UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE EDUCAÇÃO / CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
MESTRADO PROFISSIONAL EM GESTÃO NAS ORGANIZAÇÕES APRENDENTES

FERNANDO ANTONIO FERREIRA DE SOUZA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS: elementos para elaboração de uma política de segurança da informação na Biblioteca Central da Universidade Federal da Paraíba

JOÃO PESSOA
2017

FERNANDO ANTONIO FERREIRA DE SOUZA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS: elementos para elaboração de uma política de segurança da informação na Biblioteca Central da Universidade Federal da Paraíba

Dissertação apresentada ao Mestrado Profissional em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, como requisito final para obtenção do Título de Mestre.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

Linha de Pesquisa: Gestão de Projetos Educativos e Tecnologias Emergentes

JOÃO PESSOA

2017

Catalogação na publicação
Universidade Federal da Paraíba
Serviço de Catalogação da Biblioteca Setorial do CCEN/UFPB

S729s Souza, Fernando Antonio Ferreira.
Gestão da segurança da informação em bibliotecas: elementos para elaboração de uma política de segurança da informação na Biblioteca Central da Universidade Federal da Paraíba / Fernando Antonio Ferreira Souza. – João Pessoa, 2017.
155 f.: il.

Dissertação (Mestrado Profissional em Gestão nas Organizações Aprendentes) – Universidade Federal da Paraíba.
Orientador: Profº Dr. Wagner Junqueira de Araújo.

1. Gestão da Segurança da Informação. 2. Biblioteca Universitária. 3. Política de Segurança da Informação.

BS-CCEN/UFPB CDU 004.056:023(043)

FERNANDO ANTONIO FERREIRA DE SOUZA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS: elementos para elaboração de uma política de segurança da informação na Biblioteca Central da Universidade Federal da Paraíba

Dissertação apresentada ao Mestrado Profissional em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, como requisito final para obtenção do Título de Mestre.

Aprovada em: 02 / agosto / 2017

BANCA EXAMINADORA

Prof. Dr. Wagner Junqueira de Araújo
Orientador

Prof. Dr. Marckson Roberto Ferreira de Sousa
Examinador Interno

Profa. Dra. Alzira Karla Araújo da Silva
Examinador Externo

Prof. Dr. Miguel Mauricio Isoni
Examinador Interno

Profa. Dra. Julianne Teixeira e Silva
Examinador Externo

AGRADECIMENTOS

Primeiramente, agradeço a Deus, Inteligência Suprema, causa primária de todas as coisas. Agradeço aos meus pais Maria Helena e Francisco Inácio, por seus valiosíssimos ensinamentos a mim passados. Aos meus irmãos, aos meus sobrinhos.

Meu especial agradecimento ao meu grande amigo Emmanuel Souza, pelo apoio, força, encorajamento e incentivos constantes.

Meu agradecimento ao meu orientador, Prof. Dr. Wagner Junqueira de Araújo, pelo incentivo, apoio e por acreditar neste trabalho.

Agradeço às amigas bibliotecárias Josélia Oliveira e Rosilene Machado, pela força, apoio, encorajamento.

Às professoras Ediane Carvalho, Edilene Toscano, Beliza Áurea pelo apoio e encorajamento. Aos colegas de trabalho Ana Karla Pereira, Anna Regina Ribeiro, Viviane Lima, Fátima Santos, Fernando Augusto, Ruston Sammerville, Jaqueline Rimá, Walkeline Araújo, André Domingos, Clébson Leandro e demais colegas do SISTEMOTECA da UFPB.

Aos amigos Cláudio Galvino, Neude Souza, Fernando Cordeiro, Vitor Macêdo, Émerson Cardoso, Patrício Inácio. Meu agradecimento aos colegas de mestrado (Mpgoa – 2015), em especial Andreza Serafim, Milena Borges e Hellys Sousa pela amizade e compartilhamento de aprendizados.

Agradeço à banca na pessoa da Profa. Dra. Alzira Karla e Prof. Dr. Markson Roberto, pelas valiosíssimas contribuições.

RESUMO

A proteção da informação tornou-se fator de extrema criticidade para as organizações e entidades de governo. Esta envolve não somente o ambiente convencional, mas a infraestrutura tecnológica e de redes informacionais. Este estudo se propôs abordar a Segurança da Informação no âmbito de uma biblioteca universitária. Mesmo sendo um ambiente familiarizado com os processos de gestão da informação, as bibliotecas vêm sofrendo com os problemas relacionados à falta de gestão da segurança da informação. Para tanto, esta pesquisa estuda os elementos de Gestão da Segurança da Informação que permitam a elaboração de uma minuta de Política de Segurança da Informação para a Biblioteca Central da Universidade Federal da Paraíba. Quanto os aspectos metodológicos, se caracteriza como qualitativa, do tipo descritiva. Como instrumento metodológico de coleta de dados, tabulação e análise, utiliza o Processo Facilitado de Análise e Avaliação de Risco (FRAAP), que foi complementado com questionário e a análise de conteúdo conforme Bardin. Os resultados apresentados indicam um grupo de quinze ameaças, dentre as quais se detectou nove ameaças físicas, duas ameaças lógicas e quatro ameaças relacionadas aos processos gerenciais. Por fim, verifica-se que a Biblioteca Central da UFPB necessita refletir sobre um plano de ação direcionado à segurança da informação, para a garantia de confidencialidade, integridade e salvaguarda das informações gerenciais críticas da organização. Com os resultados, espera-se contribuir com a Segurança da Informação no âmbito da Biblioteca Central da UFPB com uma proposta de minuta para Política de Segurança da Informação, permitindo novas contribuições para o desenvolvimento dos processos de gestão da Biblioteca Universitária.

Palavras-chave: Gestão da Segurança da Informação. Biblioteca Universitária. Política de Segurança da Informação. UFPB.

ABSTRACT

The information protection has become an extremely critical factor for organizations and Government entities. This involves not only the conventional environment, but also the technological and informational networking infrastructure. This study set out to address the information security as part of a University Library context. Even though a familiar environment with the information management processes, the libraries come suffering with problems related to lack of information on security management. For this purpose, this research studies the elements of information security management that allow the elaboration of a minute of information security policy for the Central Library of the Federal University of Paraíba. As the methodological aspects, is characterized as qualitative, descriptive type. As instrument methodology of data collection, tabulation and analysis, uses the Facilitated Process of risk analysis and assessment (FRAAP), which was supplemented with quiz and analysis of content according to Bardin. The results indicat a group of fifteen threats, among which detected nine physical threats, two logical threats and four threats related to processes. Finally, it was found that the Central Library of UFPB needs to reflect on an action plan directed to information security, to guarantee the confidentiality, integrity and safeguard of the organization's critical management information. With the results, it is expected to contribute with information security in the context of the Central Library of UFPB with the proposed minute information security policy, enabling new contributions to the development of the processes of management of the University Library.

Keywords: Information Security Management. University Library. Information Security Policy. UFPB.

LISTA DE SIGLAS E ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas

APF - Administração Pública Federal

BC - Biblioteca Central

BS - British Standards Institution

BU - Biblioteca Universitária

C&T - Ciência e Tecnologia

CAIS - Centro de Atendimento a Incidentes de Segurança

CCN - Catálogo Coletivo Nacional

CDN - Conselho de Defesa Nacional

CERT - Centro de Estudos, Resposta e Treinamento de Incidentes de Segurança no Brasil

CGSI - Comitê Gestor de Segurança da Informação

COBIT - Control Objectives for Information and Related Technology

CONSUNI - Conselho Universitário

DDC - Divisão de Desenvolvimento de Coleções

DDoS - Distributed Denial of Service

DNS - Domain Name System

DPT - Divisão de Processos Técnicos

DSU - Divisão de Assistência ao Usuário

GRC - Gestão da Governança, Risco e Conformidade

GSI - Gabinete de Segurança Institucional

GSI - Gestão da Segurança da Informação

GSIC - Gestão da Segurança da Informação e Comunicação

ICT - Informação em Ciência e Tecnologia

IEC - International Electrotechnical Commission

ISACA - Information Systems Audit and Control Association

ISMS - Information Security Management System

ISO - International Organization for Standardization

ITSEC -The Information Technology Security Evaluation Criteria

NSA - National Security Agency

NTP - Network Time Protocol

PDCA - Plan, Do, Check, Act (Planejar – Fazer – Checar – Agir)

PSI - Política de Segurança da Informação

PWC – PricewaterhouseCoopers

RNP - Rede Nacional de Ensino e Pesquisa

SegCiber - Segurança Cibernética

SGSI - Sistema de Gestão da Segurança da Informação

SI - Segurança da Informação

SIC - Segurança da Informação e Comunicação

SIGAA - Sistema Integrado de Gestão de Atividades Acadêmicas

SISTEMOTECA - Sistema de Bibliotecas da UFPB

SNBU - Seminário Nacional de Bibliotecas Universitárias

STI - Superintendência de Tecnologia da Informação

TCU - Tribunal de Contas da União

TI - Tecnologia da Informação

TIC - Tecnologia de Informação e Comunicação

UFPB - Universidade Federal da Paraíba

LISTA DE QUADROS

LISTA DE FIG URAS

SUMÁRIO

1 INTRODUÇÃO

A informação instantânea, que se vivencia na contemporaneidade, é marcada pela conectividade em um contexto evidenciado pelo uso intensivo e massivo das Tecnologias de Informação e Comunicação (TIC). Este fenômeno é marcado, também, pela grande produção de informação e conhecimento que impactam em todas as áreas do conhecimento e da sociedade. Isto se dá em decorrência da rápida expansão e crescimento da *Internet* – rede mundial de computadores – que, nas últimas décadas do século XX, e adentrando no século XXI, revela-se como canal de comunicabilidade. A *Internet* possibilitou a conexão em tempo real, de um sem números de computadores, e estes, muitas vezes, estão desprovidos de proteção, como sugere Silva, Araújo e Azevedo (2013, p. 2):

> Na sociedade da informação, com a difusão da Internet e o desenvolvimento das Tecnologias da Informação e Comunicação (TIC), as empresas se utilizam cada vez mais da rede mundial de computadores como principal canal para geração de negócios, ampliando, dessa forma, a possibilidade de incidentes no ciclo de vida da informação (criação, manuseio, armazenamento, transporte e descarte), podendo comprometer os resultados organizacionais.

Nota-se que, neste ambiente, os indivíduos estão mais expostos aos riscos e ameaças digitais, bem como à segurança dos sistemas, no ambiente organizacional. No planejamento organizacional, a segurança da informação tornou-se elemento crucial, como fator de preocupação no âmbito das instituições e governos, que empreendem esforços na articulação de processos gerenciais, com estratégias direcionadas a ações na busca de soluções que venham a garantir a salvaguarda de seus ativos (tudo que tem valor para a organização), na perspectiva de minimizar riscos e ameaças ao patrimônio, à integridade dos indivíduos, quer seja moral ou física, no ambiente organizacional e na sociedade como um todo.

A prática da segurança é responsabilidade de todos os profissionais envolvidos na organização. Tem como objetivo principal a garantia de continuidade das operações e competitividade no mercado que a organização atua, bem como a proteção dos seus ativos. A missão da segurança organizacional se caracteriza, conforme Gil (1995, p. 12), por “prover sintonia aos ativos tangíveis e intangíveis organizacionais, quanto à eficácia dos resultados e da eficiência dos processos, para alcance da qualidade total das linhas de negócios [...]”.

No que diz respeito ao campo da segurança da informação, nota-se nas organizações, que esta não é matéria menos importante, pois cada vez mais dependem da informação.

