	Segurança do conhecimento	Araújo (2009)

Fonte: BDTD. Disponível em bdtd.ibict.br, acesso em 29/05/2012.

De acordo com o quadro 7, os temas foram representados baseados nos seguintes conceitos teóricos:

Autenticação – componente vital para sistemas que têm informações críticas, pois distingue usuários autorizados de outros não autorizados (SILVA, 2007, p. 14).

Gestão de Segurança da Informação – processo que visa “assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas” (ABNT, 2006, p. 5).

Medidas de segurança – referem-se a sistemas de proteção para navegadores web modernos e redes de computadores que demonstrem uma nova abordagem e produzam melhores resultados do que os existentes.

Métricas/Métodos – De acordo com Batista (2007, p. 37), “uma métrica consiste em uma unidade de medida e a correspondente medição (definição + processo) utilizada para medir ou avaliar uma determinada propriedade de uma unidade”. Portanto, métricas de segurança de software são ferramentas utilizadas

por profissionais de segurança da informação para avaliar os níveis de segurança de seus sistemas, produtos e processos, possibilitando tratar as ameaças existentes.

Modelos teóricos – apresentam metodologias para a implantação da segurança da informação, tomando como base diversos parâmetros, entre eles: a fenomenologia, os elementos gerais da gestão da segurança, os riscos do negócio, o *Balanced Scorecard*, as políticas arquivísticas e os padrões e normas atuais da SI em automação.

Segurança do conhecimento – processo que visa proteger os ativos do conhecimento, ou seja, aqueles presentes na mente dos colaboradores de uma organização e que são capazes de proporcionar aos produtos e aos serviços uma vantagem competitiva (ARAÚJO, 2009, p. 89).

Em relação às dissertações, as classificações das quarenta e quatro unidades encontradas estão demonstradas no próximo quadro 8:

Quadro 7 – Classificação das dissertações entre 2007 e 2011

Quant.	Tema	Autor
5	Criptografia	Oliveira (2007); Fagundes (2007); Ferreira (2008); Costa (2008); João Filho (2009).
4	Gestão de risco	Melo (2008); Pudenzi (2008); Santana (2009); Silva, L. (2010).
7	Gestão de segurança da informação	Mendonça (2007); Wilson Junior (2008); Silva, C. (2009); Oliveira (2009); Nobre (2009); Ribas (2010); Kronst (2010).
1	Medidas de segurança	Afonso (2011)
4	Medição de maturidade	Janssen (2008); Paranhos (2010); Gotteberg (2010); Britto (2011).
8	Modelos teóricos	Ramos (2007); Nascimento (2008); Fróio (2008); Souza (2008); Pinto (2008); Silva, R. (2010); Luz (2011); Azevedo (2011).
5	Métricas/Métodos	Favero (2007); Batista (2007); Winter (2010); Filho (2010); Amaral (2011).
3	Normas	Lorens (2007); Strohe (2009); Wagner (2011).
3	Percepção da segurança da informação	Sakaue (2008) e Silva, W. (2011).
4	Política de segurança da informação	Benz (2008); Moreira (2009); Fachini (2009); Ellwangner (2009).
1	Segurança do conhecimento	Jacinto (2008).

Fonte: BDTD. Disponível em: bdtd.ibict.br, acesso em 29/05/2012.

Observa-se, no quadro 8, uma adição de seis novos temas que tiveram sua representação conceitual para a classificação da seguinte forma:

Criptografia - um conjunto de métodos e técnicas que procura estabelecer transmissão segura de informação, viabilizando diferentes características, como confidencialidade, integridade de dados, autenticação e irretratabilidade.

Gestão de risco – processo que permite aos gerentes de Tecnologia da Informação equilibrarem o funcionamento e os custos econômicos referentes às medidas de proteção, obtendo ganhos na missão de proteger sistemas e dados organizacionais (STONEBURNER at. al., 2002, p.4).

Medição de maturidade – uma das formas de medir "a extensão em que o processo é explicitamente definido, gerenciado, medido, controlado e eficaz" (SIQUEIRA, 2005, p. 4). Além do mais, a medição de maturidade deve ser efetuada ao longo do tempo, não somente quanto à qualidade do plano, mas em relação a sua evolução e aos resultados obtidos (JANSSEN, 2008, p. 54).

Normas – referencial teórico de uma regulamentação normativa sobre segurança da informação, que discute o modelo de regulamentação normativa da segurança da informação proposto em contextos organizacionais - experimentar o uso de padrões de segurança para adaptações de processos de software.

Percepção da segurança da informação – consiste em dar meios para que o controle de acesso à informação gerencie as permissões de modo mais abrangente (SAKAUE, 2008, p. 18) e descobrir os fatores mais importantes para explicar a eficácia de uma Política de Segurança da Informação através da análise dos seus usuários.

Política de segurança da informação – dispositivo por meio do qual "a instituição explicita o que será protegido e quais as restrições e descrições a que os controles devem obedecer para implementar a política" (SILVA, 2011, p. 12).

A classificação temática referente à segurança da informação, nos cinquenta e dois trabalhos de pós-graduação, coletados no site da BDTD entre 2007 e 2011, contribuiu para importantes conclusões. Os temas mais destacados entre as teses foram "Autenticação" e "Modelos Teóricos", empatados numa distribuição de dois documentos para cada segmento classificatório. No caso das dissertações, novamente "Modelos Teóricos" prevaleceu e se configurou em oito trabalhos aprovados, demonstrando sua posição de preferência na formulação de pesquisas sobre a SI. A Ciência da Informação apresentou um percentual participativo de 8,92%, em razão das cinco dissertações apuradas, dando margem para um direcionamento exclusivo na formulação de novas pesquisas. Além do mais, foi

possível identificar a Universidade de Brasília como a instituição que teve o maior número de qualificações, tanto em termos de teses quanto de dissertações. Por outro lado, a Universidade Federal da Paraíba aprovou apenas uma dissertação com o tema “Percepção da segurança da informação” na área de Informática.

Convém enfatizar que, apesar de ser um tema recorrente na mídia e uma preocupação constante nas organizações, ainda são poucas as pesquisas sobre segurança da informação. Os resultados apurados na pesquisa demonstraram que ainda há muito a se fazer para que esse tema se consolide como objeto de pesquisa e que seus resultados contribuam para a evolução das organizações.

4 PROCEDIMENTOS METODOLÓGICOS

Este capítulo tem como objetivo explanar os procedimentos metodológicos utilizados para a realização desta pesquisa, definida por Chizzotti (2008, p. 19) como “uma busca sistemática de informações para descobrir a lógica e a coerência de um conjunto de dados a fim de encontrar resposta fundamentada num problema e contribuir para o desenvolvimento em uma área”.

A metodologia científica é uma das condições necessárias para o êxito da pesquisa, ao passo que “a ciência e a metodologia caminham juntas, intrincavelmente engajadas” (MINAYO, 1996, p.23). De acordo com Minayo (op. cit., p. 22), “a metodologia inclui as concepções teóricas de abordagem, o conjunto de técnicas que possibilitam a apreensão da realidade e também o potencial criativo do pesquisador”.

4.1 CARCTERIZAÇÃO DA PESQUISA

Esta pesquisa visa fazer 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.

Em razão de os questionamentos nesse projeto envolverem a análise da viabilidade de alguns procedimentos que podem ou não resolver um problema pouco conhecido em uma organização, esta pesquisa se enquadra como um estudo exploratório. Normalmente, realizam-se estudos exploratórios quando o objetivo é

examinar um tema ou problema de pesquisa pouco estudado, do qual se tem muitas dúvidas ou não foi abordado antes (SAMPIERI, 2006, p.99).

As pesquisas exploratórias proporcionam uma visão geral acerca de determinado fato e é realizada especialmente quando o pesquisador tem alguma dificuldade de formular hipóteses precisas e operacionalizáveis sobre o tema (GIL, 1999, p.43). A autora Ciribelle (2003, p. 54) complementa os argumentos da pesquisa exploratória quando define que ela “tem por objetivo não só registrar, analisar e interpretar os fenômenos estudados, mas procura mostrar por que eles ocorrem e os fatores que os determinam”.

Os procedimentos de análise dentro da prática de pesquisa podem ser qualitativos ou quantitativos. O termo qualitativo “implica uma partilha densa com pessoas, fatos e locais que constituem objetos de pesquisa, para extrair desse convívio os significados visíveis e latentes que somente são perceptíveis a uma atenção sensível” (CHIZZOTTI, 2008, p. 28) Em contraste, a pesquisa qualitativa lida com números, utilizando modelos estatísticos a fim de explicar dados (BAUER at al., 2002, p. 23). Através do modelo qualitativo, é possível conhecer e compreender opiniões, vivências, sentimentos e expectativas, já que ele é capaz de incorporar a questão dos significados e da intencionalidade como inerentes aos atos, às relações e às estruturas sociais (MINAYO, 1998, p. 45).

A pesquisa se caracteriza como qualitativa em função dos procedimentos metodológicos introduzidos na avaliação efetuada no sistema, onde foram priorizados os riscos e identificadas as ameaças de ação imediata e melhoria. Além do mais, o estudo também teve abordagens quantitativas, devido à necessidade de parâmetros de escalas de medição para as probabilidades e os impactos usados na análise dos dados coletados.

Para que o trabalho seja bem elaborado, é fundamental estabelecer que

> tanto do ponto de vista quantitativo quanto do ponto de vista qualitativo, é necessário utilizar todo o arsenal de métodos e técnicas que ambas as abordagens desenvolveram para que fossem consideradas científicas (MINAYO, 1993, p. 247).

A pesquisa qualitativa advoga variadas estratégias de pesquisa, entre elas, destaca-se o estudo de caso. De acordo com Yin (2005, p. 20), o estudo de caso permite uma investigação para se preservarem as características holísticas e

significativas dos acontecimentos da vida real – tais como ciclos de vida individuais, processos organizacionais e administrativos, mudanças ocorridas em regiões urbanas, relações internacionais e a maturação de setores econômicos.

O método aplicado nesta pesquisa está enquadrado 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, Ibidem, p. 32). Assim, essa pesquisa se configura como um estudo de caso qualitativo e quantitativo, exploratório e descrito, em que se empregaram as técnicas e os instrumentos de coleta de dados demonstrados a seguir.

4.2 TÉCNICAS E INSTRUMENTOS DE COLETA DE DADOS

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).

A princípio, a proposta para a coleta de dados desta pesquisa utilizaria o método Delfos, que “visa obter o consenso de opiniões de especialistas sobre o que está se investigando” (VERGARA, 2008, p. 172). Na concepção de Aragão (1985, p. 58), o método contribui para obter ajuda em determinada área de incerteza, face à necessidade de uma tomada de decisão sobre eventos futuros. Caracteriza-se pela aplicação de um questionário, durante sucessivas rodadas entre os participantes. Com a identidade preservada e no decorrer de cada rodada, os envolvidos recebem um *feedback* sobre os resultados da rodada anterior, o que acarreta a modificação dos questionários posteriores através da inclusão ou supressão de questões no processo da pesquisa (VERGARA, 2008, p. 172).De acordo com Tarapanoff (1995, p. 61), a aplicação do Delfo envolve dez etapas, incluindo a elaboração de, no mínimo, três questionários.

Após a avaliação do método Delfos e os primeiros contatos com o grupo de participantes, constatou-se que não era possível aplicá-lo. Houve situações de incompatibilidade de agenda dos participantes, baixo índice de retorno do questionário inicial, tempo elevado para aplicação da segunda rodada de questões,

dificuldades de compreensão dos fundamentos teóricos da técnica pelos servidores e resultados preliminares apontados como ambíguos.

Portanto, devido às dificuldades identificadas nessa fase inicial da coleta, optou-se pela entrevista estruturada como instrumento para a coleta de dados. Trata-se de uma metodologia 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).

Em conjunto com a entrevista, a técnica de observação direta também foi empregada neste estudo, por meio de anotações em diário de campo, com o fim de explorar os aspectos positivos e negativos dos procedimentos de gestão da segurança da informação e identificar seus traços existentes na cultura organizacional, para verificar o comportamento dos técnicos em suas rotinas de trabalho, como, por exemplo, se as informações são asseguradas observando-se os requisitos de integridade, disponibilidade e confidencialidade. Para Richardson (1999, p. 259), a observação é o exame minucioso ou a mirada atenta sobre um fenômeno em seu todo ou em algumas de suas partes; é a capacitação precisa do objeto examinado.

A análise de dados coletados buscou demonstrar a situação do setor contábil e financeiro da UFPB, no que se refere aos aspectos da existência ou não de uma gestão de segurança a fim de proteger os ativos da informação do SCDP.

4.3 O CAMPO DE PESQUISA: DEPARTAMENTO CONTÁBIL DA UNIVERSIDADE FEDERAL DA PARAÍBA

A estrutura hierárquica da UFPB é regulamentada pelo Regimento Interno aprovado pela Resolução N° 257/79. O Órgão Máximo dessa Instituição é a Reitoria, com suas várias Pró-reitorias, entre elas: a Pró-reitoria Administrativa (PRA), a Pró-reitoria de Assistência e Promoção ao Estudante (PRAPE), a Pró-reitoria de Extensão e Assuntos Comunitários (PRAC), a Pró-reitoria de Graduação (PRG), a Pró-reitoria de Pós-graduação e Pesquisa (PRPG), a Pró-reitoria de Planejamento e Desenvolvimento (PROPLAN) e a Pró-reitoria de Gestão de Pessoas (PROGEP). Subordinados à Pró-reitoria Administrativa, temos os seguintes centros acadêmicos: Centro de Ciências Exatas e da Natureza (CCEN), Centro de Ciências Humanas, Letras e Artes (CCHLA), Centro de Ciências Médicas (CCM), Centro de Educação (CE), Centro de Ciências Sociais Aplicadas (CCSA), Centro de Tecnologia (CT), Centro de Tecnologia e Desenvolvimento Regional (CTDR), Centro de Ciências da Saúde (CCS), Centro de Ciências Jurídicas (CCJ), Centro de Biotecnologia (CB), Centro de Comunicação, Turismo e Artes (CCTA) e Centro de Energias Alternativas e Renováveis (CEAR).

O departamento contábil desse órgão federal é representado pela Coordenação de Contabilidade e Finanças (CCF), vinculada à PRA, por meio de cujos serviços é possível acompanhar a execução do orçamento, conhecer a composição patrimonial e analisar, interpretar e evidenciar os fatos ligados à administração orçamentária e financeira (BRASIL, 1964).

Em relação ao acompanhamento e ao controle das viagens e das diárias concedidas aos servidores da instituição, a Coordenação passou a desempenhar esse serviço em tempo real, com a implantação do SCDP. Nesse caso, o registro passou a ser executado desde o início da solicitação da diária e/ou passagem, pulverizando essa atribuição às Pró-reitorias e aos centros descritos acima. Portanto, a fim de prover mais consistência ao estudo, procurou-se abranger, na coleta de dados, não apenas a Coordenação de Contabilidade e Finanças da Pró-

reitoria Administrativa, mas também todos os outros pontos de acesso ao SCDP localizados no Campus I de João Pessoa.

4.4 DEFINIÇÃO DO UNIVERSO E DA AMOSTRA

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 é composto pelas sete Pró-reitorias e por 13 centros de ensino do Campus I da UFPB.

Quanto à amostra, que Richardson (1999, p. 158) define como “qualquer subconjunto do conjunto universal”, foi divida em dois grandes grupos: a amostragem probabilística e a não probabilística. A amostragem probabilística é rigorosamente científica e apresenta fundamentação matemática ou estatística (Silva, 2010, p. 74). Em relação à amostragem não probabilística, o critério de seleção depende unicamente do pesquisador, e seus elementos podem relacionar-se por acessibilidade, tipicidade e cotas. 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 definição da amostra partiu dos servidores que alimentam as informações do SCDP, lotados na CCF, no momento em que a técnica da pesquisa estava baseada no Delfos. Por razões já explicitadas, não foi possível aplicar a técnica Delfos, e a coleta de dados desta pesquisa mudou para entrevista estruturada. Diante disso, 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.

Para uma melhor visualização, elaboramos o demonstrativo abaixo, que expõe os usuários que acessaram o SCDP com mais frequência em 2012, alimentando-o com informações e efetuando autorizações:

Quadro 8 – Demonstrativo da amostragem

N°	Departamento	Setor/Centro	Quantidade de usuários
1	Reitoria	Secretaria	02
2	PRA	CCF	01
		DA	02
		BC	02
		CCS	02
		UAB	01
		NTI	01
		CCSA	01
		CCHLA	02
		CT	03
		CE	03
		CCJ	01
		CCM	01
		CCEN	01
		EDU	01
		PU	01
3	PRPG	DAF	01
4	PROGEP	Secretaria	01
5	PRG	Secretaria	01
6	PRAC	DA	01
7	PROPLAN	CODEOR	01
Total		**21**	**30**

Fonte: Pesquisa direta no SCDP (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.

4.5 MODELO ADOTADO COMO PARÂMETRO PARA A ANÁLISE DE RISCO

O objetivo geral desta pesquisa visa analisar o SCDP, sob a ótica da gestão da segurança da informação. Para atingir esse objetivo, é necessário efetuar uma análise de risco nos setores que utilizam o SCDP. Para tal atividade, utilizou-se como suporte metodológico o FRAAP (Processo Facilitado da Análise e Avaliação de Risco). Por causa do uso de especialistas da própria organização, esse método

permite que o processo seja conduzido, em questão de dias, com um custo-benefício baixo, o que proporciona um nível maior de aceitação por não ser estabelecido através de uma consultoria externa com procedimentos genéricos (PELTIER, 2005, p. 131). Esses fatores contribuíram para o FRAAP ser o procedimento escolhido a fim de se atingirem os objetivos desta pesquisa.

O modelo proposto para análise de risco teve em sua estrutura algumas adaptações para ser aplicado adequadamente aos setores em estudo, pois se trata de uma organização pública sem fins lucrativos, onde consideramos os clientes internos os próprios técnicos que atuam na UFPB, e os externos, os outros servidores, convidados, colaboradores eventuais e assessores especiais quando recebem as diárias e as passagens pelo SCDP. A primeira adaptação acrescentou 19 perguntas no formulário utilizado para a entrevista estruturada, pois o modelo do autor indica apenas 10 questões. As perguntas complementares foram elaboradas após consulta direta ao “Guia de Referência para Segurança da Informação Usuário Final”, fornecido pelo Ministério do Planejamento Orçamento e Gestão e, dessa forma, adequar-se ao órgão em estudo, com vistas a avaliar a segurança da informação. A outra adaptação foi um reflexo proveniente da mudança de técnica para coleta de dados, já mencionada, que reduziu os dois encontros presenciais com os técnicos especialistas a um encontro presencial individual através da aplicação da entrevista estruturada.

A estrutura da análise de risco desta pesquisa, com base no FRAAP, é 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 10, empregado como parâmetro:

Quadro 9 – 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, efetua-se uma segunda classificação (alto, médio ou baixo), de acordo com o impacto causado na instituição, com base no próximo quadro 11.

Quadro 10 – 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 2, 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.

Tabela 2 – Estrutura do FRAAP para ameaça

Ameaça	Aplicação Sim/Não	Probabilidade 1 = Baixa 2 = Média 3 = Alta	Impacto 1 = Baixo 2 = Médio 3 = Alto	Nível de Risco	Controle/ medida sugerida
Intrusão física					
Falha de energia					
Insuficiência na classificação e no tratamento da informação					
Fraqueza no uso da senha ou sua partilha					
Pessoas disfarçadas de propostos					
Preocupações de firewall					
Vírus de computador					
Estações de trabalho deixadas sem vigilância					
Falta de treinamento em servidores					
Ameaças individuais identificadas					

Fonte: Peltier (2005, p. 208, tradução nossa, com adaptações)

A coluna referente ao “Nível de risco”, que pode ser observada na tabela 2, 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 será aplicado no quadro 12 para se achar a matriz do nível de risco que cada ameaça representa para a instituição.

Quadro 11 – 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)

Encontrada a matriz do nível de risco para cada ameaça, identificam-se os controles a serem implantados na empresa. O quadro 13, seguinte, sugere alguns desses controles que podem ser usados para minimizar os riscos:

Quadro 12 – Controles sugeridos do FRAAP

N° do controle	Grupo	Descrição	Definição
1	Controle de operações	Backup	Requisitos de backup serão determinados e comunicados para os setores, incluindo envio de uma notificação eletrônica ao administrador do sistema aletando que os backups foram concluídos. Operações para testar os procedimentos de backup também são necessárias.
2	Controle de operações	Plano de recuperação	Desenvolver, documentar, testar os procedimentos de recuperação destinados a assegurar que a aplicação e a informação possam ser recuperadas, usando-se os backups criados, em caso de perda.
3	Controle de operações	Análise de risco	Realizar uma análise de risco para determinar o nível de exposição para identificar ameaças e identificar garantias possíveis de controles.
4	Controles de operação	Antivírus	(1) Certificar-se de que o administrador da área local de rede (LAN) instala o padrão corporativo de software antiviral em todos os computadores. (2) Incorporar nas políticas e normas da empresa técnicas de prevençao de vírus, bem como um programa de conscientização entre os envolvidos.
5	Controles de operação	Manutenção	Monitorar o tempo necessário do técnico na manutenção e, se necessário, elaborar um pedido de ajuste à administração.
6	Controles de operação	Acordo de nível de serviço	Adquirir e/ou manter acordos de nível de serviços com prestadores para garantir o estado operacional contínuo das aplicações.
7	Controles de operação	Mudar Gestão	Migração dos controles de produção após procura ou remoção de processos a fim de garantir proteção aos dados armazenados.
8	Controles de operação	Análise de impacto no negócio	Uma análise de impacto formal de negócios será realizada para determinar a criticidade relativa do ativo com outros ativos da empresa.

Quadro 12 – Controles sugeridos do FRAAP

N° do controle	Grupo	Descrição	Definição
9	Controles de operação	Treinamento	Formalizar e implementar um programa de conscientização atualizado e apresentar aos funcionários pelo menos uma vez por ano.
10	Controles de operação	Plano de recuperação	Implementar um mecanismo para limitar o acesso a informaççoes confidenciais, portas de rede ou locais físicos.
11	Controles de operação	Análise de risco	Implementar mecanismos de autenticação de usuário (como firewalls, senhas de acesso) para limitar permissões de acesso.
12	Aplicação de controles	Aplicação de controles	Projetar e implementar aplicativos de controle (editar veirificação de entrada de dados, campos requerendo validação, indicadores de alarme, capacidades de expiração de senha, checksums) para garantir confidencialidade, integridade e disponibilidade de aplicação de informação.
13	Aplicação de controles	Aplicação de controles	Desenvolver procedimentos de teste para serem seguidos durante o desenvolvimento das aplicações e durante as modificações necessárias, incluindo utilizadores de participação e aceitação.
14	Aplicação de controles	Aplicação de controles	Implementar programas de usuários (avaliação de desempenho) destinados a incentivar a conformidade com as políticas e procedimentos para garantir a utilização adequada das aplicações.
15	Aplicação de controles	Treinamento	Os desenvolvedores de aplicativos devem fornecer apoio e documento de orientação à equipe de operações relativo à execução dos mecanismos para assegurar que a transferência de informações entre as aplicações sejam seguras.
16	Aplicação de controles	Estratégias de correção	A equipe de desenvolvimento deve desenvolver estratégias de correção tais como processos reformulados, lógica de aplicação, processos de revista e outros.
17	Controles de segurança	Política	Desenvolver políticas e procedimentos para limitar o acesso de operações, concedendo privilégios aos que realmente precisam para o negócio.
18	Controles de segurança	Treinamento	Treinamento do usuário irá incluir documentação sobre o uso correto das aplicações. Será destacada a importância de manter o sigilo das contas de usuário, senhas e informação competitiva.

Quadro 12 – Controles sugeridos do FRAAP

N° do controle	Grupo	Descrição	Definição
19	Controles de segurança	Inspeção	Incluir mecanismos de monitoração, relatórios e identificar atividades necessárias para avaliação por auditoria independente, incluindo revisões periódicas de IDs de usuário para que executem suas tarefas realmente necessárias ao negócio da instituição.
20	Controles de segurança	Classificação de ativos	Revisão na classificação de ativos de acordo com políticas, normas e procedimentos da empresa.
21	Controles de segurança	Controle de acesso	Mecanismos para proteger o banco de dados de acessos não autorizados e modificações feitas de conexões externas.
22	Controles de segurança	Apoio da gestão	Pedir apoio à gestão para assegurar a cooperação e coordenação por todos na empresa.
23	Controles de segurança	Licenças	Manter atualizados os acordos de licença com terceiros e guardá-los em local seguro.
24	Controles de segurança	Mecanismo de diagnóstico	Implementar mecanismo de controle para evitar acesso não autorizado à informação. Esse mecanismo deverá ter a capacidade de detectar, registrar e relatar tentativas de violação à segurança da informação.
25	Controles de segurança	Controle de acesso	Implementar mecanismo de criptografia (de dados, de entrada e saída) para impedir o acesso não autorizado protegendo a integridade e a confidencialidade das informações.
26	Controles de segurança	Controle de acesso	Aderir a uma gestão destinada a mudanças de processos para facilitar uma estrutura na empresa de modificação e assegurar que as precações sejam seguidas. Modificações de emergência devem ser incluídas nesse processo.
27	Controles de segurança	Controle de acesso	Consultar o Núcleo de tecnologia para facilitar a implementação física dos controles de segurança projetados para proteger informação, software, hardware e sistemas.
28	Controles de segurança	Segurança física	Realizar uma análise de risco para determinar o nível de exposição às ameaças identificadas e encontrar os controles possíveis.

Fonte: Peltier (2005, p. 176, tradução nossa e adaptações)

5 COLETA E ANÁLISE DOS DADOS

Neste capítulo, descreve-se como ocorreram os procedimentos de coleta e a análise dos dados de informações oriundas dos processos e das atividades propostas para a realização desta pesquisa. Está estruturado de forma a apresentar os resultados obtidos, relacionando-os aos objetivos específicos dessa dissertação.

A coleta de dados começou pelas 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, instrumento primário desta pesquisa, 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 não ter atingido sua totalidade, entre eles, a falta de tempo dos escolhidos para o diálogo e o período do ano costumeiro das férias, que provocou a ausência de servidores na instituição.

Essas entrevistas foram realizadas de forma estruturada, conforme apêndice A, visando registrar as observações dos entrevistados com método de gravação e salientando, antecipadamente, a questão do anonimato da pesquisa para não intimidar os atores sociais.

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.

Já com respeito à análise da coleta, optou-se por fazer alguns ajustes no processo de quantificação das repostas, tornando-as dicotômicas. Esses ajustes basearam-se em considerar 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. O próximo quadro demonstra esse tratamento adotado com as alternativas de respostas, cujos dados foram aplicados para a obtenção de informações sobre os níveis de risco no FRAAP.