Belarmino e Araújo (2014, p. 7) asseveram que “o recurso informacional é um bem precioso para pessoas, empresas, organizações e instituições, constituindo uma mercadoria indispensável principalmente para o processo de tomada de decisões”.

No contexto contemporâneo, os ataques à Segurança da Informação (SI) tornam-se mais sofisticados, forçando as organizações a pensar estratégias de ações direcionadas à Gestão da Segurança da Informação (GSI) que, aliadas aos seus objetivos e metas, possam melhorar seu desempenho e garantir competitividade.

Na visão de Manoel (2014, p. 57): “A Gestão da Segurança da Informação tem por objetivo o planejamento, a execução e a monitoração das atividades de SI, e a aplicação de processos de melhoria contínua”. Isto corrobora com Fontes (2006, p. 11), que a descreve como: “conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada”.

Uma proteção eficaz e eficiente da informação dependerá, acima de tudo, de uma real compreensão dos conceitos e regulamentos de segurança por parte dos indivíduos participantes da organização que estejam imbuídos de consciência e compromisso com a Segurança da Informação no ambiente organizacional. Cada pessoa na organização tem a responsabilidade de proteger a informação (FONTES, 2006). Isto converge para a elaboração da Política de Segurança da Informação, que se refere a “um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos” (TRIBUNAL DE CONTAS DA UNIÃO - TCU, 2012, p. 10). Tais princípios estabelecem diretrizes que determinarão o caminho que a instituição deverá seguir, de modo a garantir a salvaguarda dos recursos informacionais, computacionais e humanos.

A problemática da Segurança da Informação emerge do cenário de mudanças alavancadas pelo desenvolvimento e expansão das TIC. Surge, com isto, a necessidade imperativa da biblioteca alinhar suas práticas gerenciais aos princípios que contemplem a Gestão da Segurança da Informação, não só nos aspectos que envolvem o uso seguro dos recursos tecnológicos, mas também no uso da informação no ambiente organizacional.

Entende-se que a Biblioteca Central (BC) da Universidade Federal da Paraíba (UFPB), enquanto organização educacional e gestora dos registros do conhecimento, necessita inserir-se no contexto de proteção dos seus ativos de informação, no desenvolvimento de ações que alinhem seus processos administrativos aos aspectos relacionados à Gestão da Segurança da Informação (GSI), com vistas ao compromisso de prática efetiva e consciente de uma cultura

de Segurança da Informação que envolva, de forma integrada, os aspectos de pessoa, processos e tecnologia.

Nesta perspectiva, a Universidade Federal da Paraíba (UFPB), por meio da Resolução 32/2014 (UFPB, 2014) do Conselho Universitário (CONSUNI), institui a sua Política de Segurança da Informação (PSI) da UFPB. O Capítulo I (Objeto) traz, no seu Art. 1º, o seguinte: "Fica estabelecida a Política de Segurança da Informação (PSI) da Universidade Federal da Paraíba (UFPB), contendo as diretrizes de segurança da informação a serem observadas no âmbito desta Universidade". O Parágrafo Único, do referido Capítulo, afirma: "As diretrizes estabelecidas na PSI/UFPB determinam as bases a serem seguidas pela UFPB com relação à segurança dos recursos de tecnologia da informação (TI) e informações geradas na UFPB". Já o Art. 2º, afirma que: "A PSI consiste em um quadro de referência contendo princípios que norteiam a Gestão da Segurança da Informação e que devem ser observados por professores, alunos, servidores e demais usuários que interagirem com os "ativos" de TI da UFPB" (UFPB, 2014, p. 3).

Diante do exposto, entende-se que é relevante uma PSI para a BC da UFPB uma vez que, enquanto unidade de informação, a BC está diretamente ligada às transformações e desafios gerados pelas TIC uma vez que ainda não contempla, em suas rotinas, práticas formalizadas de Segurança da Informação que permitam integrar-se ao contexto de proteção da informação, tanto no ambiente organizacional, quanto no ambiente tecnológico e digital. Assim, formulou-se a seguinte questão: **Como ordenar elementos de Gestão de Segurança da Informação em uma Política de Segurança para uma biblioteca universitária?**

A partir da questão de pesquisa, tem-se como objetivo geral: **Analisar os elementos de Gestão da Segurança da Informação que permitam a elaboração de uma minuta de Política de Segurança da Informação para a Biblioteca Central da UFPB**. Para atender a este propósito, estabeleceram-se os seguintes objetivos específicos:

- diagnosticar os aspectos de gestão de segurança da informação no ambiente da BC/UFPB;
- mapear riscos, vulnerabilidades e ameaças à Segurança da Informação na BC/UFPB;
- elaborar uma minuta de política para gestão da segurança da informação adaptada as necessidades da BC.

As motivações que levaram a este estudo estão relacionadas à observações empíricas do pesquisador, que atua como bibliotecário da Instituição UFPB e pôde, desse modo, colher

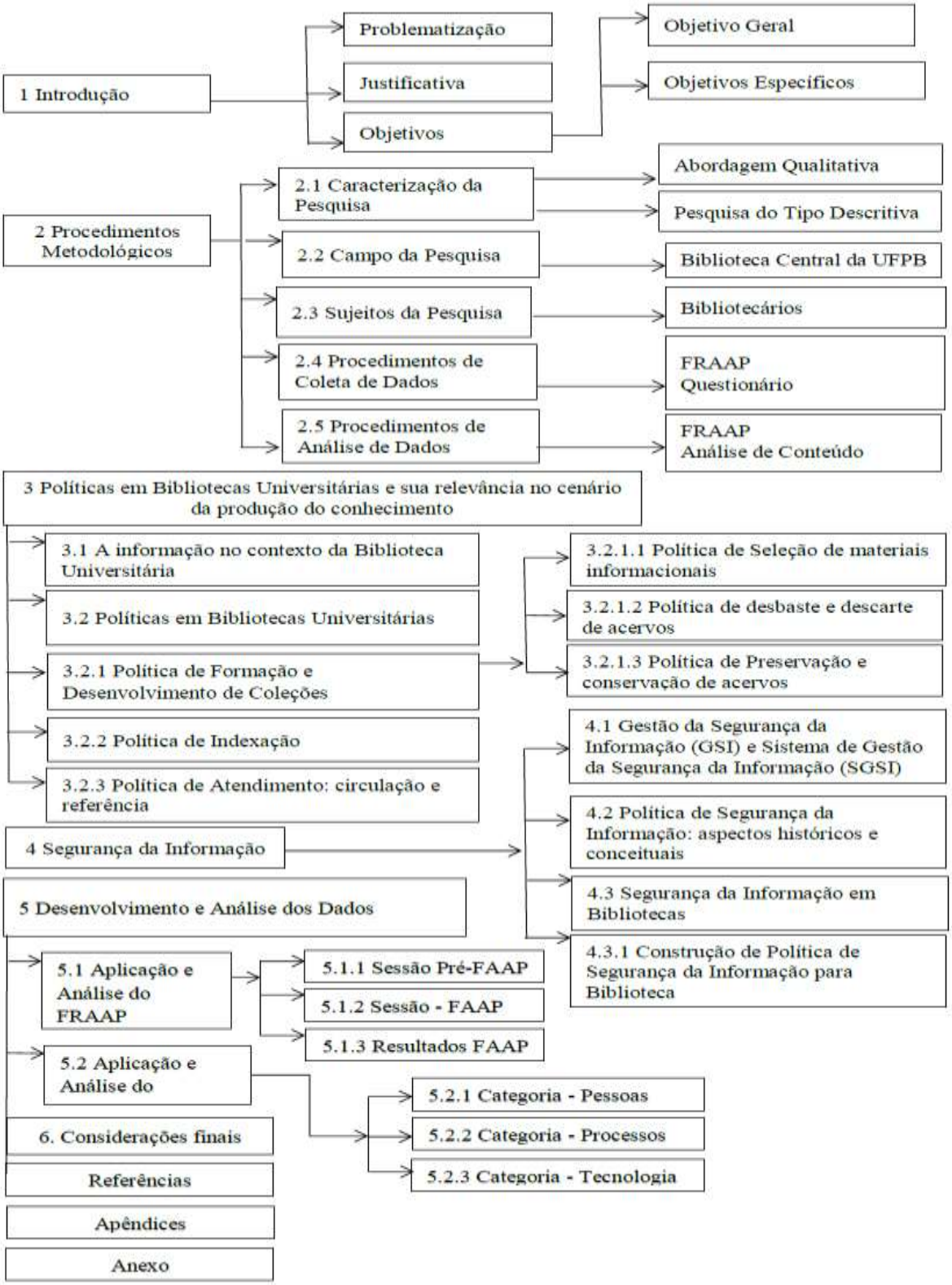
as experiências vivenciadas no cotidiano profissional como gestor de biblioteca universitária pública e interações com os colegas bibliotecários, colegas de trabalho e também durante o curso na disciplina Gestão de Segurança da Informação (Seminário I), no Programa de Pós-Graduação Mestrado Profissional em Gestão nas Organizações Aprendentes da UFPB, ministrada pelo Prof. Dr. Wagner Junqueira de Araújo. O estudo da disciplina despertou no pesquisador a percepção da relevância que a Segurança da Informação exerce, não só no que se refere ao aspecto pessoal, mas ao seu cotidiano profissional.

A pesquisa em pauta traz uma abordagem da Gestão da Segurança da Informação com a intenção de subsidiar ações voltadas ao planejamento de SI com foco na elaboração de uma minuta de Política de Segurança da Informação adaptada ao contexto organizacional da Biblioteca Central da UFPB.

Entende-se que a construção de um conjunto de políticas, diretrizes, procedimentos e normas de segurança da informação em bibliotecas é condição essencial, dado os avanços necessários para qualquer organização, uma vez que um alinhamento dos objetivos da organização a um sistema de gestão de segurança da informação irá minimizar a exposição aos riscos e ameaças relacionados à SI.

No que diz respeito aos aspectos metodológicos, esta pesquisa se caracteriza como qualitativa e utiliza a técnica de pesquisa descritiva. Como instrumento metodológico de coleta de dados, tabulação e análise, adotou o *Facilitated Risk Analysis and Assessment Process (*FRAAP) ou Processo Facilitado de Análise e Avaliação de Risco, que foi complementado com questionário e a análise de conteúdo conforme Bardin. Esta pesquisa está estruturada em 6 seções, além das referências, apêndices e anexo. A Figura 1 representa a estrutura da pesquisa.

Figura 1 – Estrutura da Pesquisa



Fonte: Elaborada pelo autor (2017).

A primeira seção constitui-se da Introdução, compondo-se da problematização, justificativa, objetivo geral e objetivos específicos. A segunda seção traz os Procedimentos

Metodológicos, com a caracterização da pesquisa, campo da pesquisa, sujeitos da pesquisa, procedimentos de coleta de dados e procedimentos de análise. A terceira seção discorre sobre a temática Políticas em bibliotecas universitárias, discute sobre a relevância da Biblioteca Universitária (BU) no contexto da construção do conhecimento, apresentando aspectos históricos e conceituais, busca discutir sobre a evolução das políticas de informação no desenvolvimento da BU.

A quarta seção aborda a temática da Segurança da informação, discute ainda os aspectos relacionados a Gestão da Segurança da Informação no contexto das organizações, Segurança da Informação em biblioteca e construção de Políticas de Segurança da Informação para biblioteca.