Quadro 13 – Tratamento dos dados coletados

	Nº	PERGUNTAS	Resposta		Resultado		Percentual	
			Detalhada	Agrupada	Det.	Agr.	Det.	Agr.
IDENTIFICAÇÃO	1	Sexo	Masculino			13		65%
			Feminino			7		35%
	2	Qual seu cargo na organização?	Resposta aberta					
	3	Sua função no SCDP exige conceder autorização?	Sim			8		40%
			Não			12		60%
MÓDULO I -PROCESSOS	4	Em sua opinião, qual a importância do SCDP para a organização onde você trabalha?	Muito importante	Sim	16	19	80%	95%
			Importante		3		15%	
			Com alguma importância		0		0%	
			Pouquíssima importância	Não	1	1	5%	5%
			Sem importância		0		0%	
	5	Você classifica as informações do SCDP como confidenciais?	Sim			13		65%
			Não			7		35%
	6	O SCDP atende às necessidades da organização?	Sim			16		80%
			Não	Não	1	4	5%	20%
			Às vezes		3		15%	
	7	Faz uso de outros programas a fim de controlar as informações que são processadas no SCDP?	Sim			13		65%
			Não	Não	7	7	35%	35%
			Às vezes		0		0%	
	8	É necessário armazenar a documentação de forma impressa?	Sim	Sim	17	20	85%	100%
			Às vezes		3		15%	
			Não			0		0%

Quadro 13 – Tratamento dos dados coletados

	Nº	PERGUNTAS	Respostas		Resultado		Percentual	
			Detalhada	Agrupada	Det.	Agr.	Det.	Agr.
MÓDULO I - PROCESSOS	9	As informações físicas podem ser recuperadas em lixeiras ou em outros depósitos?	Sempre	Sim	2	9	10%	45%
			Às vezes		4		20%	
			Raramente		3		15%	
			Nunca	Não		11		55%
	10	Documentações para diferentes interessados são enviadas num único envelope?	Sempre	Sim	1	6	5%	30%
			Às vezes		3		15%	
			Raramente		2		10%	
			Nunca/Não			14		70%
	11	Recebeu orientação sobre a manutenção sigilosa de sua senha de acesso e a responsabilidade envolvida pelo mau uso dela?	Sim			13		65%
			Não	Não	6	7	30%	35%
			Não lembro		1		5%	
	12	Em algumas situações, as informações enviadas a terceiros podem ser mal utilizadas?	Sempre	Sim	2	9	10%	45%
			Às vezes		4		20%	
			Raramente		3		15%	
			Nunca	Não		11		55%
	13	As solicitações para novas identificações de usuários e alteração de privilégios são feitas por escrito e aprovadas pela chefia imediata do usuário?	Sempre			17		85%
			Às vezes	Não	1	3	5%	15%
			Raramente		0		0%	
			Nunca		2		10%	
	14	Todos os usuários que desejam usar o SCDP assinam o Termo de Responsabilização e Sigilo pelo qual concordam com as políticas, os padrões, as normas e os procedimentos do Órgão Público relacionados ao ambiente de TI?	Sempre	Sim		9		45%
			Às vezes	Não	0	11	0%	55%
			Raramente		1		5%	
			Nunca		10		50%	
	15	O Centro exige autorização no acesso ao setor por pessoas que não sejam servidoras da instituição?	Sempre	Sim	3	7	15%	35%
			Às vezes		4		20%	
			Raramente	Não	1	13	5%	65%
			Nunca		12		60%	
	16	O centro utiliza-se de identificação pessoal com o uso de crachás nos servidores?	Sempre	Sim		1		5%
			Às vezes	Não	0	19	0%	95%
			Raramente		3		15%	
			Nunca		16		80%	
	17	Os papéis de trabalho geralmente são deixados à vista na mesa de trabalho?	Sempre	Sim	9	17	45%	85%
			Às vezes		8		40%	
			Raramente		0		0%	
			Nunca	Não		3		15%

Quadro 13 – Tratamento dos dados coletados

	Nº	PERGUNTAS	Resposta		Resultado		Percentual	
			Detalhada	Agrupada	Det.	Agr.	Det.	Agr.
MÓDULO I - PROCESSOS	18	O Centro exige autorização no acesso ao setor por pessoas que não sejam servidoras da instituição?	Sempre	Sim	3	7	15%	35%
			Às vezes		4		20%	
			Raramente	Não	1	13	5%	65%
			Nunca		12		60%	
	19	O Centro utiliza-se de identificação pessoal com o uso de crachás nos servidores?	Sempre	Sim		1		5%
			Às vezes	Não	0	19	0%	95%
			Raramente		3		15%	
			Nunca		16		80%	
	17	Os papéis de trabalho geralmente são deixados à vista na mesa de trabalho?	Sempre	Sim	9	17	45%	85%
			Às vezes		8		40%	
			Raramente		0		0%	
			Nunca	Não		3		15%
	18	É costume, no ambiente de trabalho, deixar o computador ligado com as janelas abertas?	Sempre	Sim	0	3	0%	15%
			Às vezes		1		5%	
			Raramente		2		10%	
			Nunca			17		85%
MÓDULO II - PESSOAS	19	A alta administração está ciente de que as instituições precisam de um programa eficaz de segurança da informação?	Sim	Sim		10		50%
			Não	Não	7	10	35%	50%
			Não tenho conhecimento		3		15%	
			Não lembro		0		0%	
	20	Os gestores do Centro incentivam uma política de segurança da informação?	Sim	Sim		15		75%
			Não	Não	3	5	15%	25%
			Não lembro		2		10%	
	21	Em sua opinião, classifique a importância de haver na instituição uma ação efetiva dos usuários do SCDP sobre a Política de Segurança da Informação?	Muito importante	Sim	17	19	85%	95%
			Importante		1		5%	
			Com alguma importância		1		5%	
			Pouquíssima importância	Não	0	1	0%	5%
			Sem importância		1		5%	
	22	Você guarda em local seguro o dispositivo móvel (token) que dá acesso ao SCDP?	Sempre	Sim	7	7	35%	35%
			Às vezes		0		0%	
			Raramente	Não	1	1	5%	5%
			Nunca		0		0%	
			Não se aplica			12		60%
	23	Você permite que terceiros saibam sua senha de acesso?	Sempre	Sim	0	3	0%	15%
			Às vezes		3		15%	
			Raramente		0		0%	
			Nunca	Não		17		85%
	24	Procura discutir assuntos de trabalho em ambientes que não sejam da instituição?	Sempre	Sim	2	7	10%	35%
			Às vezes		2		10%	
			Raramente		3		15%	
			Nunca	Não		13		65%

Quadro 13 – Tratamento dos dados coletados

	Nº	PERGUNTAS	Resposta		Resultado		Percentual	
			Detalhada	Agrupada	Det.	Agr.	Det.	Agr.
MÓDULO III - TECNOLOGIA	25	Armazena ou usa programas que não sejam destinados ao objetivo de sua função na instituição?	Sempre	Sim	2	7	10%	35%
			Às vezes		5		25%	
			Raramente		0		0%	
			Nunca	Não	13		65%	
	26	Qual a frequência de atualização do seu antivírus?	Todos os dias	Sim	7	15	35%	75%
			Duas ou mais vezes p/sem.		4		20%	
			Uma vez por mês		1		5%	
			Uma vez por semana		3		15%	
			Não atualizo	Não	5		25%	
	27	O antivírus tem algum custo financeiro?	Sim	Sim	0		0%	
			Não	Não	15	20		100%
			Não, mas já teve		0			
			Nunca		5			
	28	Certifica-se de que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação?	Sempre	Sim	14		70%	
			Às vezes	Não	3	6	15%	30%
			Raramente		2		10%	
			Nunca		1		5%	
	29	Os equipamentos do setor são suficientes para executar seu trabalho no SCDP?	Sim	Sim	12		60%	
			Às vezes sinto dificuldade	Não	6	8	30%	40%
			Não		2		10%	

Fonte: Elaborado pelo autor em pesquisa direta (2013)

Pode-se examinar, no quadro 15, que a coluna referente ao item “Resposta” divide-se em duas. A primeira descreve as alternativas das questões do formulário, e a segunda agrupa essas alternativas conforme o tratamento adotado, já mencionado, para se obterem respostas dicotômicas. As outras colunas seguintes têm a mesma estrutura, mas se diferenciam em relação ao conteúdo dos dados, ou seja, uma representa o total dos resultados das respostas, e a outra, os percentuais calculados que servirão de base para a análise de risco.

As três primeiras perguntas do questionário contribuíram para levantar o perfil dos vinte usuários do SCDP entrevistados quanto ao gênero, ao cargo ocupado na instituição e à função de autorização no sistema.

Através das questões 4, 5 e 6, iniciou-se o módulo “Processos” coletando informações sobre a visão dos usuários em relação ao SCDP. Salienta-se que será dada mais atenção à segurança da informação quando o sistema apresentar elevada importância para os envolvidos. Portanto, um subtópico posterior dará mais detalhes sobre esse assunto.

A sétima questão procura identificar se são necessários outros programas para executar as atividades relacionadas à concessão de diárias e de passagens. A pesquisa apontou que 65% dos entrevistados responderam positivamente sobre essa característica. Portanto, no desenvolvimento de uma política de segurança da informação, é imprescindível enfatizar o uso de programas de computador licenciados, de acordo com as disposições previstas em contrato, e que a instalação deles seja atribuição da administração de sistemas e TI.

As alternativas de números 8, 9 e 10, do quadro 15, investigaram a necessidade do uso de documentação impressa nas atividades do sistema, bem como sua recuperação indevida em lixeiras e visualização não autorizada. Nesse ponto, 100% afirmaram que usam documentos impressos. No entanto, 55% negam que esses materiais sejam recuperados após seu descarte, e 70% são contrários à possibilidade de haver uma vista nesses impressos por terceiros. Esses índices não resultaram em um nível de risco elevado, conforme demonstrado na análise. Por outro lado, os 45% que responderam que é possível recuperar documentos descartados, e os 30% que afirmaram o envio desses junto com outros num único envelope sinalizam a possibilidade de que terceiros utilizem indevidamente as informações.

Quanto à questão 11 - sobre se é necessária uma PSI no órgão em estudo - os resultados demonstraram que 65% dos envolvidos afirmaram ter recebido orientação sobre a manutenção sigilosa de sua senha de acesso e da responsabilidade envolvida pelo mau uso dela.

Através da questão 12, o estudo procurou diagnosticar alguma utilização indevida das informações do SCDP que são fornecidas verbalmente a terceiros, seja por telefone ou contato direto. Nove dos respondentes (45%) afirmaram ser possível isso acontecer, ao passo que não existe certificação de identidade no fornecimento dos dados às pessoas que não sejam usuárias ou beneficiárias do sistema informacional.

As perguntas 13 e 14 observaram a utilização de documentação escrita para permitir que novos usuários tenham acesso ao sistema, tanto no uso da senha quanto na responsabilização de suas ações. A pesquisa aponta que apenas 15% afirmaram que não há esse tipo de documentação para o uso da senha de acesso, e 55% responderam não ter assinado o Termo de Responsabilização e Sigilo, antes de começar suas atividades no SCDP. Portanto, é preciso mais atenção nesse aspecto para que haja um alto índice de utilização do Termo de Responsabilização e Sigilo na organização.

Com respeito às questões 15 e 16, a pesquisa investigou a possibilidade de haver acesso não autorizado nos locais onde tramitam as informações do sistema. Em relação ao procedimento que identifica as pessoas na entrada desses locais, os entrevistados referiram que, em 65% dos ambientes visitados, isso não acontece. Inclusive, durante as visitas, em alguns locais para a recepção de pessoas, seu objetivo não era cumprido plenamente, pois se permitia que qualquer indivíduo penetrasse no ambiente informacional. Ainda dentro desse tópico, um fator preocupante foi o percentual de 95% relativos à não identificação pessoal pelos servidores da instituição. Esse tema será discutido, posteriormente, quando forem sugeridos os controles após a análise de risco.

Outro fator preocupante foi o resultado da pergunta 17, em que se confere o costume de deixar papéis de trabalho sobre a mesa. Entre os envolvidos, 85% afirmaram ter esse hábito na realização das tarefas relativas ao SCDP. Além do mais, observou-se que, em alguns setores, vários processos para a liberação das diárias e das passagens contendo informações pessoais e financeiras ficavam durante longo período sobre a mesa ou visíveis em cima de um armário próximo ao usuário. Por outro lado, a questão de número 18 representou um aspecto positivo na SI, pois, com o mesmo percentual da anterior, informou que os usuários do sistema procuram não deixar aberta a janela do computador quando o usam.

O comprometimento da alta administração, dos gestores e dos envolvidos na pesquisa com uma política de segurança da informação foi analisado na aplicação nos itens 19, 20 e 21 do questionário. Os dados revelaram que os gestores participam mais nesse aspecto em relação à alta administração, uma vez que seu percentual positivo foi de 75% em relação ao percentual de 50% do grupo de hierarquia superior. Acredita-se que o contato mais direto dos gestores com os servidores usuários do SCDP tornou mais fácil essa percepção e contribuiu para

esse resultado. Entretanto, nada superou o interesse dos próprios pesquisados quanto ao assunto da segurança da informação, ao passo que 95% deles consideram importante o tema em estudo.

A fim de acessar o sistema, os usuários com perfil de autorização necessitam de um dispositivo móvel de segurança para, junto com a senha, poderem começar suas atividades nele. O item 22 questionou se há guarda segura desse equipamento. Todavia, como 12 participantes (60%) não o possuem, devido à própria estrutura do sistema, os 35% restantes que responderam “sim” compreenderam 87,5% de usuários que apresentaram aplicar satisfatoriamente as medidas de segurança. Ou melhor, dos oito usuários que possuem o dispositivo, um deles não o guarda de forma segura. Quanto ao uso da senha, a pergunta 23 questionou a existência de sua partilha, e os dados apurados demonstraram que três usuários tendem a compartilhar o seu código pessoal de acesso.

A vigésima quarta alternativa do questionário procurou captar os assuntos discutidos fora do ambiente de trabalho e que podem dar margem à divulgação indevida de informações. Nesse aspecto, a possibilidade de executar as ações do SCDP, em qualquer computador pessoal, desde que o aparelho contenha as chaves de segurança instaladas, contribuiu para que 35% dos entrevistados admitissem essa possibilidade.

Quanto à questão de número 25, o estudo procurou avaliar a frequência do uso de programas que não estejam relacionados ao objetivo do servidor no órgão. A maioria dos respondentes negou, e 35% admitiram que baixam e instalam programas no computador, colocando a instituição pesquisada em risco, uma vez que tais softwares podem conter vírus e outros programas maliciosos capazes de comprometer o ambiente de TI.

Ainda no módulo relativo à tecnologia, a abordagem feita aos servidores avaliou a frequência de uso do programa antivírus, bem como o tipo utilizado nas estações de trabalho, através das perguntas 26 e 27. Quanto a isso, 75% atualizam suas ferramentas de segurança, embora 100% dos programas da instituição com esse objetivo tenham nenhum custo financeiro. Infere-se, pois, que não é recomendável o uso de antivírus gratuitos nos setores da UFPB, pois eles têm eventuais limitações e não existe suporte técnico para algum problema que aconteça ou alguma dúvida.

Quando perguntados sobre se o usuário se certifica de que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, 70% dos participantes afirmaram ter tal atitude ao navegar na rede mundial de computadores. Por outro lado, os usuários que não atentam para esse procedimento correm o risco de sofrer um ataque de *phishing,* um processo fraudulento empregado para se adquirirem informações confidenciais através da simulação de sites confiáveis (MARTINO, 2010, p 163).

A última questão, de número 29, avaliou a suficiência dos equipamentos usados nas ações do SCDP, pois alguma deficiência nesse aspecto contribui para uma estação de trabalho ficar sem vigilância. Apurou-se que 60% dos usuários estão satisfeitos com os instrumentos do setor, e para os insatisfeitos, a falta de um aparelho profissional para escaneamento de documentos foi o motivo principal.

De acordo com a próxima tabela 3, os dados obtidos pelas entrevistas foram numerados em códigos para facilitar a localização e a compreensão de algumas frases alinhadas com as referências de significado que emergiram dessas entrevistas.

Tabela 3 – Codificação das entrevistas

Código	**Setor**	**Função**	**Data da entrevista**	**Tempo de gravação**
Participante 1	Pró-reitoria de Pós-graduação / Departamento Contábil e Financeiro	Coordenador contábil e financeiro	23/01/13	00:18:04
Participante 2	Pró-reitoria de Administração / Coordenação de Administração	Auxiliar de Administração	05/02/13	00:24:01
Participante 3	Pró-reitoria de Administração / Divisão Administrativa e Financeira	Assistente de Administração	05/02/13	00:13:14
Participante 4	Pró-reitoria de Planejamento / Coordenação de Orçamento	Contador	05/02/13	00:20:20
Participante 5	Pró-reitoria de Administração / Coordenação de Administração	Assistente de Administração	06/02/13	00:15:40

Tabela 3 – Codificação das entrevistas

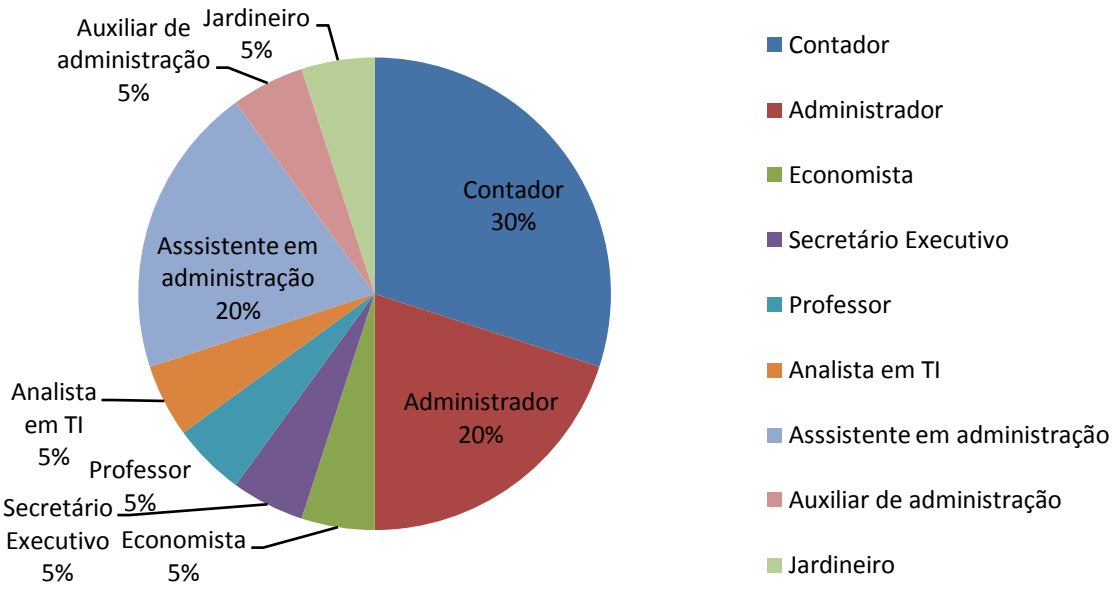
Código	Setor	Função	Data da entrevista	Tempo de gravação
Participante 6	Pró-reitoria de Administração / Biblioteca Central	Diretor Administrativo	06/02/13	00:39:36
Participante 7	Pró-reitoria de Administração / Biblioteca Central	Secretária	06/02/13	00:33:55
Participante 8	PRA/Escola Técnica de Saúde	Administrador	06/02/13	00:23:31
Participante 9	PRA/Centro de Tecnologia	Assistente de Administração	06/02/13	00:11:57
Participante 10	PRA/Centro de Educação	Contador	07/02/13	00:32:32
Participante 11	PRA/Centro de Ciências Jurídicas	Assistente de Administração	07/02/13	00:19:36
Participante 12	PRA/Centro de Ciências Humanas, Letras e Artes	Administrador	08/02/13	00:42:47
Participante 13	PRA/Centro de Ciências Humanas, Letras e Artes	Contador	08/02/13	00:09:55
Participante 14	PRA/Prefeitura Universitária	Diretor de Contabilidade	08/02/13	00:10:49
Participante 15	PRA/Centro de Ciências Sociais e Aplicadas	Gestor financeiro	14/02/13	00:29:02
Participante 16	PROGEP/Secretaria	Secretária executiva	14/02/13	00:19:49
Participante 17	PRA/Centro de Ciências Exatas e da Natureza	Contador	15/02/13	00:21:01
Participante 18	PRA/Centro de Ciências da Saúde	Diretor de Centro	15/02/13	00:26:22
Participante 19	Pró-reitoria de Assuntos Comunitários / Divisão Administrativa	Administrador	15/02/13	00:14:43
Participante 20	PRA/Núcleo de Tecnologia da Informação	Analista de Tecnologia da Informação	18/02/13	00:28:08

Fonte: Elaborado pelo autor, adaptado de fonte primária (2013)

5.2 PERFIL DOS USUÁRIOS DO SCDP

Conforme já salientado, as questões iniciais do formulário contribuíram para diagnosticar o perfil dos usuários do SCDP. Em primeiro lugar, apurou-se que 65% deles são do sexo masculino, e os sete restantes, do feminino. Quanto à formação acadêmica, 16 dezesseis técnicos têm graduação, e quatro, nível médio. Em relação aos cargos que desempenham, a pesquisa apontou: seis contadores, quatro administradores, um economista, um secretário executivo, um professor, um analista de Tecnologia da Informação, quatro assistentes de Administração, um auxiliar de Administração e um jardineiro. O gráfico 2 ilustra esses resultado:

Gráfico 2 – Perfil dos entrevistados por cargo

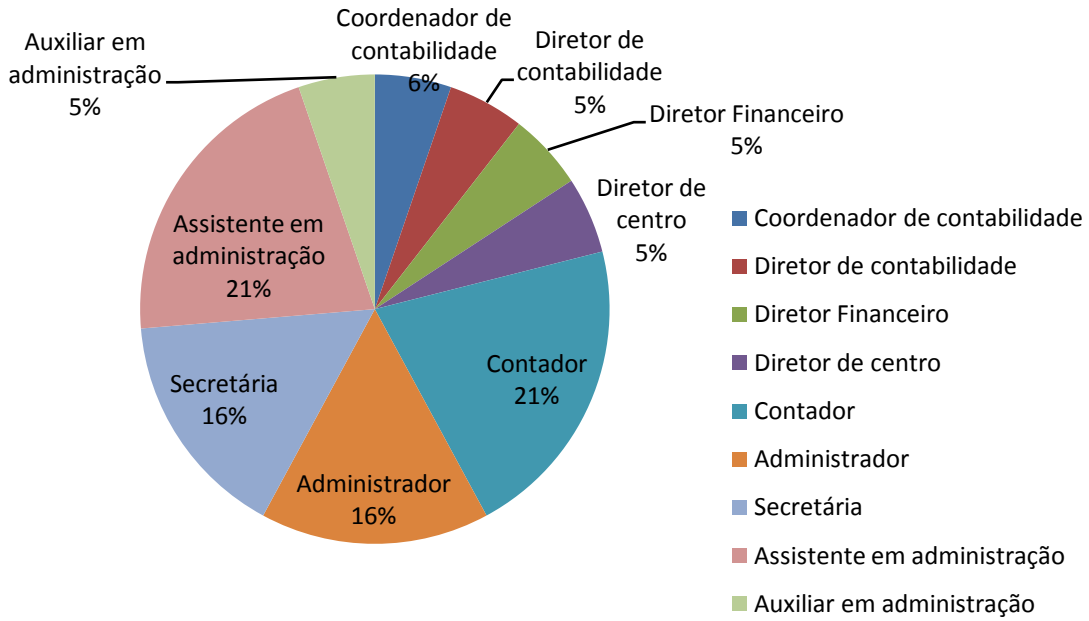


Fonte: Elaboração própria (2013)

Em relação aos servidores demonstrados no gráfico 2, dois contadores desempenham funções de chefia, um, como coordenador contábil e financeiro, e o outro, como diretor de Contabilidade. O economista executa seu trabalho como diretor financeiro, e o bibliotecário assume a direção administrativa do seu setor. Portanto, considerando as funções dos envolvidos na pesquisa, temos: um coordenador contábil e financeiro, um diretor de Contabilidade, um diretor financeiro, um diretor de centro, quatro contadores, três administradores, três secretárias,

quatro assistentes de Administração e um auxiliar de Administração. O gráfico 3 demonstra melhor essa estrutura de funções:

Gráfico 3 – Perfil dos entrevistados por funções



Fonte: Elaboração própria (2013)

Nessa estrutura de cargos e funções dos entrevistados, constataram-se diferentes áreas de atuação que saem do âmbito da Contabilidade. Isso é reflexo da dimensão que o SCDP atinge no órgão estudado, caracterizada desde sua implantação em 2008. Portanto, o controle e o registro dos atos e dos fatos administrativos de uma entidade, cujas funções são típicas do setor contábil, passaram a ser incluídas nas rotinas de servidores de outras áreas, como Economia e Secretariado. Infere-se nisso a importância de haver uma conscientização quanto ao alto nível de responsabilidade das ações executadas no sistema, pois erros de expediente serão refletidos, posteriormente, nos demonstrativos contábeis.

Na sequência da estrutura do método para a coleta de dados, questionou-se sobre quem tinha perfil de autorização no SCDP, pois qualquer servidor ativo pode ser usuário do sistema, desde que sua função envolva atividades relativas à concessão de diárias ou passagens. Portanto, se houver necessidade de usar o Certificado digital em suas atribuições, será enviada uma comunicação formal à

Autoridade Certificadora, que providenciará a chave privada, tornando-se apto a aprovar ações no sistema.

De acordo com o Manual de Implantação do SCDP (2007, p. 13), os perfis e as atribuições que foram alvo desta pesquisa compreenderam:

Solicitante – cadastra uma Proposta de Concessão de Diárias e Passagens (PCDP) no sistema; inclui roteiro da viagem; anexa documentação como: e-mail, justificativas para o deslocamento ou viagem; efetua correções solicitadas referentes a data, roteiro, justificativas e outros; efetua prorrogações ou redução de viagem; altera ou exclui uma PCDP; altera trechos; cancela viagem e formaliza prestação de contas anexando documentos como: relatórios de viagem, bilhetes de passagem, comprovantes de gastos para reembolso, comprovante de depósitos correspondentes à devolução de valores e outros.

Representante administrativo – verifica pesquisa de preço de passagens; mantém contato com agência de viagem; define a reserva de passagens de acordo com a política de menor preço e cancela bilhete.

Proponente – analisa os dados e os documentos anexados; aprova administrativamente a viagem, devolve para corrigir ou não aprova (cancela) e aprova prestação de contas.

Ordenador de Despesas – verifica a PCDP e analisa os dados da viagem; altera projeto atividade ou empenho, se necessário; aprova a viagem, devolve para corrigir ou cancela.

Autoridade Superior – verifica a PCDP de viagem com programação inferior a 10 dias, bem como os documentos anexados; aprova, devolve para corrigir ou cancela a viagem.

Coordenador orçamentário – atualiza a tabela “Cadastra Teto Orçamentário” e controla os limites do orçamento.

Coordenador de Contabilidade e Finanças – efetua empenhos no SIAFI; efetua autorização de viagem (AV) e a ordem de pagamento (OB) no SIAFI; cancela a execução financeira (AV e OB) no SCDP.