A quinta seção apresenta o desenvolvimento da pesquisa que trata da Coleta e Análise dos Dados, aplicação e análise do FRAAP e aplicação e análise do questionário, dividido nas categorias: pessoas, processos e tecnologia. Por fim, as Considerações Finais, Referências, Apêndices e Anexo.

2 PROCEDIMENTOS METODOLÓGICOS

Nesta seção, levanta-se o caminho percorrido para atingir os objetivos da pesquisa.

2.1 CARACTERIZAÇÃO DA PESQUISA

Conforme Marconi e Lakatos (2013, p. 43), “a pesquisa pode ser considerada um procedimento formal com método de pensamento reflexivo que requer um tratamento científico [...]”, é um caminho que leva ao conhecimento de uma realidade ou descoberta de uma verdade parcial. Vai mais além da procura de uma verdade, pois se constitui na busca de resposta à questões formuladas, em que se utiliza métodos científicos.

Desse modo, esta pesquisa tem uma abordagem qualitativa, do tipo descritiva, tendo como fontes de informação para compor o *corpus* teórico a pesquisa documental e bibliográfica, segue as orientações do método *Facilitated Risk Analysis and Assessment Process* (FRAAP) ou Processo Facilitado de Análise e Avaliação de Risco que usa como procedimentos de coletas de dados questionário e reunião dirigida. Para análise e tratamento dos dados, se utilizou orientações do FRAAP e análise de conteúdo de acordo com Bardin.

A pesquisa descritiva tem como objetivo “escrever as características de um objeto de estudo”. A exemplo das “que atualizam as características de um grupo social, nível de atendimento do sistema educacional, como também aquelas que pretendem descobrir a existência de relações entre variáveis” (GONÇALVES, 2001, p. 65). Segundo o autor, ela visa ao atendimento dos objetivos a que a pesquisa se propõe e está ligado ao seu objeto.

Para compor o *corpus* teórico, utilizou-se as técnicas da pesquisa documental e bibliográfica. A técnica documental viabiliza a fundamentação teórica baseada em fontes primárias que “são aquelas de primeira mão, provenientes dos próprios órgãos que realizam as observações” (MARCONI; LAKATOS, 2013, p. 43).

A técnica bibliográfica por sua vez, segundo Marconi e Lakatos (2013, p. 43): “Trata-se de levantamento de toda a bibliografia já publicada, em forma de livros, revistas publicações avulsas e imprensa escrita”. Estes materiais são denominados de fontes secundárias. E foram utilizados para construção dos capítulos de revisão desta dissertação.

2.2 CAMPO DE PESQUISA

O campo de pesquisa é a Biblioteca Central, em específico a Direção, Vice-Direção, Divisão de Serviço ao Usuário (DSU), Divisão de Processos Técnicos (DPT), Divisão de Desenvolvimento das Coleções (DDC), Seção de Periódicos, Portal de Periódicos da Capes, Seção de Bases Digitais (SBD). Estas, por sua vez, comporam o universo de análise dos dados.

A Biblioteca Central situa-se no Campus I, João Pessoa - PB, é o órgão suplementar, vinculado à Reitoria da UFPB, e responsável pelo SISTEMOTECA (Composto por 17 Bibliotecas Setoriais - distribuídas entre quatro *Campi)*. Sua formação administrativa compõe-se de: Diretoria, Vice-Diretoria, Secretaria; Contabilidade, três Divisões, subdivididas em doze Seções.

Segundo Cunha (2014), a criação da Biblioteca Central se deu em 1961, inicialmente em uma sala do Instituto de Matemática, mas de forma improvisada. Posteriormente, se transferiu para a Biblioteca da Escola de Engenharia, em seguida para o prédio da Faculdade de Educação e, finalmente, se instalou em um prédio anexo da Reitoria. Pela ocasião, em 1967, da primeira etapa de edificação do Campus João Pessoa, é dado o passo inicial de construção das instalações da BC, tendo como idealizador do projeto de Estruturação da Biblioteca Central Edson Nery da Fonseca, sob o título “Teoria da Biblioteca Central. ” Só no final de 1976, é dado início ao processo de estruturação e implantação da Biblioteca Central, composta pela junção do acervo das 13 bibliotecas setoriais. Na sequência, surgiram ações voltadas para a contratação de profissional bibliotecário, atualização de acervos, automação dos processos técnicos, elaboração e aprovação de regimento para o Sistema de Bibliotecas, criação de novos serviços.

Estes acontecimentos impulsionaram a construção definitiva do prédio atual da Biblioteca Central, compreendendo uma área de 8.500m² e, em 1980, é aprovado pelo CONSUNI, através da resolução 201/1980, o primeiro regulamento do Sistema de Bibliotecas da UFPB. Após mais de 20 anos, é elaborado um novo regulamento do Sistema de Bibliotecas e aprovado pelo CONSUNI, através da resolução 31/2009. A partir de então, o Sistema de Bibliotecas é definido como um conjunto de bibliotecas integradas configurando-se nos aspectos funcional e operacional com vistas à unificação e harmonização das atividades voltadas às áreas educacionais, científicas, tecnológicas e culturais da UFPB, pautadas no apoio aos programas de ensino, pesquisa e extensão, através do desenvolvimento de ações que permeiam a coleta, armazenagem, recuperação e disseminação da informação.

De acordo com o Regimento Interno (2009, p. 9), a Biblioteca Central mantém órgão de direção superior com as seguintes denominações: Divisões e Seções, conforme Quadro 1.

Quadro 1 - Divisões e Seções da Biblioteca Central

DIVISÃO DE SERVIÇO AO USUÁRIO (DSU)	**Seção de Referência (SRE)** • Acervo nas diversas áreas do conhecimento (para consulta); • Cadastro de usuários; • Orientação aos usuários no acesso à informação; • Orientação aos usuários na consulta e uso do acervo.
	Seção de Circulação (SCI) • Organização e manutenção de empréstimo do material documental; • Organização do material documental nas estantes e leitura de estantes; • Organização do espaço de leitura e controle de entrada e saída de pessoas na BC; • Reposição do material documental nas estantes e outros.
	Seção de Periódicos (SPE) • Acervo de periódicos científicos nas diversas áreas do conhecimento; • Organização do acervo documental de periódicos científicos; • Atualização dos dados para o Catálogo Coletivo Nacional de Publicações Seriadas; • Portal da Capes.
	Seção de Coleções Especiais (SCE) • Acervo de Dissertações e Teses; • Coleção Paraibana; • Coleção Brasiliana.
	Seção de Multimeios (SMU) • Coleção de acervo audiovisual; • Coleção de mídias (CD; DVD – Dissertações e Teses).
	Seção de Bases Digitais (SBD) • Coleção da produção científica da UFPB (Dissertação e Teses); • Comut (Comutação Bibliográfica); • Serviços de Cooperação para Acesso a Documentos (SCAD/BIREME); • Indexação e atualização de documentos nas Bases de Dados; • Atividades pertinentes à disseminação da informação.
	Seção para Desenvolvimento da Leitura (SDL) • Acervo de obras didáticas e paradidáticas; • Promoção do hábito de leitura para crianças e adolescentes; • Orientação dos usuários na pesquisa escolar.
	Seção de Inclusão para Usuários com Necessidades – Seção Braille • Disponibiliza acervo impresso em Braille para usuários com deficiência visual.

<table>
<tr><td rowspan="1">DIVISÃO DE DESENVOLVIMENTO DAS COLEÇÕES (DDC)</td><td>Seção de Seleção (SSE)
Seleção do material documental;
Comunicação com Editoras para aquisição de material documental e bases de dados digitais;</td><td>Seção de Compra (SCO)
Aquisição de material documental e bases digitais através de compra.</td><td>Seção de Intercâmbio (SIN)
Atualização de cadastro de órgãos que mantêm intercâmbio com o Sistemoteca;
Obtenção e/ou intercâmbio de material por doação ou permuta;</td></tr>
<tr><td rowspan="2">DIVISÃO DE PROCESSOS TÉCNICOS (DPT)</td><td colspan="3">Seção de Catalogação e Classificação (SCC)
Organização do acervo (Catalogação, Classificação e Indexação);
Automação do acervo;
Elaboração da catalogação na fonte das dissertações e teses defendidas na UFPB;
Elaboração de manuais e códigos que contenham as normas gerais de rotinas específicas do processamento técnico fixando o grau de centralização dos trabalhos de catalogação e do controle técnico perante as bibliotecas setoriais do SISTEMOTECA;</td></tr>
<tr><td colspan="3">Seção de Manutenção do Patrimônio Documental (SMD)
Organização dos registros de entrada do material documental;
Serviço de conservação e restauração do material documental;
Orientação e controle da Sinalização da biblioteca;
Estabelecimento de normas e procedimentos padrões para uso nas bibliotecas do SISTEMOTECA, especificando material, inscrição, letras e outros detalhes, visando à uniformidade possível das encadernações, pastas, caixas e outros envoltórios e suportes para as coleções;
Reparações de pequena montagem do material documental;
Promoção da desinfecção periódica das coleções.</td></tr>
</table>

Fonte: Adaptado para quadro com base no Regimento Interno da Biblioteca Central da UFPB (2009).

Tais Divisões possuem um diretor designado pelo Reitor, indicado pela direção da BC e as Seções possuem um chefe designado pela direção da BC, indicado pelo diretor de Divisão. À época em que foi realizada a pesquisa, realizavam-se reuniões para a restruturação do Regimento interno da BC. Algumas Seções foram extintas, outras aglutinadas a Seções cujo acervo tenha pertinência. Até o término desta pesquisa, o Regimento Interno ainda não havia sido submetido ao CONSUNI.

2.3 SUJEITOS DA PESQUISA

Num universo de 31 bibliotecários da Biblioteca Central da UFPB, foram incluídos na pesquisa oito sujeitos: diretor, vice-diretor, três diretores de Divisões e três gestores de Seção.

Esses sujeitos foram selecionados por estarem envolvidos diretamente no processo de geração, processamento, acesso, recuperação, uso e disseminação da informação.

2.4 PROCEDIMENTOS DE COLETA DE DADOS

Os instrumentos de coleta de dados são orientados pelo *Facilitated Risk Analysis and Assessment Process* (FRAAP) ou Processo Facilitado de Análise e Avaliação de Risco, que usa questionário e reunião dirigida.

A elaboração das questões do questionário seguiu orientações da Escala de Likert, que trata de "uma escala de classificação amplamente utilizada, exigindo que os entrevistados indiquem um grau de afirmações sobre objetos de estímulo" (VIEIRA, 2011, p. 36). As questões foram elaboradas em enunciados, de forma que os participantes pudessem exprimir sua opinião ou atitude, apontando um dos itens acerca da temática SI: concordância, indiferença ou discordância, numa escala de: Concordo fortemente (muito), Concordo (parcialmente), Indiferente (neutro), Discordo (parcialmente), Discordo fortemente (muito).

Elaborou-se 23 questões relacionadas à Segurança da Informação, que compreendem as categorias pessoas, processos e tecnologia. As questões relacionadas ao aspecto pessoas, visam obter informações acerca da percepção e comportamento dos respondentes em relação à Segurança da Informação. Nos aspectos que correspondem a processos e tecnologia, objetiva-se verificar as práticas em segurança da informação.

Para a reunião dirigida, foi agendado um dia com os 8 (oito) participantes da pesquisa, em que se aplicou a metodologia do FRAAP. De acordo com Peltier (2005, tradução nossa), tem como objetivo assegurar que as informações referentes à segurança dos riscos nas operações de negócios sejam consideradas e documentadas, e isto envolve análise de sistema, aplicações e processos de negócios da organização. É uma metodologia aplicada por meio do apoio dos próprios participantes da organização, gestores familiarizados com as necessidades e missão da organização.