Gestor setorial – representa o Órgão no MP; providencia apresentações do sistema e reuniões com o representante do MP; elabora ofício do Dirigente do Órgão solicitando a disponibilização do SCDP; atualiza tabelas com dados setoriais; mantém as unidades internas informadas dos passos para implantação, inclusive da certificação digital; coordena os intervenientes do SCDP no órgão e esclarece

dúvidas sobre o processamento do sistema; comunica ao MP qualquer problema relativo ao sistema sem solução no âmbito do órgão.

Os outros agentes do processo de concessão de diárias e de passagens são:

Proposto – pessoa que viaja e presta contas da viagem realizada ou cancelada no prazo legal. Nesse caso, é necessário entregar o relatório de viagem, bilhetes/canhotos de embarque e devolver valores recebidos ou bilhetes não utilizados.

Agência de Viagem – pessoa jurídica ganhadora da licitação que fornece dados e valores de passagens dos roteiros para o representante administrativo; reserva e emite bilhetes de passagem; devolve a PCDP para correções, como voo sem lugar disponível, alteração de valores e outros; fatura os bilhetes emitidos e reembolsa os bilhetes não utilizados.

Através do detalhamento de perfis e atribuições apurados, podem-se identificar os usuários responsáveis por conceder autorizações no SCDP. O grupo é formado pela autoridade superior, o ordenador de despesa, o proponente, o coordenador de contabilidade e finanças, o coordenador orçamentário e o gestor setorial. Eles precisam avaliar e analisar os documentos anexados nas solicitações de diárias e passagens, pois suas ações garantem a integridade e a autenticidade das informações do sistema.

No âmbito da UFPB, o Reitor é a autoridade superior, o Pró-reitor de Administração representa o ordenador de despesa, e o coordenador de Administração é o proponente da PRA. Já em relação aos coordenadores de contabilidade e de orçamento, as funções apresentam a mesma nomenclatura atribuída ao sistema. Quanto ao gestor setorial, é um assistente administrativo lotado na Coordenação de Administração. Convém salientar que há um preponente em cada centro acadêmico do campus, e todos são representados pela função de diretor administrativo ou de Centro.

5.3 O SISTEMA NA VISÃO DOS USUÁRIOS

O Sistema de Concessão de Diárias e Passagens tem na sua administração geral a Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão (MPOG), em parceria com o Gestor Setorial de cada Órgão do governo federal. Dele são extraídos dados relativos às diárias de servidores para o Portal da Transparência e informações que subsidiam o Relatório de Gestão do Processo de Tomada de Prestação de Contas, exigido pela Controladoria Geral da União.

Para implantar o sistema na UFPB, a Reitoria emitiu um ofício de solicitação ao Ministério do Planejamento, indicando o gestor setorial que ficou encarregado dos procedimentos preliminares. As ações prévias envolveram: 1) uma reunião de implantação entre o MP e os servidores da universidade compostos por representantes das áreas administrativa, orçamentária, financeira, de recursos humanos, informática e o responsável pela reserva de passagem e prestação de contas de viagem; 2) treinamento do gestor setorial pelo MP; 3) comunicação formal da instituição às outras unidades administrativas sobre a implantação do SCDP e sobre o processo de certificação digital e 4) elaboração da listagem dos usuários, com respectivos perfis, para processo de certificação digital.

Mediante dados levantados na entrevista, o SCDP representou para os participantes elevada contribuição para a instituição. As questões iniciais do módulo “Processos” permitiram-se levantar informações sobre a importância do sistema na instituição, bem como seu grau de sigilo e melhoria para as atividades de concessão de diárias e passagens. É o caso dos 80% dos entrevistados que responderam como “Muito importante”, 15%, como “Importante”, e apenas 5% consideraram de “Pouquíssima importância” o SCDP para a UFPB.

Em relação ao grau de sigilo das informações do sistema, 65% disseram “Sim” quando questionados sobre a confidencialidade das informações, e o restante, ou seja, os 35%, responderam de forma negativa.

Em relação aos participantes que não consideraram como confidenciais as informações, perceberam-se dúvidas quanto à classificação das informações, e outros se justificaram utilizando como parâmetro a Lei 12.527, de 18 de novembro

de 2011, que estabelece a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação.

> Não são tão confidenciais não [...] não é nem confidencial, é pessoal [...] tem a lei da transparência e eu não vejo nenhum motivo para não ser público, quando entra na área de valor, conta de A, B e C, dados desse tipo, tudo bem, mas no geral, não vejo porque (Participantes 1, 3, 6, 2013).

A lei referente à gestão da transparência da informação também estabelece, no sexto artigo, que se deve assegurar a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade. O decreto nº 4.553/2002 classifica como confidenciais os dados de conhecimento restrito que, se usados de forma indevida, podem causar danos à sociedade. É o caso do SCDP por onde tramitam históricos pessoais, informações de contato e identificadores oficiais como o Cadastro de Pessoa Física e a cédula de identidade. Nesse aspecto, infere-se haver preocupação em proteger os dados do sistema, procurando identificar as pessoas que desejam receber informações dele. Além do mais, as informações necessárias para a sociedade referentes às diárias e às passagens do governo são evidenciadas automaticamente no site www.portaltransparencia.gov.br.

Quanto ao atendimento das necessidades do órgão pelo sistema de informação, 80% declararam sua posição positiva, enquanto 15% ficaram com “Às vezes”, e 5% atribuíram “Não” como resposta. Nesse aspecto, a abordagem apresentou um resultado satisfatório para a utilização do SCDP no processamento das atividades da UFPB. Porém, em relação aos percentuais contraditórios do argumento, a pesquisa indicou os seguintes motivos: desatualização do saldo orçamentário remanescente após realização da viagem, liberação dos recursos de diárias e passagens por um único setor e continuação do uso de documentos impressos no sistema apesar da tramitação eletrônica que ele favorece.

> O sistema é muito bom, mas tem um defeito. A gente não consegue ver o saldo do empenho atualizado quando quer fazer um pedido de diárias [...] tem que ligar pra PRA pra saber [...] imagina o fluxo de trabalho que ele já tem por ser reitor e ta homologando, autorizando ou não autorizando [...] um processo que antes demandava uma semana, passou mais de um mês, ou seja, esse servidor viajava com seus recursos para receber a posterior os valores e isso atrapalha [...] ele (sistema) pede para que não guarde, ou seja, você pega uma passagem, por exemplo, uma prestação de contas, escanea e joga

> no sistema, a solicitação do SCDP por via e-mail, você escanea e joga no sistema, mas, as pessoas ainda conseguem aderir ao papel de uma forma muito coesa, não tem jeito [...] (Participantes 1, 6, 10, 2013).

Salienta-se que a concentração na Reitoria para a liberação das diárias e das passagens procedeu, depois do Decreto Nº 7.689, de 22 de março de 2012, que estabeleceu limites e instancias de governança para os gastos com essas despesas. Quanto ao uso da documentação escrita, não impede o andamento das concessões, pois as autorizações são efetuadas mediante os documentos anexados e certificados digitalmente.

Observou-se também, nas entrevistas, que o SCDP trouxe um mecanismo confiável de controle, possibilitando evitar gastos desnecessários e contribuindo para a transparência das ações do governo.

> Não só a questão de diárias e passagens, qualquer ato que envolva recurso financeiro tem que haver um máximo de controle possível para evitar erros ou até desvios [...]É uma ferramenta muito interessante, e outra coisa, você tem um histórico de passo a passo. Eu devolvi, mas porque você devolveu? Ta lá. Devolvi por incorreção dos dados, devolvi porque não está de acordo e as pessoas que estão lá no processo conseguem visualizar isso, o andamento do processo, e isso é importante. Ele tem o fluxograma em que você visualiza e onde fica verde é onde ele está parado e limita para você até onde você pode alterar, se não, tem que esperar o passo seguinte. Eu gosto de trabalhar no SCDP [...] (Entrevistados 4, 12, 2013).

Outra característica observada na pesquisa teve contribuição do gestor da entrevista 14, quando se referiu ao arquivamento digital do sistema durante cinco anos.

> [...] o sistema ele é cumulativo, então você pode entrar, eu acho, se não me engano, cinco últimos anos, você tem tudo guardado no próprio sistema [...] (Participante 16, 2013).

Conhecer a visão dos servidores em relação ao SCDP é requisito necessário quando se deseja avaliar a segurança de sua informação. Permite diagnosticar, previamente, a intensidade que as ações preventivas de proteção devem ter e promover uma melhor abordagem quando for aplicá-las. Porém, ainda não é o suficiente. Convém, como passo seguinte, verificar quais os elementos do sistema que, no momento atual, promovem um ambiente seguro.

5.4 ELEMENTOS DE SEGURANÇA DO SCDP

Antes de iniciar os trabalhos de campo, enviou-se um e-mail para a Coordenação Geral de Segurança da Informação, do MPOG, solicitando disponibilização da Política de Segurança do SCDP a fim de subsidiar os questionamentos colocados nesta pesquisa. Tal fato ocorreu no dia 20 de setembro de 2012 e não se obteve resposta. No mês seguinte, isso se repetiu, especificamente, no dia 08 de outubro, porém, novamente, sem atendimento. As cópias desses e-mails estão demonstradas nos Apêndices B e C, no final desta pesquisa.

Uma política de segurança específica ao SCDP traria um significativo ganho de produtividade ao estudo, pois daria uma base de informações operacionais cujos procedimentos poderiam ser usados como guia para o tratamento das adequações ao contexto de atuação da universidade. Contudo, preliminar à análise de risco, levantaram-se os componentes de segurança do sistema para verificar se existem nele pontos vulneráveis que podem estar sujeitos a alguma ameaça. Na realidade, existem milhares de formas diferentes de ataques aos sistemas de informação, e essa identificação é um passo importante para a formulação de medidas apropriadas de segurança.

Os usuários com perfis de aprovação necessitaram de certificação digital para ingressar no sistema. Trata-se de um mecanismo de segurança capaz de garantir autenticidade, confidencialidade e integridade às informações eletrônicas e de permitir a guarda segura de documentos. O processo dessa certificação, na UFPB, faz parte do conjunto de normas, padrões e procedimentos relacionados à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Iniciou-se pela elaboração do documento “Certificado pela Autoridade de Registro Serpro”, que apresentava o nome de cada usuário do SCDP responsável pela movimentação das informações no sistema. Em seguida, o documento foi enviado ao Ministério do Planejamento (MP) para aprovação.

Após aprovar o “Certificado pela Autoridade de Registro Serpro”, o MP enviou os tokens ao Serpro, ou seja, as mídias utilizadas para armazenar a chave privada dos usuários inscritos no certificado. A partir desse momento, cada usuário teve que comparecer a uma unidade da Serpro, considerada a autoridade certificadora, com

seus documentos de identificação, a fim de validar o certificado, assinar o Termo de Titularidade de Certificado Digital e pegar sua chave privada armazenada no token. Desde então, para ingressar no SCDP, é necessário o uso associado do token com a senha numérica.

De acordo com a Medida Provisória nº 2.200-2, os documentos digitais do SCDP, produzidos com a utilização de certificação digital de uma autoridade certificadora vinculada à ICP-Brasil, são presumidos como verdadeiros em relação aos signatários (BRASIL, 2001).

O certificado digital é um documento de identidade eletrônico, que tem o objetivo de identificar uma pessoa, empresa ou sistema computacional no mundo da Internet e contém uma sequência de código único, chamado de chave pública, que tem a finalidade de validar uma assinatura realizada em documentos digitais. É utilizada para se certificar de que determinado documento foi assinado pelo possuidor da chave privada daquele certificado.

São várias as condições, as obrigações e as responsabilidades contidas no Termo de Titularidade de Certificado Digital, que só deve ser assinado pelo titular do certificado de assinatura digital. Todas elas se constituem importantes para a garantia da segurança da informação, no entanto, as mais relevantes para a pesquisa foram: a) responsabilização pelos atos praticados perante a Receita Federal; b) confirmação do conhecimento adquirido quanto à Política de Certificado Digital e ao uso de chaves públicas; c) responsabilização pelos atos praticados por terceiros de culpa recíproca; d) garantia pela proteção e pelo sigilo da chave pública individual, mediante uso de senha com, no mínimo, oito caracteres; e) responsabilização integral pela guarda, divulgação e uso indevido dos dispositivos criptográficos; f) informação ao Serpro sobre qualquer comprometimento ou suspeita de comprometimento da chave privada (roubo, acesso indevido, perda ou modificação), solicitando, em seguida, imediata revogação do certificado.

Outra característica do SCDP, que lhe atribui como um sistema seguro, é a impossibilidade de mantê-lo funcionando, caso permaneça sem movimentação de dados por um período de tempo. Levantaram-se informações que norteiam essa temática quando na abordagem da entrevista e se perguntou se era costume, no ambiente de trabalho, deixar o computador com as telas abertas. Durante as repostas, a maioria fez menção a esse limite estabelecido pelo sistema, e a coleta

estruturada demonstrou que 85% responderam “Nunca”, 10%, “Raramente”, e 5%, “Às vezes”.

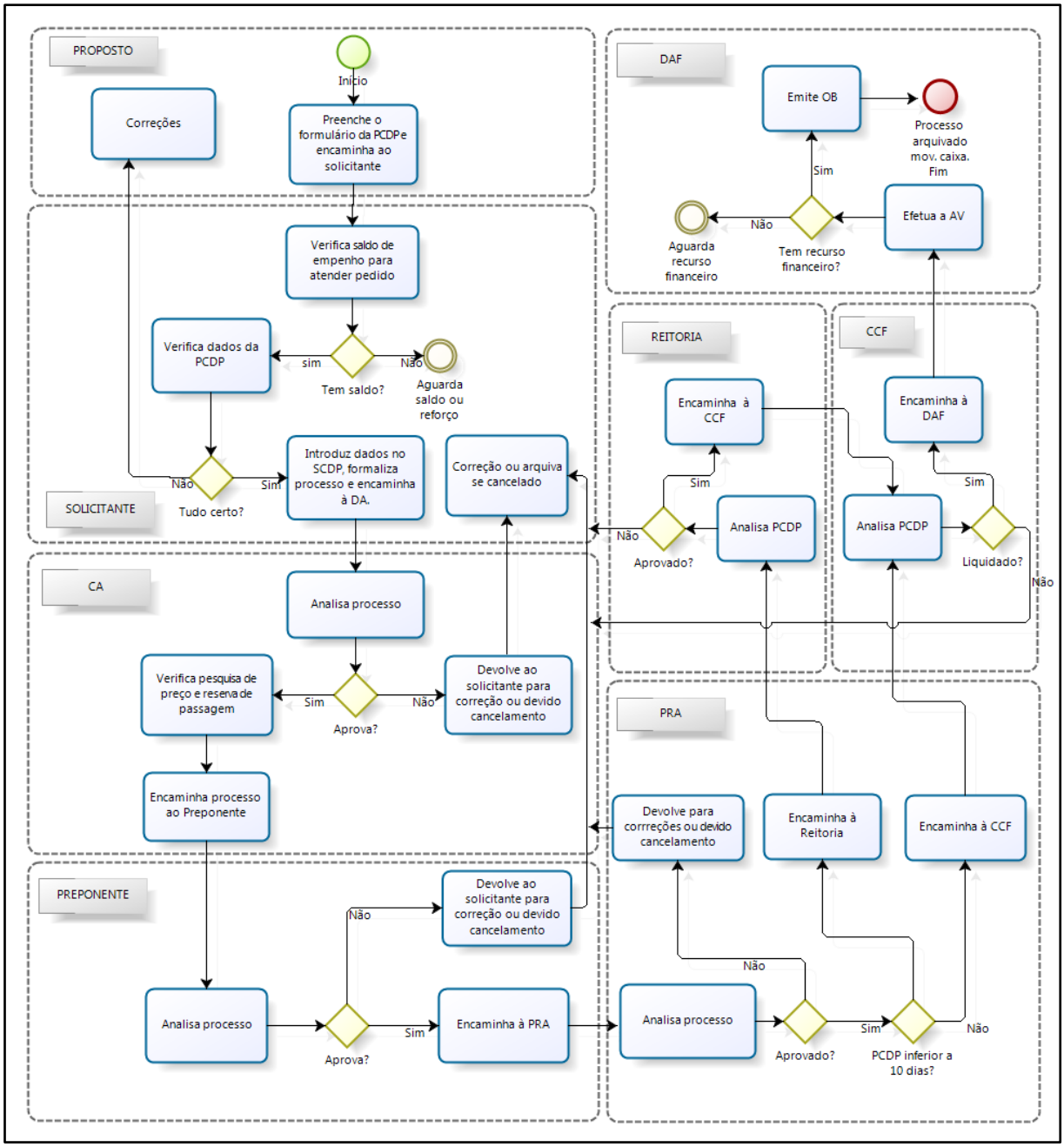
Levantaram-se, na pesquisa, os elementos de segurança do SCDP, que foram implantados de acordo com as atribuições da certificação digital ICP-Brasil. Eles enfatizam a importância de haver uma política de segurança da informação nos órgãos governamentais para dar continuidade aos objetivos estabelecidos no processo de implantação.

Segundo Beal (2011), o primeiro elemento fundamental para fundamentar uma PSI é identificar o responsável e prestar contas pela informação, bem como as linhas hierárquicas para as funções. Em relação ao sistema em estudo, é necessário conhecer as funções classificadas como tomadoras de decisão, ou seja, usuários com perfis capazes de aprovar as ações do sistema. Eles são os que asseguram que a organização cumpra sua missão de modo eficaz, atendendo às expectativas dos beneficiários das diárias e das passagens.

De acordo com dados obtidos pela entrevista, constatou-se que 40% dos entrevistados tinham a função de conceder autorização no SCDP. Os outros que formaram o total de 12 usuários não tinham certificação digital e passaram a ter acesso ao sistema através de um cadastro efetuado pelo gestor setorial lotado na Coordenação de Administração da instituição.

Objetivando uma melhor visualização dos setores que concedem autorizações, elaboramos o fluxo do processo de pedido de diárias e passagens apresentado na figura 6 seguinte.

Figura 8 – Mapa do fluxo de pedido de diárias e passagens do SCDP



Fonte: Elaborado pelo autor no BizAgi (2013)

Em resumo, a Proposta de Concessão de Diárias e Passagens é preenchida pelo proposto, que pode ser um servidor, colaborador eventual ou agente externo. Em seguida, o documento é entregue ao solicitante, ou seja, um servidor sem perfil de autorização, que fica encarregado de alimentar inicialmente os dados da viagem e incluir a documentação comprobatória. Isso analisa a disponibilidade de concessão da viagem e a PCDP, devolvendo-a para correção ou fazendo seu

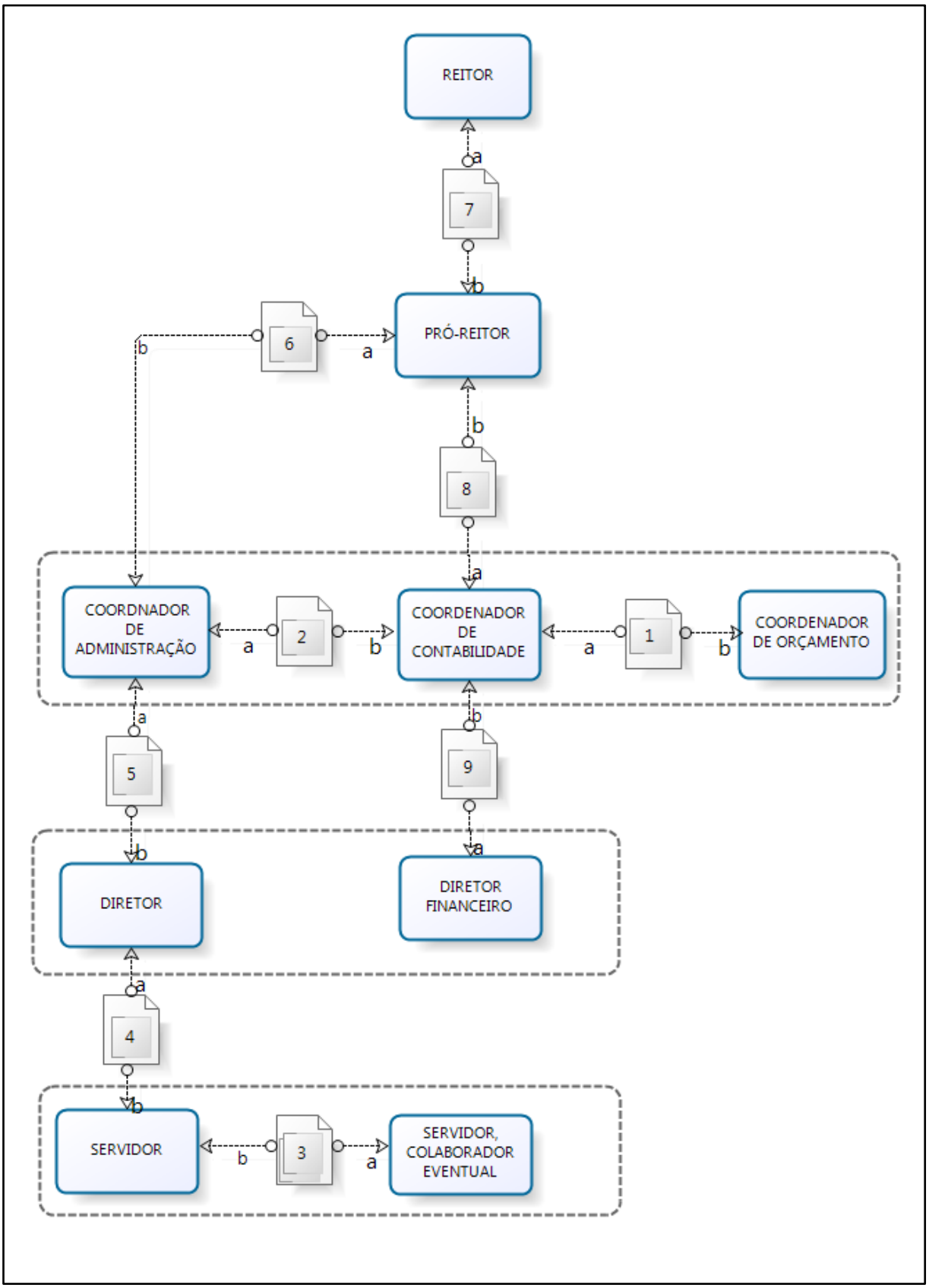
cancelamento. Caso a PCDP seja atendida, formaliza-se um processo que será encaminhado, via protocolo geral, para a Coordenação de Administração. Estando na coordenação, o processo será avaliado, e as cotações de preços efetuadas para a contratação dos serviços. Se os procedimentos preliminares estiverem em conformidade com a lei, o processo é enviado ao diretor do centro acadêmico ou ao coordenador de Administração da PRA, que são os preponentes ou concedentes da viagem. Após aprovação administrativa, o processo segue até o Pró-reitor, que ordenará o pagamento da despesa na contabilidade. Em seguida, se o rito processual estiver na Coordenação de Contabilidade e Finanças, obedecerá às fazes da despesa que se referem à liquidação e ao pagamento. A liquidação é outra etapa de aprovação em que o processo será verificado de acordo com o direito financeiro contido em leis específicas. Por fim, haverá a apropriação da despesa através da emissão da AV e o pagamento ao proposto pela OB, em ações efetuadas pela Divisão Administrativa e Financeira.

5.5 FLUXO INFORMACIONAL DO SISTEMA

Embora o SCDP permita a tramitação e a certificação digital dos documentos, o formato impresso ainda permanece como meio de comunicação entre os setores. Essa movimentação de documentos impressos, durante o processamento do sistema de informação, contribui para o surgimento de vulnerabilidades susceptíveis a diferentes ameaças.

Para apresentar uma melhor visualização do fluxo de informações, elaboramos a figura 7, a seguir:

Figura 9 – Mapa do fluxo de informações no SCDP



Fonte: Elaborado pelo autor no BizAgi (2013)

No total, são nove estações de trabalho que trocam informações quando executam o processo de solicitação das diárias e das passagens da instituição. O detalhamento do fluxo de informações do SCDP é exposto no quadro 15 mediante três colunas. A primeira representa a ordem do fluxo e a codificação do fornecimento/recebimento da informação; a segunda descreve as ações. e a última mostra o canal utilizado para a comunicação.

Quadro 14 – Conteúdo dos fluxos da informação no SCDP

Fluxo		**Descrição do conteúdo do fluxo**	**Canal de comunicação**
1	a	Memorando aberto informando a abertura de crédito orçamentário, protocolado manualmente	Documento impresso
	b	Processos que apresentam indisponibilidade de crédito	Processo aberto
2	a	Cópia do empenho feito pelo crédito aberto para cadastramento no SCDP	Documento impresso
	b	Processos autorizados pelo Pró-reitor após correções.	Documento impresso via protocolo geral
3	a	Informações sobre aquisição de viagem. Formulário da PCDP e orientações para seu preenchimento	Documento impresso, oral, telefone, e-mail.
	b	PCDP preenchida para alimentar dados no SCDP.	Documento impresso
4	a	PCDP preenchida, solicitação de viagem para assinatura, documentos comprobatórios.	Documento impresso
	b	Documentação assinada ou devolvida por motivo de cancelamento o,0 u para correções.	Documento impresso
5	a	Processo formalizado contendo memorando, formulário PCDP e comprovantes da viagem. Processo autorizado após despacho da Coordenadora de Administração.	Documento impresso via protocolo geral.
	b	Processo para autorização após consulta de preços e reservas. Devolução por motivo de cancelamento ou para correção.	Documento impresso via protocolo geral.
6	a	Processo para aprovação do Pró-reitor com despacho do Coordenador de Administração.	Documento impresso via protocolo geral.
	b	Processo com despacho aprovado ou devolvido por motivo de cancelamento ou para correção.	Documento impresso via protocolo geral.
7	a	Processo para aprovação do Reitor por viagem pedida com menos de dez dias.	Documento impresso via protocolo geral.
	b	Processo com despacho do Reitor autorizando viagem inferior a dez dias ou devido a cancelamento.	Documento impresso via protocolo geral.

Quadro 14 – Conteúdo dos fluxos da informação no SCDP

Fluxo		Descrição do conteúdo do fluxo	Canal de comunicação
8	a	Processo com despacho do Pró-Reitor para pagamento.	Documento impresso via protocolo geral
	b	Devolução do processo por falta de saldo no empenho de diária/passagem ou para correção após liquidação.	Documento impresso via protocolo geral
9	a	Processo para emissão da (AV) autorização de viagem e pagamento pela (OB) ordem bancária através do SCDP, integrado ao SIAFI.	Documento impresso via protocolo geral.
	b	Processo devolvido devido a incorreções pela emissão da ordem bancária.	Documento impresso via protocolo geral

Fonte: Elaborado pelo autor em pesquisa direta (2013)

Durante a realização das entrevistas, observou-se que alguns setores que mantinham os processos em mesas de trabalho por longo tempo, em outras situações, estavam acomodados no chão ou guardados em compartimentos abertos.

5.6 ANÁLISE DE RISCO

A análise de risco é parte fundamental da gestão da segurança da informação, porque complementa as etapas (mapeamento do processo, identificação das responsabilidades e análise do sistema em estudo) já descritas até o momento. 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, conforme demonstrados no quadro 14, na etapa seguinte, foi empregado o quadro 10, para 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 11, 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 4, os seguintes resultados da análise de risco efetuada:

Tabela 4 – 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)

Tabela 4 – 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)
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)
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)

Tabela 4 – 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)
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 4 sinaliza para 10 grupos que, 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 4, identificou-se a matriz de risco através do quadro 12, 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.