A aplicação do questionário foi feita durante a reunião FRAAP, com os 8 (oito) profissionais bibliotecários gestores da BC, que compõe a amostra, os quais são: o diretor e vice-diretor da Biblioteca; os diretores das respectivas Divisões: Divisão de Desenvolvimento das Coleções (DDC), Divisão de Processos Técnicos (DPT)**,** Divisão de Serviço ao Usuário (DSU); o gestor do Portal de Periódicos Eletrônicos da Coordenação de Aperfeiçoamento de

Pessoal de Nível Superior (CAPES), gestor da Seção de Bases de Digitais e gestor da Sessão de Periódicos.

O FRAAP divide-se em três fases: Pré-FRAAP (preparação do processo para priorizar as ameaças – preparação do material), sessão FRAAP (equipe debate e identifica as potenciais ameaças à integridade, confidencialidade e disponibilidade), os resultados do FRAAP (um conjunto de documentos que irá identificar ameaças, priorizar essas ameaças em níveis de risco e identificação de controles que ajudarão a mitigar os riscos a níveis aceitáveis).

Este método se adapta bem às instituições sem fins lucrativos, como é o caso da pesquisa em pauta. Permite, por meio do processo de avaliação de riscos, analisar ameaças que poderão causar impacto aos processos organizacionais.

Desse modo, a análise de risco se divide em três etapas: identificar as ameaças, estabelecer o nível de risco e selecionar os controles.

Após o processo de identificação das ameaças, foi feita a classificação destas em Alta, Média ou Baixa, considerando a probabilidade de ocorrência destas ameaças, de acordo com o Quadro 2 (Definições de Probabilidade FRAAP), a seguir:

Quadro 2 – Definições de Probabilidade FRAAP

Termo	Definição
Possibilidade	Probabilidade de que um evento irá acontecer ou que um valor de perda específica pode ser alcançado no caso de o evento ocorrer
Alto	Muito provável que a ameaça ocorrerá no próximo ano
Médio	Possível que a ameaça possa ocorrer no próximo ano
Baixo	Altamente improvável que a ameaça ocorrerá no próximo ano

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

Uma segunda classificação foi efetuada para avaliar o impacto (Alto, Médio, Baixo) causado à organização, de acordo com o Quadro 3 (Definições de Impacto FRAAP), a seguir:

Quadro 3 - Definições de Impacto FRAAP

Termo	Definição
Impacto	Uma medida da magnitude da perda ou danos no valor de um ativo
Alto	Missão inteira ou negócios são impactados
Médio	A perda é limitada a uma única unidade de negócio ou objetivo
Baixo	Negócios, como sempre

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

Com base nas classificações, elaborou-se uma tabela, conforme o Quadro 4 (Estrutura do FRAAP para Ameaças), onde são atribuídos, tanto para probabilidade quanto para

impacto, valores de 1 a 3, em que 1 corresponde a Baixo, 2 Médio e 3, Alto. A coluna que corresponde ao "Nível de Risco" (Quadro 4) deve totalizar a soma dos valores para cada ameaça classificada, conforme a probabilidade e o impacto.

Quadro 4 – Estrutura do FRAAP para Ameaças

Ameaça	Aplicação Sim/Não	Probabilidade 1= Baixa 2= Média 3 = Alta	Impacto 1= Baixo 2 = Médio 3 = Alto	Nível de Risco	Seleção de controles
Falta de pessoal – chave (Escassez de recursos humanos capacitados/qualificados para exercer as funções/ atividades)					
Falta de capacitação no uso das TICs					
Vazamento de água/falha de encanamento/goteira					
Falha de rede elétrica (Problemas parte elétrica – instalações)					
Ausência de manutenção predial (Estrutura física precária; ausência de controle de pragas)					
Ausência de câmeras de segurança					
Ameaças ambientais (Fungos, incêndio, falta de climatização, umidade elevada, falha de ar-condicionado)					
Falta de higienização do acervo					
Controle de acesso físico (Ausência de controle de acesso físico a determinados setores)					
Ruídos na comunicação (Conversas paralelas – problemas de comunicação)					
Sinalização precária na Biblioteca					
Invasão de *hacker*					
Cópias de segurança (Falta *backup*)					
Cabeamento de rede exposto (Estrutura lógica**)**					
Obsolescência tecnológica					

Fonte: Adaptado de Peltier (2005, p. 208, tradução nossa).

A partir da aplicação do total de valores no Quadro 4, foi encontrado a matriz de risco de cada ameaça, a qual a organização está exposta (Quadro 5):

Quadro 5 – Matriz do Nível de Risco

	IMPACTO		
	Alto	Médio	Baixo
Alta	**A (**5**)**	**B (**4**)**	**C**
Média	**B (**4**)**	**B (**4)	**C**
Baixa	**C**	**C**	**D**
PROBABILIDADE	A – Ação corretiva precisa ser implementada; B – Ação corretiva deve ser implementada; C – Requer monitoramento; D – Nenhuma ação é necessária no momento.		

Fonte: Peltier (2005, p. 174).

Após a etapa de identificação da matriz de risco relacionada a cada uma das ameaças detectadas, seguiu-se a seleção de controles que a organização deverá implantar. O FRAAP sugere uma lista de controles para o processo de mitigação dos riscos, conforme Quadro 6 (Conjunto de Controles sugeridos pelo FRAAP):

Quadro 6 – Conjunto de Controles sugeridos pelo FRAAP

Nº do Controle	Grupo	Descrição	Definição
1	Operações controles	Cópia de segurança	Os requisitos de cópia de segurança serão determinados e comunicadas as operações, incluindo um pedido de notificação electrónica que as cópias de segurança foram concluídas e enviadas e aplicadas ao sistema pelo administrador. As operações serão solicitadas para testar os procedimentos de cópia de segurança.
2	Operações de controles	Plano de recuperação	Desenvolver, documentar e testar procedimentos de recuperação projetados para garantir que o plicativo e as informações possam ser recuperados, usando as cópias de seguranças criadas, em caso de perda.
3	Operações de controles	Análise de risco	Realizar uma análise de risco para determinar o nível de exposição de ameaças identificadas e identificar possíveis salvaguardas ou controles.
4	Operações de controles	Antivírus	(1) Assegurar que a área local administrador de rede (LAN) instale o padrão corporativo de Antivírus em todos os computadores. (2) Formação e sensibilização para Técnicas de prevenção de vírus a ser incorporados na organização para Proteção Informação (PI).
5	Operações de controles	Dependências de interface	Os sistemas que fornecem informações serão identificados e comunicados a salientar o impacto para a funcionalidade se estas aplicações de alimentação não estiverem disponíveis.
6	Operações de controles	Manutenção	Requisitos de tempo para manutenção serão monitorados e um pedido de ajustamento será comunicado à gerência se a experiência garantir.

7	Operações de controles	Contrato de nível de serviço	Adquirir acordos de nível de serviço para estabelecer o nível de expectativas do cliente e garantias de operações de apoio.
8	Operações de controles	Manutenção	Adquirir acordos de manutenção e fornecedores para facilitar o status operacional contínuo do aplicativo.
9	Operações de controle	Gestão da Mudança	Controles de migração de produção, como processos de busca e remoção, para garantir que os armazenamentos de dados estejam limpos.
10	Operações de controles	Análise de impacto nos negócios	Uma análise de impacto empresarial formal será conduzida para determinar a criticalidade relativa do ativo com outros ativos da empresa.
11	Operações de controles	Cópia de segurança	Treinamento para cópia de segurança fornecido pelo Administrador do sistema e deveres alternados entre eles para assegurar a adequação do programa de treinamento.
12	Operações de controles	Cópia de segurança	Um programa formal de segurança para conscientização do funcionário. Implementado, atualizado e apresentado aos empregados anualmente.
13	Operações de controles	Plano de recuperação	Implementar um mecanismo para limitar o acesso a informações confidenciais a redes específicas ou locais físicos.
14	Operações de controles	Análise de risco	Implementar autenticação de usuário mecanismos (tais como firewalls, controles dial-in, ID seguro) paral limitar o acesso das pessoas.
15	Aplicação de controles	Aplicação ao controle	Projetar e implementar controles de aplicativos (verificação de edição de entrada de dados, campos validação, indicadores de alarme, capacidades de expiração de senha, somas de verificação) para garantir a integridade, confidencialidade e disponibilidade das informações da aplicação.
16	Aplicação de controle	Teste de aceitação	Desenvolver os rocedimentos de teste a serem seguidos durante o desenvolvimento e durante modificações no aplicativo existente que incluem participação e aceitação.
17	Aplicação de controle	Treinamento	Implementar programas de utilizador (avaliações de desempenho dos utilizadores) concebidos em conformidade com as políticas e procedimentos em vigor para assegurar a utilização adequada da aplicação.
18	Aplicação de controle	Treinamento	Os desenvolvedores de aplicativos devem fornecer documentação, orientação e apoio ao pessoal de operações (operações) implementar mecanismos para assegurar que a transferência de informações entre aplicações seja segura.
19	Aplicação de controle	Estratégias corretivas	A equipe de desenvolvimento deve desenvolver estratégias corretivas tais como processos reformulados, lógica de aplicação revisada, etc.
20	Controles de segurança	Controles de segurança	Desenvolver políticas e procedimentos para limitar o acesso e privilégios operacionais àqueles com necessidades comerciais.
21	Controles de segurança	Treinamento	O treinamento de usuário incluirá instruções e documentação sobre o uso correto do aplicativo. A

			importância de manter a confidencialidade das contas de usuários, senhas, e a natureza confidencial e competitiva da informação será enfatizada.
22	Controles de segurança	Rever	Implementar mecanismos para monitorar, reportar e auditar as atividades identificadas como revisões independentes, incluindo revisões periódicas de IDs de usuários para verificar as necessidades empresariais.
23	Controles de segurança	Classificação de ativos	O ativo em análise será classificado de acordo com as políticas, normas e procedimentos de classificação de ativos.
24	Controles de segurança	Controle de acesso	Serão determinados e implementados mecanismos para proteger o banco de dados contra acesso não autorizado, e modificações feitas fora do aplicativo.
25	Controles de segurança	Suporte da gestão	Solicitar apoio da gestão para garantir a cooperação e coordenação de várias unidades de negócios.
26	Controles de segurança	Propriedade	Os processos estão em vigor para garantir que os ativos de propriedade da empresa são protegidos e que a empresa esteja em conformidade com todos os acordos de licença de terceiros.
27	Controles de segurança	Sensibilização para a segurança	Implementar um mecanismo de controle de acesso para impedir o acesso não autorizado à informação. Esse mecanismo incluirá a capacidade de detectar, registrar e relatar tentativas de violar a segurança dessas informações.
28	Controles de segurança	Controle de acesso	Implementar mecanismos de criptografia (dados, de ponta a ponta) para impedir o acesso não autorizado para proteger a integridade e a confidencialidade das informações.
29	Controles de segurança	Controle de acesso	Aderir a um processo de gestão da mudança concebido para facilitar uma abordagem estruturada às modificações da aplicação, para garantir que as
30	Controles de segurança	Controle de acesso	Existem procedimentos de controle para assegurar que os logs do sistema apropriados sejam revisados por terceiros independentes para revisar as atividades de atualização do sistema.
31	Controles de segurança	Controle de acesso	Em consulta com a administração das instalações, facilitar a implementação de Controles de segurança projetados para proteger as informações, software e hardware do sistema.
32	Sistemas de controles	Mudança de Gestão	Os requisitos de cópia de segurança serão determinados e comunicados às operações, incluindo uma solicitação de notificação eletrônica de que os backups foram concluídos, seja enviada ao administrador do sistema do aplicativo. As operações serão solicitadas para testar os procedimentos de cópia de segurança.
33	Sistemas de controles	Monitor de Logs do sistema	Desenvolver Logs do sistema, documentar e testar procedimentos de recuperação e assegurar que a aplicação e as informações possam ser recuperadas, usando cópias de seguranças criadas, em caso de perda.