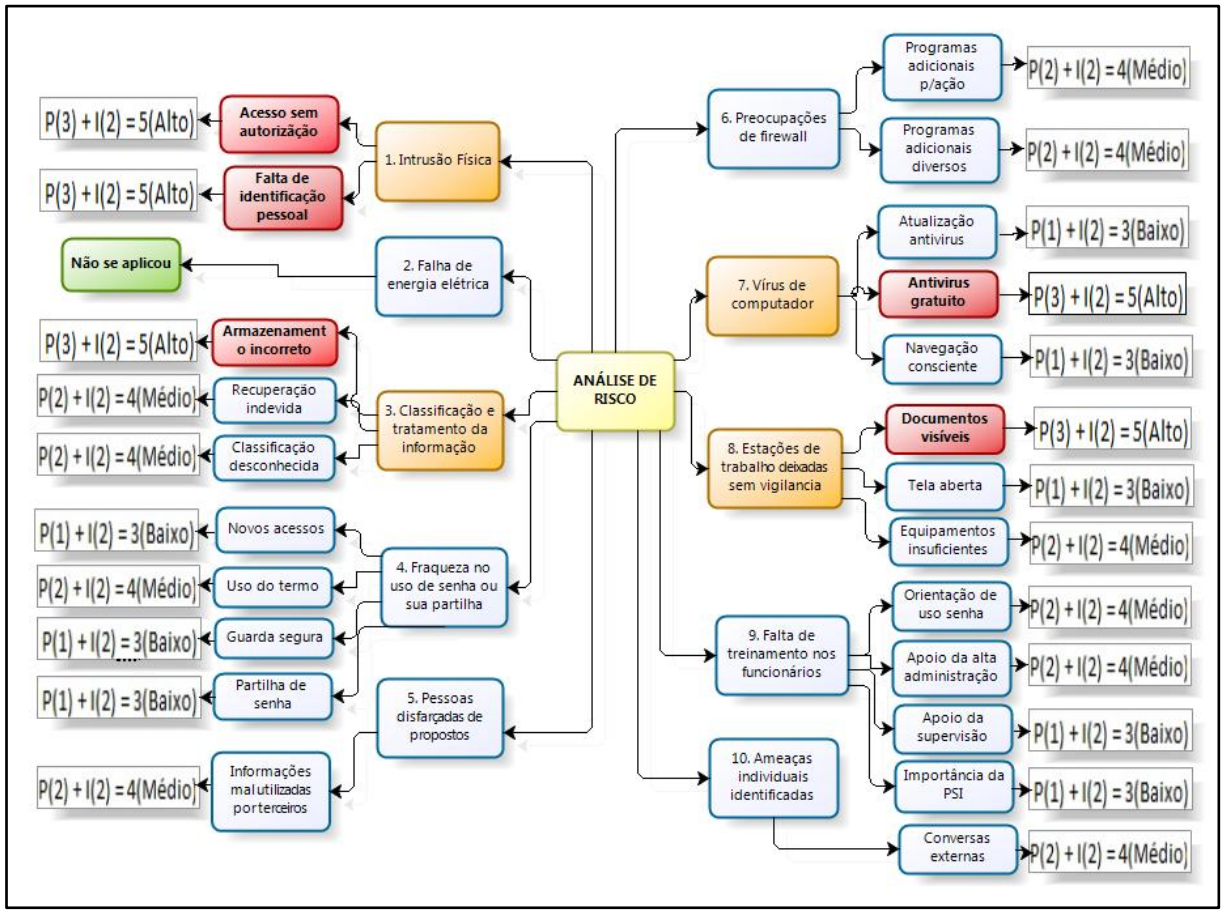
A princípio, não houve grupo cujo resultado apresentou risco alto e risco baixo, relacionado, respectivamente, a uma matriz A e D. Todavia, as ameaças classificadas em uma matriz C, relativas a um nível médio de risco, foram: fraqueza no uso de senha ou sua partilha, pessoas disfarçadas de propostos, 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 8, logo abaixo, é possível visualizar todo o processo da análise de risco:

Figura 10 – 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, enquanto para aqueles com medição alta, devem ser executados procedimentos corretivos. Essas medidas que asseguram o controle das ameaças do SCDP serão abordadas no próximo tópico.

5.6.1 Controle para ameaças

É indispensável conhecer as principais ameaças ao sistema de informação e, na mesma proporção, entender as formas de defesa contra essas ameaças. Em razão de sua importância para toda instituição, organizar um mecanismo de defesa é uma das principais atividades de qualquer gestão administrativa que queira controlar os recursos da informação. Segundo Turban (2005, p. 451), “na verdade, a segurança da TI é responsabilidade de *todos* em uma organização”. É necessário o entendimento e a contribuição dos envolvidos no processamento das informações, para atingir o nível de segurança desejável, caso contrário, serão pontos fracos que podem resultar em incidentes de segurança.

Segundo Laudon et. al. (2004, p. 467), “os controles consistem, portanto, em todos os métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão, a confiabilidade dos seus registros contábeis e a adesão operacional aos padrões administrativos”.

Observou-se que a instituição pesquisada não possui um documento formal relacionado a uma Política de Segurança da Informação, portanto, aos grupos de ameaças que apresentaram riscos de nível médio, ações de monitoramento precisam ser elaboradas. Nesse caso, sugerem-se algumas medidas destinadas ao controle, a saber:

- 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.

A seguir, serão abordadas as medidas de controle apropriadas para os grupos de ameaças que resultaram em riscos de alto nível.

a) Intrusão física

Representa o acesso não autorizado às áreas onde está sendo processada ou armazenada a informação que possa acarretar em danos, perdas ou sua divulgação indevida.

De acordo com a norma ABNT ISO/IEC (2005, p. 26), é necessário 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. Outra medida importante é a criação de pontos de acesso ao público - áreas de entrega e de carregamento - para haver mais controle das pessoas não autorizadas e que esses sejam isolados dos recursos informacionais.

Para Turban et. al. (2004, p. 452), é preciso restringir o acesso não autorizado aos recursos da informação com ênfase na identificação do usuário. Portanto, é importante, para qualquer organização, o uso de identificação visual, por meio de crachás, para que a equipe de segurança e os servidores diferenciem as pessoas que tramitam nas dependências do órgão. Além do mais, painéis indicativos de acesso restrito colocados em locais adequados podem reduzir as abordagens indevidas.

Através da observação direta, verificaram-se a falta de identificação pessoal nos servidores da universidade e a ausência de painéis indicativos nas portas de entrada que possam restringir o acesso indevido nas dependências.

b) Classificação e tratamento da informação

Compreende a falta de conhecimento pelos usuários do sistema da classificação da informação quanto aos princípios de disponibilidade, confidencialidade e integridade (BEAL, 2011, p. 60). Envolve também a deficiência de procedimentos referente ao manuseio e ao descarte da informação que possam resultar numa “divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio” (ABNT ISO/IEC, 2005, p. 29).

Segundo informações da pesquisa, ao passo que 100% utilizam documentação impressa, 30% afirmaram haver possibilidade de elas serem vistas por terceiros, e 45% apontaram para uma recuperação indevida depois do descarte. Além do mais, 35% não consideram seus papéis de trabalho como confidenciais. Esses dados levaram à ameaça “armazenamento incorreto” ao nível alto e as outras, “Recuperação indevida” e “Classificação desconhecida” ao ponto médio, necessitando de ações corretivas para o grupo “Classificação e Tratamento da Informação”.

A primeira medida de segurança para esse caso envolve uma classificação das informações do SCDP quanto aos princípios de disponibilidade, confidencialidade e integridade, enquanto vários tipos de documentos devem ser protegidos de diferentes maneiras. Esse é um dos primeiros passos para o estabelecimento da política de segurança. Em seguida, deve-se propiciar um treinamento para os usuários do sistema, a fim integrar na rotina do servidor os procedimentos provenientes da classificação, para que eles compreendam corretamente a manipulação e o armazenamento dos dados e documentos com diferentes níveis (PELTIER, 2005, p. 176).

c) Vírus de computador

São os diversos tipos de ataques contra qualquer serviço, computador ou rede que esteja acessível via Internet. A lista de ataques é bastante ampla, e os mais usados são a varredura de rede e os códigos maliciosos. Nesse aspecto, a universidade encontra-se numa posição elevada de risco, visto que todos os setores pesquisados informaram usar programas de antivírus sem custo financeiro, colocando a organização numa espécie de proteção limitada e sem padrão.

As medidas de controle incluem: instalação do padrão corporativo de software antiviral em todos os setores; incorporar nas políticas e nas 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 (PELTIER, 2005).

As organizações devem procurar adquirir um programa de antivirus que tenha algum custo financeiro devido às atualizações proporcionadas serem mais confiáveis. Além disso, evita que cada usuário instale em seu equipamento diferentes tipos de software, quebrando o padrão de segurança determinado pela empresa.

d) Estações de trabalho deixadas sem vigilância

São riscos provenientes de usuários que permitem expor, sem monitoração e proteção adequada, documentos impressos, mídias removíveis e telas de computador.

Durante as visitas nos setores para a coleta de dados, em alguns departamentos, constataram-se processos expostos permanentemente em locais de fácil alcance, outros até armazenados no chão, quando deveriam estar guardados em armários de fechadura para proteger as informações de caráter sigiloso. Esse fato foi exposto no resultado da pesquisa, quando 85% afirmaram deixar à vista os papéis de trabalho no ambiente laboral. Esse fato se agrava com a falta de controle no fluxo de visitantes durante o expediente.

O controle para esse tipo de risco envolve a atribuição de responsabilidades, através da 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, 2005, 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).

Para uma visualização direta dos controles sugeridos pela pesquisa, elaboramos o quadro 16, seguinte:

Quadro 15 – 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 27001)
	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 prevençao 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 saida) 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, 2005, 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)

6 CONSIDERAÇÕES FINAIS

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.

Apesar das dificuldades encontradas no decorrer deste estudo, isso não foi suficiente para prejudicar os resultados previstos e contribuir com o papel fundamental da instituição pesquisada. Entre esses obstáculos, destacou-se a espera pela aprovação do Comitê de Ética em Pesquisa, necessária para trabalhos que envolvam seres humanos, o que resultou na ausência de alguns servidores pelo fato de a abordagem ter ocorrido num período propício às férias. Outro fato que merece destaque foi a falta de uma resposta da Coordenação Geral de Segurança da Informação, do MPOG, referente à Política de Segurança do SCDP.

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 autorizar o sistema que 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 escrita ainda é necessária e tramita em oito estações de trabalho. 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 anual 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 TI 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, Luiz; PINOCHET, Luis. **Política de segurança de informações: uma visão organizacional para sua formulação**. São Paulo: Elsevier, 2010.

ALVES, G. A. **Segurança da Informação – Uma visão inovadora da gestão.** Rio de Janeiro: Editora Ciência Moderna, 2006.

ANGELONI, Maria Terezinha. **Elementos intervenientes na tomada de decisão**. Ci. Inf., Brasília, v. 32, n. 1, p. 17-22, jan./abr. 2003.

ARAGÃO, Lúcia B. **Autonomia universitária: tentativa de uma delimitação consensual pelo emprego da "técnica Delphi**". Rio de Janeiro: dissertação de Mestrado da Universidade do Rio de Janeiro, 1985.

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.

BRASIL**.** Lei 4.320, de 17 de março de 1964. Estatui normas gerais de Direito Financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 04 mai. 1964. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/l4320.htm>. Acesso em 20 de outubro de 2012.

_____. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 jun. 2000. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em 10 de agosto de 2011.

_____. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasi**l, Brasília, DF, 28 dez. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/ D4553.htm>. Acesso em 10 de agosto de 2011.

_____. Medida provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileiras – ICP-BRASIL - transforma o Instituto Nacional de Tecnologia da Informação em autarquia e dá outras providências. Brasília, **Diário Oficial [da] República Federativa do Brasi**l. Brasília, DF, de 27 de agosto de 2001. Disponível em:<http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm. Acesso em 24 de fev. de 2013.

_____. **Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008**. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 18 jun. 2008. Disponível em:<http://www.presidencia.gov.br/gsi/cgsi/instrucao_normativa_01_cgsi.pdf. Acesso em 25 de agosto de 2011.

_____. **Guia de Referência para a Segurança da Informação – Usuário final**. SLTI/ Coordenação de Segurança da Informação. Versão 1.0, 2005.

_____. **Manual de Implantação do SCDP.** SLTI/ Coordenação de Segurança da Informação. Brasília: Ministério do Planejamento, Orçamento e Gestão, 2007.

_____. **Proposta de política de governo eletrônico para o Poder Executivo Federal.** Grupo de trabalho, "novas formas eletrônicas de interação". Brasília: Ministério do Planejamento, Orçamento e Gestão, 2000.

BATISTA, Carlos Freud Alves. **Métricas de segurança de software**. Dissertação (Mestrado em Informática) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

BAUER, Martin; GASKELL, George. **Pesquisa qualitativa com texto, imagem e som**. 6ed. Petrópoles: Vozes, 2007.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

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.

BIBLIOTECA DIGITAL DE TESES E DISSERTAÇÕES (BDTD). Disponível em www.bdtd.com.br, acessado em 29/05/2012.

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.

BUSH, Vannevar. **As we may think**.HTML version by Denys Duchier, University of Ottawa, April 1994. Updated August 1995, Simon Fraser University. Em:<http://www.ps.uni-saarland.de/~duchier/pub/vbush/vbush-all.shtml>. Acessado em: 08 de agosto de 2011.