34	Segurança física	Segurança física	Conduzir uma análise de risco para determinar o nível de exposição a ameaças identificadas e identificar possíveis salvaguardas ou controles.

Fonte: Peltier (2005).

Como parâmetro para identificação das potenciais ameaças à SI no âmbito da BC/UFPB, baseou-se também na "Árvore de ameaças" de Shahri e Ismail (2012) no processo de classificação das ameaças, uma vez que a mesma sugere um conjunto de possíveis ameaças que se assemelham e se complementam com as sugeridas por Peltier (2005) para a identificação do nível de riscos, identificação dos ativos de informação e detecção das vulnerabilidades, com vistas a seleção de controles para mitigação dos riscos relacionadas à segurança da informação na BC/UFPB.

Para Shahri e Ismail (2012, p. 169, tradução nossa): "Ao compreender as ameaças à segurança das informações [...], a organização pode proteger melhor seus ativos de informação e fortalecer o nível de proteção da informação [...]". Desse modo, as ameaças fornecem um conjunto de controles para diminuição dos riscos relacionados à exploração de vulnerabilidades. Shahri e Ismail (2012, tradução nossa) apresentam uma lista de possíveis ameaças, conforme Quadro 7:

Quadro 7 – Lista de Ameaças

1. Falta de energia / perda;
   1.1. Falta de energia do servidor;
   1.2. Falta de energia da estação de trabalho;
2 Vazamento de água / falha de encanamento / Goteira;
3 Sabotagem física / ou danos intencionais, incêndio culposo;
4 Erros de Usuário;
   4.1. Erros do usuário na utilização dos ativos de software;
   4.2. Mascarando a Identidade do Usuário;
   4.3. Uso não autorizado de um aplicativo;
   4.4 Divulgação acidental de informações;
5 Falta de pessoal-chave;
6 Ameaças ambientais;
   6. 1 danos causados pela água;
   6. 2 fogos, falha de ar-condicionado;
   6. 3 poluições;
7 Erro de manutenção;
   7.1 Ferragens;
   7.2 Software;
   7.3 Redes;
8 Roubo de equipamentos;
9 Falha de software ou erros;
   9.1 Introdução de software prejudicial ou perturbador;
   9. 2 Sistema de falhas de software;
   9.3 Rede e falha de softwares;

9.4 Erros, problemas de códigos, brechas desconhecidas;
10 Obsolescência tecnológica;
11 Falta de Política Organizacional, Inadequada, Incompleta ou Planejamento;
12 Falta de Controles ou Inadequados ou Incompletos;
13. Ato deliberado de roubo de dados;
13.1. Roubo / perda de dado de cliente ou proprietário de informação;
13.2. Confisco ilícito de equipamentos ou informações;
13.3. Dumping arquivos físicos com informações críticas em público;
14. Uso indevido de recursos do sistema;
14.1. Terceiro;
14.2. Extorsão de informação;
15. Comunicação não autorizada;
16. Base de Dados de acesso à informação não autorizado;
Contínuo;
17. Escassez de pessoal;
18. Erros de Usuário;
18.1. Erros do usuário na utilização dos ativos de software;
18.2. Mascarando a Identidade do Usuário;
18.3. Uso não autorizado de um aplicativo HIS;
18.4. Divulgação acidental de informações;
18.5. Informações Confidenciais de Email para um Endereço Incorreto;
18.6. Entrada acidental Dados incorretos por funcionários;
19. Sabotagem ou dano intencional;
21. Ameaças Ambientais;
21.1. Danos causados pela água;
21.2. Fogo;
21.3. Falha de Ar-Condicionado;
21.4. Poluição;
21.5. Produtos químicos;
21.6. Vazamento de Líquido;
22. Desvios na qualidade de serviço;
22.1. Desvios de QoS dos provedores de serviços;
22.2. Ataques deliberados de software;
22.2.1. Tentativa proposital de burlar segurança do sistema;
22.2.2. Tentativa maliciosa de obter acesso não autorizado;
22.2.2.1. Senha Sniffing;
22.2.2.2. Telecom Eavesdropping;
22.2.2.3. Ataque de banco de dados;
22.2.2.4. Negação de serviço;
22.2.2.5. Desfiguração de sites;
22.2.2.6. Bots;
22.2.2.7. Ataques de DNS;
22.2.2.8. Ataque de Malware;
22.2.2.8.1. Worm;
22.2.2.8.2. Cavalos de Tróia;
22.2.2.8.3. Spyware;
22.2.2.8.4. Vírus;
22.2.2.8.5. Adware;
22.2.2.8.6. Macros;
23. Erro de Manutenção;
23.1. Hardware;
23.2. Programas;
23.3. Rede;
24. Uso indevido do aplicativo Web;
24.1. Cross Site Scripts;

24.2. Vazamento de informações; 24.3. Injeção SQL; 24.4. Divisão de Resposta HTTP; 25. Compromissos com a Propriedade Intelectual; 26. Política Organizacional ou Planejamento Falta, Inadequado ou Incompleto; 27. Controles Falta, Inadequado ou Incompleto; 28. Fraude Financeira; 29. Terrorismo; 30. Roubo de Equipamento.

Fonte: Adaptado para quadro de Shahri e Ismail (2012).

No processo de classificação das ameaças, é possível a elaboração de "árvores", em que os tipos de ameaças serão representados pelos ramos, enquanto que as ameaças em si, correspondem às folhas (FERREIRA, 2013). No entanto, Peltier (2005, p. 18) assevera que embora as listas de ameaças tenham sua importância no contexto de identificação das ameaças, deve-se ter o cuidado para não usar uma lista de verificação de forma incorreta, pois afetará o fluxo de ideias e informações. Deve-se usar para garantir que todo o processo esteja coberto e identificado, mas não se deve usá-las confiando que se completará o processo de avaliação de risco.

2.5 PROCEDIMENTO DE ANÁLISE DOS DADOS

Para análise e interpretação dos dados utilizou-se o Processo Facilitado de Análise e Avaliação de riscos (FRAAP), que foi complementado com questionário e análise de conteúdo de acordo com Bardin.

Segundo Bardin (2011, p. 48) a análise de conteúdo refere-se a:

> um conjunto de técnicas de análise das comunicações visando obter por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens indicadores(quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) dessas mensagens.

A autora ressalta ainda que a análise de conteúdo se refere a "iniciativas que, a partir de um conjunto de técnicas parciais, mas complementares, consistam na explicitação e sistematização do conteúdo das mensagens e da expressão de conteúdo [...]". Além disso, ela considera como um leque de instrumentos, apetrechos, com grande disparidade de formas e sua aplicação pode ser adaptada a um vasto campo, como o das comunicações. Bardin (2011, p. 44) afirma, ainda, que "a intenção da análise de conteúdo é a inferência de conhecimentos

relativos às condições de produção (ou, eventualmente, de recepção), inferência esta que recorre a indicadores (quantitativos ou não)".

Na visão de Franco (2012, p. 12), a análise de conteúdo parte da

> [...] mensagem, seja ela verbal (oral ou escrita), gestual, silenciosa, figurativa, documental ou diretamente provocada. [...] O que está escrito, falado, mapeado, figurativamente desenhado, e/ou simbolicamente explicitado sempre será ponto de partida para identificação do conteúdo, seja ele explícito e/ou latente.

O processo de analisar e interpretar os conteúdos requer a contextualização como principal requisito, de modo que se possa atribuir relevância ao sentido das mensagens.

Análise de conteúdo de acordo com Richardson (1999, p. 224) trata-se de uma técnica de pesquisa, para o estudo de material, de tipo qualitativo, em que não se é aplicado técnicas aritméticas. Consiste em se fazer uma primeira leitura para organização das ideais inclusas, em seguida a análise dos elementos e regras que as determinam. É de natureza científica, portanto, deve ser eficaz, rigorosa e precisa. Está voltada para a atividade de se obter uma melhor compreensão de um discurso, buscando aprofundar suas características, quais sejam, gramaticais, fonológicas, cognitivas, ideológicas e outras, de maneira que possa se extrair o que for mais relevante.

Entende-se que a análise de conteúdo e o FRAAP, foram métodos fundamentais no atendimento dos objetivos desta pesquisa acerca dos aspectos de gestão da segurança da informação que permitisse propor uma minuta de política de segurança da informação para a BC/UFPB.

Tanto a análise como a discussão dos resultados são apresentados no tópico 5, após os capítulos de revisão de literatura, que são compostos por: Aplicação e análise do FRAAP e Aplicação e análise do questionário.

3 POLÍTICAS EM BIBLIOTECAS UNIVERSITÁRIAS E SUA RELEVÂNCIA NO CENÁRIO DA PRODUÇÃO DO CONHECIMENTO

A universidade enquanto produtora, depositária e disseminadora do conhecimento, configura-se como agente que corrobora na construção do saber, constituindo-se promotora de mudança na sociedade. Nesta perspectiva, evidencia-se o compromisso da Biblioteca Universitária (BU), instituição inserida no contexto da universidade, como responsável pela gestão de todo conhecimento produzido.

No cenário de constantes inovações de tecnologias de informação e comunicação que propiciam mudanças na disponibilização, busca, recuperação e uso da informação, situam-se as Bibliotecas, Centro de Documentação e outras Unidades de Informação, que se deparam com novos desafios que redimensionam o modo de ver e pensar seus processos de trabalho. Estes seguimentos têm no cerne de suas atividades o objeto informacional e requer a utilização das TIC, no processamento e disponibilização de seu acervo informacional.

Evidenciam-se as bibliotecas, que se constituem em instituições que remontam há milhares de anos, e ao longo da história da humanidade, se dedicam à tarefa de reunir os registros do conhecimento. A formação de seus acervos foi se modificando ao sabor dos diversos acontecimentos históricos (CAETANO; FERNANDES, 2015).

A criação de bibliotecas ligadas às instituições de ensino refere-se ao período compreendido entre os séculos XIX e início do século XX, quando do surgimento das escolas superiores (CARVALHO, 2004). Targino (2006, p. 65) assevera que independentemente do nível em que opere a biblioteca, sua finalidade deve ser a de “maximizar a utilidade social dos registros gráficos, mantendo vivas a identidade e a memória da cultura local, o que favorece o impulso do nível cultural brasileiro”.

Nota-se que a Biblioteca Universitária tem um papel de destaque no âmbito da Instituição a que está vinculada, pois tem como função precípua suporte às atividades de ensino, pesquisa científica e extensão, no fomento à produção de novos conhecimentos e continuidade de novas pesquisas, que direcionam ao progresso científico, bem como da sociedade como um todo.

As mudanças ocorridas nas Bibliotecas Universitárias (BUs), no cenário brasileiro, decorreram dos acontecimentos históricos materializados e impulsionados pela Reforma Universitária de 1968 e movimentos sociais da década de 1980, período este marcado pela implementação de programas, projetos de desenvolvimento, ligados à área científica e

tecnológica, conferindo à universidade crescimento e configuração de uma identidade própria (SILVA, 2010).