CAPURRO, Rafael. **Epistemologia e Ciência da Informação**. Tradução de Ana Maria Rezende Cabral, Eduardo Wense Dias, Isis Paim, Lígia Maria Moreira Dumont, Marta Pinheiro Aun e Mônica Erichsen Nassif Borges. Belo Horizonte: 2003.

CARUSO, C. A. A.; STEFFEN, E. D. **Segurança em informática e de informação**. São Paulo: Administração Regional do Senac, 1999.

CHIZZOTTI, Antônio. **A pesquisa em ciências humanas e sociais. Pesquisa qualitativa em ciências humanas e sociais**. Petrópolis: Vozes, 2008, p. 19 -31.

CIRIBELLI, Marilda Corrêa. **Como elaborar uma dissertação de Mestrado através da pesquisa científica**. Rio de Janeiro: 7 Letras, 2003.

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.

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.

FUGINI, M.; BELLETTINNI, C. **Information Security: polices and actions in modern integrated systems**. Pensilvânia: Idea Group, 2004.

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

Governo bloqueia tentativa de invasão a sites. Disponível em: http://www.clicrbs.com.br/jsc/sc/impressa/4,181,3362044,17386. Acessado em 20 de setembro de 2011.

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.

ISACA, **The Risk It Framework**, USA, 2009.

JANSSEN, Luís Antônio. **Instrumento de avaliação de maturidade em processos de segurança da informação: estudo de caso em instituições hospitalares**. Dissertação (Mestrado em Administração e Negócios) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2008.

KRUTZ, Ronald L.; VINES, Russell Dean. **The CISSP Prep Guide**: mastering the ten domains of computer security. USA: Wiley Computer Publishing, 2001.

LAFER, Celso. Vazamentos, sigilo, diplomacia: a propósito do significado do WikiLeaks. Revista Política Externa. São Paulo. Vol. 19, nº 4, mar/abr/mai 2011.

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

LAUREANO, M. A. P. **Gestão de Segurança da Informação**, 2005. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> Acessado em 15 de setembro de 2011.

MACEDO, Danilo. **Tentativa de invasão a sites do governo foi a maior já registrada.** Em: <http://br.noticias.yahoo.com/tentativa-de invasão-a-sites-do-governo-foi-a-maior-já-registrada.html>. Acessado em: 10 de agosto de 2011.
MARTINO, A. S. & PERRAMON, X. Phishing Secrets: History, Effects, and Countermeasures. **International Journal of Network Security**, vol. 11, nº 3, p. 163-171, nov. 2010.

MENEZES, Josué Chagas. **Gestão da segurança da informação**. Leme: Mizuno, 2006.

MYNAYO, Maria Cecília de Souza. **A análise de dados em pesquisa qualitativa. In:** _____ **Pesquisa Social.** 22 ed. Petrópolis: Vozes, 1998, p. 67 – 79.

MYNAYO, M. C. S. & SANCHES, O. **Quantitativo-qualitativo: oposição ou complementaridade?** Cad. Saúde Pública, Rio de Janeiro, 9 (3): 239 – 262, 1993.

MYNAYO, Maria Cecília de Souza. **Introdução à metodologia de pesquisa social. In:** _____ **O desafio do conhecimento**. 4 ed. São Paulo: Hocitec, 1996, p. 19 – 87.

MORIMOTO, Carlos Eduardo. **Redes - guia prático**. Porto Alegre: Sul Editores, 2010.

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.

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.

SAKAUE, Eduardo. **Estendendo modelos de controle de acesso para uma nova abordagem em segurança**. Dissertação (Mestrado em Engenharia Eletrônica e Computação) – Instituto Tecnológico de Aeronáutica, São José dos Campos, 2008.

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

SANTOS. Boaventura de Sousa. **O norte, o sul e a utopia. In:** _____ **Pela mão de Alice**. São Paulo: Cortez, [1997]. Cap. 10, p.281-348.

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

SHAHRI, Ahmad; ISMAIL, Zuraini. A tree model for identification of threats as the first stage of risk assessment in HIS. **Journal of Information Security**, USA, v. 3, n. 02, p. 169-176, abr. 2012.

SHERA, JH; CLEVELAND, DB. **History and foundations of information-science, Annual review of information science and technology**, 12: 249-275. 1977.

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

SILVA, Denise Ranghetti Pilar da. **A memória humana no uso de senhas**. Tese (Doutorado) – Faculdade de Psicologia. Programa de Pós-graduação em Psicologia. PUCRS, 2007.

SILVA, P. T.; CARVALHO, H.; TORRES, C. B. **Segurança dos Sistemas de Informação: gestão estratégica da segurança empresarial**. Portugal: Centro Atlântico, 2003.

SILVA, Walber José Adriano. **Investigação empírica sobre a percepção da segurança da informação pelos usuários de uma Universidade Pública Baseada na Análise Fatorial Exploratória**, 2011. 155 f. Dissertação (Mestrado em Informática) – Universidade Federal da Paraíba, João Pessoa.

SIQUEIRA, J. **Nucleando qualidade**. Instituto Brasileiro de Qualidade Nuclear. Rio de Janeiro, n. 45, p. 4, ano XI, 2005.

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.

Symantec Intelligence Report: novembro 2012. Estados Unidos, 2012, p. 3. Disponível em: <http://www.symantec.com/pt/br/theme.jsp?themeid=gin>. Acesso em: 22/12/2012.

TARAPANOFF, Kira. **Técnica para tomada de decisão nos sistemas de informação**, 2ª Ed, Brasília: Thesaurus, 1995.

TITTEL, Ed; CHAPPLE, Mike; STEWART, James Michael. **Certified information systems, security professional:** study guide. San Francisco: SYBEX, 2003.

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.

VERGARA, Sylvia Constant. **Métodos de pesquisa em Administração** – 3. Ed. – São Paulo: Atlas, 2008.

VLACHOS, Vasileios; SPINELLIS, Diomidis. **A PRoactive malware identification system based on the computer hygiene principles**. Information Management & Computer Security, Vol. 15 Iss: 4, p. 295-312.

WORMAN, Michael**. Wisecrakes: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security.** Journal of the American Society for Information Science and Technology, 59(4): 662-674, 2008.

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

APÊNDICE A – QUESTIONÁRIO PARA ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO SISTEMA DE CONCESSÃO DE DIÁRIAS E PASSAGENS DA UFPB.

O questionário aplicado como roteiro de entrevista objetivou levantar evidências para a análise de risco com foco na segurança da informação nos documentos processados no SCDP.

O questionário foi estruturado e elaborado com base no FRAAP (Facilitated Risk Analysis and Assessment Process) e pelo "Guia de Referência para a Segurança da Informação – Usuário Final", da Coordenação de Segurança da Informação. São 29 perguntas divididas em três módulos: processos, pessoas e tecnologia.

Item	Pergunta	Resposta
Identificação		
1	Sexo:	( ) Masculino ( ) Feminino
2	Qual seu cargo na organização?	R.: _____ _____
3	Sua função no SCDP exige conceder autorização?	( ) Sim ( ) Não ( ) Às vezes
Módulo I – Processos		
4	Em sua opinião, qual a importância do SCDP para a organização onde você trabalha?	( ) Muito importante ( ) Importante ( ) Com alguma importância ( ) Pouquíssima importância ( ) Sem importância
5	Você classifica as informações do SCDP como confidenciais?	( ) Sim ( ) Não
6	O SCDP atende às necessidades da organização?	( ) Sim ( ) Não ( ) Às vezes
7	Faz uso de outros programas a fim de controlar as informações que são processadas no SCDP?	( ) Sim ( ) Não ( ) Às vezes
8	É necessário armazenar a documentação de forma impressa?	( ) Sim ( ) Não ( ) Às vezes
9	As informações físicas podem ser recuperadas em lixeiras ou em outros depósitos?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca

Item	Pergunta	Resposta
Módulo I – Processos		
10	Documentações para diferentes interessados são enviadas num único envelope?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
11	Recebeu orientação sobre a manutenção sigilosa de sua senha de acesso e a responsabilidade envolvida pelo mau uso dela?	( ) Sim ( ) Não ( ) Não lembro
12	Em algumas situações, as informações enviadas a terceiros podem ser mal utilizadas?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
13	As solicitações para novas identificações de usuários e alteração de privilégios são feitas por escrito e aprovadas pela chefia imediata do usuário?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
14	Todos os usuários que desejam usar o SCDP assinam o Termo de Responsabilização e Sigilo pelo qual concordam com as políticas, padrões, normas e procedimentos do Órgão Público relacionados ao ambiente de TI?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
15	A alta administração está ciente de que as instituições precisam de um programa eficaz de segurança da informação?	( ) Sim ( ) Não ( ) Não tenho conhecimento ( ) Não lembro
16	Os gestores do centro incentivam uma política de segurança da informação?	( ) Sim ( ) Não ( ) Não lembro
17	Em sua opinião, classifique a importância de haver na instituição uma ação efetiva com os usuários do SCDP sobre a Política de Segurança da Informação?	( ) Muito importante ( ) Importante ( ) Com alguma importância ( ) Pouquíssima importância ( ) Sem importância
Módulo II – Pessoas		
18	O Centro exige autorização no acesso ao setor por pessoas que não sejam servidoras da instituição?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
19	O centro utiliza-se de identificação pessoal pelo uso de crachás nos servidores?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
20	Você guarda em local seguro o dispositivo móvel (token) que dá acesso ao SCDP?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
21	Você permite que terceiros saibam sua senha de acesso?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca

Item	Pergunta	Resposta
Módulo II – Pessoas		
22	Os papéis de trabalho costumam ser deixados à vista na mesa de trabalho?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
23	Procura discutir assuntos de trabalho em ambientes que não sejam da instituição?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
24	É costume, no ambiente de trabalho, deixar o computador ligado com as janelas abertas?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
25	Armazena ou usa programas que não sejam destinados ao objetivo de sua função na instituição?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
Módulo III – Tecnologia		
26	Qual a frequência de atualização do seu antivírus?	( ) Todos os dias. ( ) Uma vez por semana. ( ) Duas ou mais vezes por semana. ( ) Uma vez por mês. ( ) Desconheço o período. ( ) Não atualizo
27	O antivírus tem algum custo financeiro?	( ) Sim ( ) Não ( ) Não, mas já teve. ( ) Nunca
28	Certifica-se de que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação?	( ) Sempre ( ) Às vezes ( ) Raramente ( ) Nunca
29	Os equipamentos do setor são suficientes para executar seu trabalho no SCDP?	( ) Sim ( ) Às vezes sinto dificuldade ( ) Não

APÊNDICE B – E-MAIL ENVIADO AO MPOG EM 20 DE SETEMBRO DE 2012 SOLICITANDO A POLÍTICA DE SEGURANÇA DO SCDP

De:	"Josivan de Oliveira Ferreira" <josivan@pra.ufpb.br>
Assunto:	Política de Segurança do SCDP
Data:	Qui, Setembro 20, 2012 4:00 pm
Para:	joseney.lima@planejamento.gov.br

Boa tarde Sr. Coordenador José Ney de Oliveira Lima. Meu nome é Josivan de Oliveira Ferreira, sou pesquisador da Universidade Federal da Paraíba (UFPB)do curso de mestrado em Ciência da Informação, cujo projeto de pesquisa está titulado como "ANÁLISE SOB A ÓTICA DA SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: estudo de caso aplicado ao SISTEMA DE CONCESSÃO DE DIÁRIAS E PASSAGENS (SCDP) no departamento contábil da UFPB". No entanto, venho através deste email perguntar ao senhor se já existe uma política de segurança da informação aplicado ao SCDP que possa enrriquecer, ainda mais, minha pesquisa. Caso a resposta seja positiva, ficaria muito agredecido ao senhor pela possibilidade de indicar-me o caminho de acesso à esta informação.

Pedindo desculpas pelo tempo ocupado, finalizo aguardando ansiosamente a sua resposta.

Josivan de Oliveira Ferreira
Mestrando em Ciência da Informação da UFPB
Fone: (83) 3216-7408

APÊNDICE C – E-MAIL ENVIADO AO MPOG EM 08 DE OUTUBRO DE 2012 SOLICITANDO, NOVAMENTE, A POLÍTICA DE SEGURANÇA DO SCDP

De: "Josivan de Oliveira Ferreira" <josivan@pra.ufpb.br>
Assunto: [Fwd: Política de Segurança do SCDP]
Data: Seg, Outubro 8, 2012 10:10 am
Para: jofer2011@gmail.com

---------- Mensagem Original ----------
Assunto: Política de Segurança do SCDP
De: "Josivan de Oliveira Ferreira" <josivan@pra.ufpb.br>
Data: Qui, Setembro 20, 2012 4:00 pm
Para: joseney.lima@planejamento.gov.br

Boa tarde Sr. Coordenador José Ney de Oliveira Lima. Meu nome é Josivan de Oliveira Ferreira, sou pesquisador da Universidade Federal da Paraíba (UFPB)do curso de mestrado em Ciência da Informação, cujo projeto de pesquisa está titulado como "ANÁLISE SOB A ÓTICA DA SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: estudo de caso aplicado ao SISTEMA DE CONCESSÃO DE DIÁRIAS E PASSAGENS (SCDP) no departamento contábil da UFPB". No entanto, venho através deste email perguntar ao senhor se já existe uma política de segurança da informação aplicado ao SCDP que possa enrriquecer, ainda mais, minha pesquisa. Caso a resposta seja positiva, ficaria muito agredecido ao senhor pela possibilidade de indicar-me o caminho de acesso à esta informação.

Pedindo desculpas pelo tempo ocupado, finalizo aguardando ansiosamente a sua resposta.

Josivan de Oliveira Ferreira
Mestrando em Ciência da Informação da UFPB
Fone: (83) 3216-7408