Estes acontecimentos suscitaram mudanças no âmbito das universidades, no campo educacional, fomentando desenvolvimento no ensino e pesquisa, tendo a Ciência e a Tecnologia (C&T) como fatores que impulsionaram mudanças estruturais significativas no âmbito destas, paralelo às mudanças sociais.

Neste sentido, Carvalho (2004, p. 90) afirma:

> No decorrer da última década do século XX, as bibliotecas universitárias, acompanhando a dinâmica de seu macroambiente, entram numa fase de transição, buscando definir uma nova identidade, adaptar-se às mudanças sociais, econômicas e tecnológicas que influem na questão da socialização do conhecimento e conviver com dois modelos, aparentemente, antagônicos: o da biblioteca convencional e o da virtual, já que por muito tempo os átomos e os bits deverão estar presentes em nosso cotidiano.

Essas mudanças surgem como marcas da sociedade da informação e do conhecimento em que informação e conhecimento são valorizados e reconhecidos como elementos essenciais que geraram um redimensionamento no ambiente organizacional das BUs, consequentemente gerando novas ferramentas de trabalho integradas a sistemas de informação em rede, redimensionando também a gestão dos recursos humanos e informacionais.

Silveira (2014, p. 73) destaca, ainda, o impacto que as transformações tecnológicas causaram diretamente no ambiente organizacional das bibliotecas universitárias, em que se pode perceber claramente “o aumento do fluxo de informações, a fluidez das relações interpessoais, a automatização de diversos processos e produtos, a quebra de paradigmas e o surgimento de novos conceitos como a globalização e as tecnologias da informação”.

Nota-se que a BU está inserida no contexto da Era da informação e do conhecimento e estes impõem desafios e mudanças, que se revelam na incorporação de novos paradigmas que a biblioteca universitária precisou e precisa, para se capacitar de maneira que possa acompanhar os avanços científicos e tecnológicos, também impactados na Universidade em que está inserida, de modo que possa dinamizar seus serviços.

Entende-se que a BU enquanto organização, de acordo com Maciel e Mendonça (2006, p. 10) tem a “capacidade de criar organismos, estruturas e sistemas bem integrados e constituídos, como base para atividades operacionais e administrativas de uma empresa, com o menor dispêndio e risco”.

Sua estrutura se expressa em um conjunto de atividades efetivadas por equipes de trabalho, com um propósito direcionado ao provimento de acesso à múltiplas fontes de informação e conhecimento, de maneira que possa oferecer serviços e produtos de qualidade, na direção de resultados que venham condizer com seus objetivos e metas.

Desse modo, a biblioteca, que outrora tinha como elemento basilar a disponibilização de suportes informacionais, se converte em espaço de acesso e "interatuação do saber e comunicação", passando a ser também:

> Pensada como um dos espaços facilitadores da aprendizagem, [e] deve ser encarada como um espaço de múltipla comunicação, disponibilizando itens informacionais, dentro de padrões de agilidade e adequabilidade necessários à geração de novos conhecimentos, representando um fórum de interação entre emissores e receptores do conhecimento e da informação e um recurso social comprometido com a comunicação pedagógica (CARVALHO, 2004, p. 96).

Nesta perspectiva, as atividades de planejamento de políticas para bibliotecas universitárias são cruciais para o bom funcionamento dos serviços oferecidos, que devem ser avaliados periodicamente, a fim de se mensurar a qualidade no atendimento das necessidades informacionais de seus usuários (MACIEL; MENDONÇA, 2006).

As decisões que precisam ser tomadas no ambiente organizacional da BU, têm como base a informação. São implementadas políticas que regulam os processos de tratamento, recuperação, uso e disseminação da informação, que são cruciais para que a biblioteca possa se adequar às mudanças impostas pelo avanço tecnológico.

Isto se aplica, também, no contexto da produção do conhecimento científico, de maneira que possa atender às demandas acadêmicas, no oferecimento de produtos e serviços de qualidade e, dessa forma, integrar-se a um novo contexto de construção do conhecimento, no enfrentamento constante dos desafios gerados por um cenário de complexidade e competitividade, imperativos da sociedade da informação e do conhecimento.

3.1 A INFORMAÇÃO NO CONTEXTO DA BIBLIOTECA UNIVERSITÁRIA

A informação é um determinante nos processos decisórios das organizações, de modo que seu uso estratégico aponta para ações na geração de conhecimento, inovações e desenvolvimento, o que oportuniza a organização manter-se competitiva e produtiva.

A partir da aplicação das inovações tecnológicas, a sociedade se depara com o desafio de comungar as ações de gestão e tecnologia, exigindo habilidades de gerenciamento nas diversas formas de uso da informação.

A dinâmica da sociedade da informação e do conhecimento influencia diretamente no fazer dos processos de gerenciamento informacional em unidades de informação. Contudo, é necessário entender o que é a informação, que segundo Capurro e Hjorland (2007, p. 187) "é o que pode responder a questões importantes relacionadas às atividades do grupo alvo". Duarte (2012, p. 1) considera "que a informação foi se tornando presente, cada vez mais, em nossas vidas - sua área de ação e atuação, sua visibilidade, seu papel e aplicação e o seu destaque como um bem valioso na Sociedade da Informação e do Conhecimento".

Para Setzel (2015, não paginado): "*Informação* é uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa". A informação, de acordo com o autor, é "objetiva-subjetiva", é dependente do usuário. Neste sentido, "é descrita de uma forma objetiva (textos, figuras etc.) ou captada a partir de algo objetivo [...]".

Informação precisa fazer sentido para quem a recebe, para quem se apropria dela. Quando inteligível, passa a fazer sentido. É uma interpretação pessoal. Pode pertencer ou ser recebida por uma pessoa. É uma representação que pode mudar dependendo de quem a recebe, modificando, assim, o receptor. A informação perpassa pela associação de conceitos. Por meio dessas associações, o ser humano atribui significado às coisas para entender o mundo que o circunda, bem como, seu interior pessoal (SETZEL, 2015).

Segundo Choo (2003, p. 27): "A informação é um componente intrínseco de quase tudo que uma organização faz". Desse modo: "A organização usa a informação para dar sentido às mudanças do ambiente externo".

Choo (2003) ressalta que, com a posse da informação, a organização torna-se bem-informada e capacitada para perceber e discernir, pois suas ações são baseadas na compreensão adequada de seu ambiente organizacional, nas necessidades, em que as fontes de informação e competências de seus membros servem de alavanca, que permitirá a organização agir com inteligência e criatividade. Nas organizações as pessoas buscam entender o que as circundam, dão sentido ao que acontece no ambiente, desenvolvem uma interpretação comum, compartilhamento de informação que aplicada gera novos conhecimentos.

Para Beal (2004, p. 21): "A informação possibilita a redução da incerteza na tomada de decisão, permitindo que escolhas sejam feitas com menor risco e no momento adequado". De acordo com a autora, decisões de qualidade, dependem igualmente da qualidade da

informação fornecida, bem como da habilidade de interpretação dos tomadores de decisões, do uso para escolher as melhores alternativas, e o acesso a informações certas, o que confere sucesso na decisão.

> A informação exerce influência sobre o comportamento dos indivíduos e dos grupos, dentro e fora das organizações: internamente, a informação busca influenciar o comportamento dos indivíduos para que suas ações sejam condizentes com os objetivos corporativos; externamente, a informação visa influenciar o comportamento dos envolvidos (clientes atuais ou potenciais, fornecedores, governo, parceiros etc.), de modo que se torne favorável ao alcance dos objetivos organizacionais (BEAL, 2004, p. 22).

Nesse sentido, sendo um recurso determinante nos processos gerenciais das organizações e produtor de conhecimento, e consequentemente de transformações, a informação está presente no campo das preocupações relacionadas as políticas institucionais, que, por meio de ações de fomento às políticas de informação, empreende esforços para minimizar os problemas sociais e culturais, por meio do acesso a informação, paralelo à iniciativas que se ocupam da difusão de recursos tecnológicos e redes informacionais (AUN, 1999).

Na perspectiva de um melhor entendimento das políticas de informação, no contexto das bibliotecas universitárias, que precisaram se reinventar diante das transformações tecnológicas e científicas que as levaram a um redimensionamento de suas políticas, apresenta-se, a seguir, a visão de alguns autores sobre políticas de informação e referência aos acontecimentos ligados ao desenvolvimento de políticas de informação em ciência e tecnologias (ICT), no contexto das políticas públicas que foram cruciais ao desenvolvimento das bibliotecas universitárias.

Cunha e Cavalcanti (2008, p. 285) definem política de informação como um “plano para a provisão e acesso à informação no âmbito de uma cidade, organização, região ou país. Política nacional de informação”.

Segundo Araújo (2015, p. 35): “As políticas de informação inserem-se no campo das políticas institucionais, em geral. Expressam um conjunto de ações e escolhas baseadas em metas, e objetivos, e envolvem vários atores e níveis de decisão”.

Araújo (2015, p. 356) ressalta que, atualmente, as políticas de informação,

> [...] relacionam-se, por um lado, com a necessidade de maior institucionalização das atividades, visando maior eficácia e eficiência dos processos. Por outro lado, o incremento das tecnologias digitais imprime nova realidade às políticas informacionais, em termos de acesso e sigilo,

> estratégias de preservação e de armazenamento, condições de produção e de uso (ARAÚJO, 2015, p. 356).

O autor ressalta, ainda, que as questões relacionadas à "transparência de valores" e o "exercício da cidadania", sobretudo nas organizações públicas, tornaram-se imperativos mais evidentes, com o acesso à informação. E afirma que as políticas de informação se estruturam no Quadro desses fatores.

Numa referência às iniciativas de fomento às políticas de informação, tanto no âmbito nacional quanto internacional, em relação ao posicionamento dos governos, de acordo com Aun (1999, não paginado):

> O que os governos têm buscado, com programas e decisões públicas, é garantir a participação do país na sociedade da informação. Assim, os problemas referentes à informação estão sendo tratados por duas categorias: o grupo preocupado com o lado que chamaremos de material, direcionado para a difusão de materiais informáticos, visando ao estabelecimento de redes informacionais e ao grupo que se ocupa de problemas sociais e culturais ligados à informação, voltado então para o domínio imaterial, refletindo sobre a questão do conteúdo na sociedade da informação.

Aun (1999, não paginado) destaca ainda que: "A construção de uma política de informação implica o que é verdadeiramente prioritário: o desenvolvimento da sociedade de forma justa e democrática".

Para Accart (2012, p. 31, tradução nossa) uma política de informação trata de um:

> [...] conjunto de objetivos que pode visar a um serviço de informação para servir a um público bem definido. Uma política documentária [informação] é necessariamente baseada em parte em uma política de constituição de coleções, incluindo aquisições e descartes e, em parte, em uma análise do público servido ou para ser servido. Ela é construída obrigatoriamente a partir de uma avaliação de resultados com base em resultados estatísticos (atendimento, número de empréstimos,...) e qualitativo. É realista, tendo em conta os seus recursos financeiros e humanos. É registrada em um determinado período. Enfim, um elemento fundamental, uma política documentária [informação] necessita de uma validação por uma autoridade colocada acima daquele que é responsável por implementá-la (o conselho de administração de forma mais geral), firmando um consenso em torno de pilares e um projeto que pode ser implementado.

Recuando um pouco mais no tempo, no contexto brasileiro, percebe-se que é na década de 1950, que se expressa o marco inicial de iniciativas voltadas para a criação de diversos organismos, institutos de pesquisa, que se encarregaram da formulação e implantação de políticas públicas de Ciência e Tecnologia (C&T), que culminou no desenvolvimento de um sistema de C&T, integrando diversos órgãos de ensino e pesquisa, com programas, apoio

legal, orçamentos (SILVA; GARCIA, 2009, DIAS; SILVA; CERVANTES, 2013). Época também em que "a informação começava a ser vista como um fator estratégico para o desenvolvimento de países, pois a produção científica e tecnológica necessitava da informação como insumo para transformar conhecimentos em bens e serviços". (SILVA; GARCIA, 2009)

Desse modo, a informação deveria ser organizada e disponibilizada para o atendimento das demandas informacionais. Segundo Silva e Garcia (2009), nessa mesma época se iniciou:

> [...] um movimento vertiginoso para a produção de bancos de dados, para o desenvolvimento de linguagens, os investimentos em bibliotecas, centros de informação e documentação - órgãos por natureza armazenadores e distribuidores de informações.

De acordo com Silva e Garcia (2009), surge, a partir de então, uma necessidade do estabelecimento de políticas para a informação científica e tecnológica (C&T), de modo que pudesse ser regulada: a geração, fluxos e usos da informação científica e tecnológica, contemplando, também, a organização dos canais formais e informais da produção e distribuição, bem como, a solução de conflitos nas relações entre produtores e receptores de informação.

Percebe-se que tais acontecimentos impactaram a biblioteca universitária e as unidades ligadas a ela (bibliotecas setoriais), ao longo de sua trajetória histórica, exigindo um redimensionamento de sua estrutura administrativa, bem como infraestrutura física, referente ao estabelecimento de políticas com diretrizes que pudessem tornar claras as escolhas que a BU precise fazer para orientar racionalmente suas atividades (rotinas de trabalho) no suporte informacional à comunidade acadêmica e público em geral.

Dias, Silva e Cervantes (2013, p. 44) destacam também a criação, na década de 1970, do evento que se denominou Seminário Nacional de Bibliotecas Universitárias (SNBU), que tem sua origem a partir das discussões e questões relacionadas ao contexto da biblioteca universitária, levantadas por um grupo de bibliotecários, à época criadores deste evento. Ressalta-se que as discussões levantavam questões que envolviam a estrutura física da biblioteca, automação de acervo, aquisição de equipamentos, periódicos científicos, livros, bem como questões que envolviam a gestão das bibliotecas universitárias, tecnologias de informação e comunicação, temas esses tratados nos trabalhos apresentados ao longo do evento SNBU.

Esses acontecimentos evidenciam-se como iniciativas relevantes para um novo olhar e um efetivo redimensionamento dos processos administrativos e operacionais que direcionaram a ampliação e otimização dos serviços de informação nas bibliotecas universitárias, mobilizando sua entrada na sociedade da informação e do conhecimento.

3.2 POLÍTICAS EM BIBLIOTECAS UNIVERSITÁRIAS

Em sua estrutura administrativa, a biblioteca contempla políticas, baseadas em sua missão, em que são estabelecidos princípios que, através de diretrizes, orientam e dão sentido às atividades fins, aos seus produtos e serviços destinados à comunidade acadêmica e à sociedade.

Na visão de Cunha e Cavalcanti (2008, p. 285), referem-se a ideia de políticas em bibliotecas a uma "formulação, formal ou informal, ligada ao atendimento da missão da biblioteca, bem como os critérios de avaliação".

No caso da biblioteca universitária, estas políticas estão relacionadas diretamente aos programas de ensino, pesquisa e extensão, pois se consubstanciam nas atividades direcionadas à formação e manutenção das coleções e controle dos serviços bibliotecários.

Segundo Almeida (2005, p. 6), no que se refere às bibliotecas e serviços de informação, "as políticas ou diretrizes são planos gerais de ação, guias genéricos que definem linhas mestras, orientam a tomada de decisão e dão estabilidade à organização. " E vão desde as gerais as mais específicas, dependendo da área de atuação da biblioteca. De acordo com a autora, para que se possa alcançar eficácia na consecução dos objetivos organizacionais, é necessário que estejam coerentes e integradas, considerando que existem diversas políticas em uma mesma organização.

Nesse sentido, pode-se considerar que são diversas as políticas em vigor em uma biblioteca universitária. Elas se aplicam ao estabelecimento de normas e regulamentos que norteiam o uso das coleções, bem como dos serviços bibliotecários. Para orientar a organização, temos o regimento interno, "um instrumento organizacional que complementa e explica o organograma. Contém: constituição, competências e atribuições" (ALMEIDA, 2005, p. 7). Este instrumento estrutura aspectos administrativos e operacionais da biblioteca, e estabelece como as atividades serão executadas, quais serviços e produtos serão oferecidos, contratação de pessoal técnico, recursos financeiros destinados à formação e desenvolvimento das coleções, à manutenção da infraestrutura, manutenção das coleções, e outros. Cada

biblioteca tem suas peculiaridades, de modo que as políticas são elaboradas de acordo com sua linha de atuação.

Nota-se que as políticas são guias racionais no apoio a tomada de decisões e ações, que diferem de regras e procedimentos, estes direcionados à execução de tarefas.

> Os procedimentos são instrumentos que estabelecem métodos rotineiros de execução das atividades e detalham a maneira exata pela qual uma atividade deve ser realizada e a sequência (sic) em que essas rotinas são realizadas. As regras relacionam-se aos procedimentos, pois orientam a ação, mas não especificam a sequência cronológica. Como exemplo, temos as normas e os regulamentos. As normas são comandos diretos e objetivos de curso de ação a seguir [...] (ALMEIDA, 2005, p. 6)

As políticas em vigor na biblioteca universitária compõem-se de um conjunto de princípios fundamentais que estão ligados ao processo de planejamento e, como complementa Almeida (2005, p. 6), "um processo contínuo, permanente e dinâmico, que fixa objetivos, define linhas de ação, detalha as etapas para atingi-lo e prevê os recursos necessários a consecução desses objetivos".

O planejamento permite uma visualização do futuro, a otimização do tempo e melhor controle dos planos (linha de ação, meio de se chegar aos objetivos), na implementação e avaliação das atividades que, quando bem desempenhadas, em consonância com os objetivos e metas da biblioteca, e com a missão da instituição a qual está vinculada, contribui na redução das incertezas na organização e aponta para mudanças e melhor desempenho. Neste sentido, Almeida (2005, p. 3) afirma:

> O planejamento reduz riscos, ao mesmo tempo em que tira proveito das oportunidades. À medida que o profissional da informação analisa, de uma perspectiva estratégica, as ameaças e oportunidades do ambiente externo e interno, estará definindo objetivos com mais segurança e tomando decisões que afetarão o futuro dos serviços com maior grau de certeza quanto a atingir aqueles objetivos.

Almeida (2005) ressalta, ainda, que as decisões tomadas no ambiente organizacional da biblioteca baseiam-se em informações e, uma vez que são tomadas antecipadamente, devem obedecer a critérios objetivos, o que confere a estas informações um caráter independente de oscilações de humor e questões subjetivas. Nota-se que a prática de planejar as decisões confere à organização maior estabilidade, equilíbrio no ambiente e maior produtividade.

É peculiar a biblioteca universitária armazenar uma quantidade exponencial de informação, que formará as coleções, e pode se encontrar em diversos suportes, quer seja impresso, eletrônico ou digital.

Os documentos que irão compor a coleção, necessitam de preparo técnico que posteriormente serão disponibilizados através de serviços que são orientados por políticas, diretrizes e normas que propiciarão acesso, recuperação e uso, com eficiência. Assim, temos que:

> O conjunto de políticas e diretrizes não só esclarece a filosofia e os objetivos que norteiam as práticas diárias e a consistência nas diversas etapas do tratamento bibliográfico e de atendimento ao usuário, mas as articula, fornecendo um sentido cooperativo e agregador de valor a cada etapa de processamento (CAETANO; FERNANDES, 2015, p. 435).

Percebe-se, desse modo, que é tarefa precípua, no ambiente organizacional da biblioteca universitária, a elaboração de documentos que visam à implementação de rotinas, planejamento dos fluxos das atividades, manuais, guias para os usuários, procedimentos de formação, manutenção e uso das coleções, normas de uso da biblioteca, bem como procedimentos para os processos de trabalho, avaliações (CAETANO; FERNANDES, 2015).

As atividades de identificação, organização, acesso, recuperação e disseminação da informação, a elaboração de tais documentos que padronizem as rotinas de trabalho e possibilitem o acesso e uso dos recursos informacionais, são cruciais no fazer bibliotecário, e devem estar alinhados às demandas informacionais de seus usuários. De acordo com Caetano e Fernandes (2015, p. 435), tais documentos possibilitam:

> [...] realizar avaliações periódicas dos resultados das ações e planos e rever os procedimentos que precisem ser readequados à dinâmica própria dos usos da informação e de novas disponibilidades metodológicas, técnicas e tecnológicas. Eles também são fundamentais para dar transparência sobre decisões tomadas pela biblioteca como a distribuição dos recursos informacionais no atendimento aos segmentos de usuários, as decisões sobre escolha de linguagens documentárias para representação de conteúdos, do alcance ou limite da cooperação com outras bibliotecas etc.

Neste contexto, Pasquarelli (1996) destaca também a figura do usuário da informação que está intrínseca à razão principal da biblioteca, que justifica, para tanto, a existência das principais atividades direcionadas ao desenvolvimento e manutenção das coleções: aquisição de material bibliográfico e multimeios, que pode ser por compra, permuta e doação; preparo técnico do material, que envolve a representação descritiva e temática dos documentos e o

serviço de referência: que refere-se ao atendimento ao usuário, [bem como recuperação, uso eficaz dos serviços de informação, dos recursos informacionais e tecnológicos].

Para melhor compreender a relevância das políticas em vigor no âmbito da BU, destacam-se, a seguir, algumas das que se consideram como principais dentre as políticas existentes na biblioteca, para a consecução de suas atividades de geração, organização, acesso, uso e disseminação da informação. Elas se consolidam em: 1) Política de formação e desenvolvimento de coleções: política de seleção de materiais informacionais, política de desbaste e descarte e política de preservação e conservação de acervos; 2) Política de indexação; e 3) Política de atendimento (circulação e referência).

3.2.1 Política de Formação e Desenvolvimento de Coleções

Entende-se que para a efetividade dos serviços no âmbito da biblioteca são criadas políticas, que se relacionam com o processo de desenvolvimento de coleções. Este processo, para Weitzel (2006, p. 19), "compreende atividades de estudo da comunidade, política de seleção, seleção, aquisição, desbastamento e descarte e avaliação". Essas atividades corroboram no sentido de conhecer as demandas e necessidades informacionais dos usuários, quer sejam atuais ou mesmo potenciais. E a ênfase nas etapas citadas acima está determinada pelos objetivos da instituição e sua clientela. No caso da biblioteca universitária, o acervo é formado com base nas demandas informacionais advindas dos programas de graduação, pós-graduação e extensão.

Vergueiro (1989) assevera que o desenvolvimento de coleções é um processo de planejamento de acervos, o qual afeta e é afetado por inúmeros fatores externos, envolve um compromisso com metodologias, tem um caráter contínuo, não é homogêneo, e considera as especificidades de cada biblioteca. As atividades de desenvolvimento de coleções são influenciadas pelo tipo de biblioteca, seus objetivos específicos e a comunidade a ser atendida.

No caso da biblioteca universitária, de acordo com o autor, o acervo é desenvolvido para atender aos objetivos da universidade, voltados ao ensino, pesquisa e extensão, considerando o fato de que o caráter da comunidade, é relativamente homogêneo, dessa forma a ênfase maior será no desbastamento e avaliação da coleção.

Para Vergueiro (1989, p. 23), "o desenvolvimento de coleções, como atividade de planejamento, deve ter um plano detalhado preestabelecido, a fim de garantir um mínimo de continuidade ao processo e correções de rota, quando necessárias".

E esse “planejamento inclui, necessariamente, a formação de coleções seguindo rigoroso critério seletivo, direcionado para usuários de cada categoria de biblioteca” (FONSECA, 2007, p. 49).

O quisto implicará, de acordo com Vergueiro (2010), na elaboração de um documento – a política de desenvolvimento de coleções – que estabelece a quem a coleção atenderá, os parâmetros gerais da coleção, e critérios de formação e desenvolvimento da mesma.

A política de desenvolvimento de coleções mostra-se como “um instrumento importante para desencadear o processo de formação e crescimento de coleções, constituindo-se num documento formal elaborado pela equipe responsável pelas atividades que apoiam o processo de desenvolvimento de coleções como um todo” (WEITZEL, 2006, p. 18). Esta política se constitui numa das mais relevantes na biblioteca universitária, bem como em qualquer biblioteca, cuja formação e manutenção das coleções está diretamente ligada aos seus objetivos e fins, sua razão de ser, o usuário, como já destacado anteriormente.

No processo de desenvolvimento de coleções, as bibliotecas não se bastam a si mesmas, pois nota-se, de acordo com Vergueiro (1989), que é um processo influenciado também pelo intercâmbio entre as bibliotecas de instituições congêneres, elas utilizam-se dos recursos disponíveis e compartilham dos mesmos. Além de ser uma medida econômica, frente aos parcos recursos financeiros na aquisição de produtos informacionais, também se mostra como medida de melhoramento dos serviços prestados aos usuários, que terão um universo amplo de recursos informacionais disponíveis. No entanto, para o autor, os propósitos para a elaboração de uma política são amplos e vão além de questões financeiras, no tange à formação do acervo informacional. Desse modo:

> Trata-se de deixar clara a filosofia a nortear o trabalho bibliotecário no que diz respeito à coleção. [...] Trata-se de tornar público, expressamente, o relacionamento entre o desenvolvimento da coleção e os objetivos da instituição a que esta coleção deve servir, tanto por causa de um guia prático na seleção diária de itens, como devido ao fato de ser tal documento uma peça-chave para o planejamento em larga escala (VERGUEIRO, 1989, p. 25).

Vergueiro (1989) destaca ainda, que o processo de elaboração dessa política tem caráter pedagógico, no momento em que ao bibliotecário, enquanto gestor das coleções, é oportunizado exercer uma autoavaliação e uma reflexão da sua prática de desenvolvimento das coleções.

Nota-se que a existência deste documento garantirá um crescimento equilibrado dos recursos informacionais, funcionando como diretriz nas tomadas de decisões, no que se refere à seleção dos materiais que irão compor o acervo, bem como a gestão dos recursos informacionais.

A política de desenvolvimento de coleções proverá uma descrição do estado geral do acervo, apontando a metodologia que guiará as atividades para a consecução dos objetivos e obtenção de subsídios para novas aquisições e otimização das coleções.

3.2.1.1 Política de Seleção de materiais informacionais

O processo de seleção é um momento de decisão. Considerando-se o aumento vertiginoso dos recursos informacionais e as transformações que impactaram o campo da pesquisa científica, requer-se do profissional bibliotecário, responsável pela seleção, um poder de decisão assertivo, coerente, um conhecimento do estado geral da coleção, do mercado editorial, das demandas informacionais da unidade de informação no que se refere à seleção dos itens relevantes, que serão incorporados ao acervo ou que irão formar a coleção.

Embora nem sempre a decisão final na seleção possa pertencer ao bibliotecário, faz-se necessário um conhecimento preciso de sua parte, em relação aos procedimentos do processo de decisão, de maneira que o mesmo possa vir a defender as necessidades da coleção, exercer uma atitude de zelo pelo desenvolvimento da coleção que se adeque aos seus objetivos, pois é necessária uma análise criteriosa, objetiva e bem elaborada de cada material que será incluso ao acervo, possibilitando-se uma discussão com o usuário sobre a relevância de cada item, a negociação de interesses divergentes, de maneira que possa evidenciar, em seus atos, decisões precisas (VERGUEIRO, 2010). O autor ressalta que o processo de seleção implica critérios, que estão ligados à especialidade da biblioteca e do usuário. E esses critérios precisam estar bem definidos e documentados formalmente (institucionalizados), para que se possa dar garantia de continuidade da prática através de outros profissionais bibliotecários que venham a suceder.

Vergueiro (2010) assevera, ainda, que há, no processo de seleção, uma graduação de critérios na seleção dos materiais informacionais, que vão de grandes ou amplos aos mais específicos. Compara o processo de seleção a uma corrida de obstáculos, em que os documentos competem para atingir o objetivo de ser incorporado ao acervo e, desse modo enfrentam obstáculos que são os critérios de seleção. O que será preponderante é a questão de se colocar os critérios corretamente. Não é tarefa simples, que possa trazer respostas fáceis.

Faz-se necessário uma reflexão acerca dos fatores gerais que influenciam no processo de seleção dos materiais informacionais.

Vergueiro (2010, p. 12) ressalta que "a forma de abordar esse processo será diretamente influenciada pela tipologia da biblioteca". O autor argumenta que nas bibliotecas especializadas, por exemplo, a ênfase se dará na temática do acervo, em que o processo de seleção se inicia pela definição dos grandes assuntos. Já nas bibliotecas públicas o ponto de partida se dá pela definição da comunidade a ser atendida, em que pese a caracterização dos usuários reais e potenciais, mas não excluindo os grandes assuntos. Ele considera, também, que os procedimentos citados são comuns e presentes nas instituições bibliotecárias, de modo que o processo de seleção traça considerações abrangentes (assunto, usuário, documento e preço), para a *posteriori* serem refinadas e adequadas às particularidades de cada instituição.

A política de seleção é, antes de tudo, um instrumento formal da biblioteca, que diz respeito ao estabelecimento de critérios de seleção na formação e desenvolvimento das coleções, cuja aquisição do material informacional se fará por compra, doação ou permuta. Neste sentido, são estabelecidas diretrizes que guiarão as atividades de seleção, conferindo à coleção qualidade e dinamismo.

Segundo Vergueiro (2010, p. 71): "Os critérios de seleção devem funcionar, para a biblioteca, como funcionam as leis para um país: enquanto não são modificadas, devem ser obedecidas. O documento registrará os critérios de seleção vigentes na biblioteca; [...] deverão justificar todas as decisões". Nesta perspectiva, a utilização objetiva dos critérios conferirá um enfrentamento eficiente frente às pressões que, por vezes, o acervo venha a sofrer, de modo que as decisões atuais e futuras possam ser justificadas por este documento:

> [...] um documento formal de política de seleção justifica-se por seu caráter: *administrativo*, com a finalidade de garantir a continuidade dos critérios além da presença física de seus elaboradores; de *relações públicas*, ao tornar a biblioteca simpática aos olhos da comunidade; e *político*, ao proporcionar um instrumento para resistência ou gerenciamento dos conflitos e pressões em torno da coleção (VERGUEIRO, 2010, p. 71).

Neste sentido, o autor ressalta que a elaboração de documento de uma política deve ser um instrumento que expresse clareza nos objetivos, simplicidade, que conste a identificação dos responsáveis pela seleção, os critérios que serão utilizados no processo de seleção, instrumentos auxiliares, bem como as políticas específicas e documentos correlatos. Estes elementos adequadamente elaborados darão suporte às decisões que deverão ser tomadas no processo de seleção dos materiais informacionais.

Não existe uma fórmula para a elaboração do documento, isto dependerá das especificidades de cada instituição bibliotecária, sua missão, seus objetivos e metas específicas, dos seus usuários, bem como a missão da instituição a qual a biblioteca serve. Vale lembrar que a política de seleção não é algo estanque, ela poderá vir a sofrer alterações, avaliações, que forem necessárias para conferir uma melhor qualidade às coleções.

3.2.1.2 Política de desbaste e descarte de acervos

O processo de desbaste ou descarte permite que o acervo se desenvolva de maneira racional, com uma boa qualidade, renovação de espaços de armazenamento, dando uma maior otimização no acesso às coleções. Desse modo, o processo de avaliação das coleções permitirá a identificação dos títulos que serão remanejados para outro local com um armazenamento especial, para fins de preservação e conservação ou descarte (WEITZEL, 2006). As ações de desbaste ou descarte se dão a partir das regras e procedimentos estabelecedores de uma política.

A este respeito, Cunha (2008, p. 285) a política de descarte trata-se de um "documento que regulariza e padroniza as atividades de descarte no acervo de uma unidade de informação". Está, portanto, inserida na política de desenvolvimento de coleções.

3.2.1.3 Política de preservação e conservação de acervos

A trajetória da sociedade, no decorrer dos séculos, é marcada pelo esforço em manter registrado o conhecimento, fazendo uso de diversos suportes e políticas que irão garantir a salvaguarda da memória documental, processo esse que se entende como um compromisso social.

Nesta perspectiva, a biblioteca universitária, através de suas unidades de informação, se posiciona como depositária do conhecimento registrado, e exerce um papel relevante na geração, organização, preservação, acesso, uso e transmissão do conhecimento, através do conteúdo informacional em diversos suportes físicos e digitais.

As bibliotecas convivem com problemas de instalações físicas para armazenar seus acervos e prover serviços a seus usuários mediante o surgimento das Tecnologias de Informação e Comunicação (TIC). A utilização dos sistemas de automação causa impacto na rotina da biblioteca. Assim, as bibliotecas tiveram que adotar novas formas de gestão, de acordo com as novas demandas (CUNHA, 2000).

Neste contexto, destaca-se a política de preservação e conservação, que está inserida nos processos de gestão das coleções. Essa política origina-se da necessidade imperativa que a biblioteca tem da manutenção e salvaguarda das coleções, de modo que possa postergar a vida útil do documento, através de ações preventivas, e dar acesso ao seu conteúdo informacional cumprindo assim sua função social.

Compreende-se a urgência de uma mudança de mentalidade, articulação de um trabalho de conscientização do pessoal lotado nas unidades de informação, mobilizando a participação integrada nas medidas de manutenção do patrimônio cultural (MESQUITA, 2012). Assim sendo, deve-se atentar para o estado de conservação das coleções, no sentido de articular uma gestão de políticas de preservação, estabelecendo ações técnicas relacionadas ao ambiente, capacitação e motivação das equipes de trabalho. São estas medidas que vão maximizar a vida útil do acervo, bem como o acesso à informação e a satisfação do usuário, permitindo uma melhor preservação do patrimônio cultural às gerações futuras. Desse modo, como propõe Duarte (2014, p. 9):

> A preservação de documentos compreende estratégias de ação que devem ser mantidas pela administração de quem os mantêm. Com relação à políticas de preservação, a realidade dos acervos de arquivos e bibliotecas tem se mostrado fragilizada. Há carências de ações mais decisórias quanto a definições de medidas para a salvaguarda do patrimônio documental que representa e expressa uma estética em sua temporalidade.

Para que haja um bom desempenho das tarefas, é necessário um posicionamento assertivo na consecução dos objetivos da biblioteca universitária, comungados com sua missão e a missão da instituição ao qual está vinculada.

Nota-se que grande parte do acervo das bibliotecas universitárias está em suporte papel, embora já se verifiquem informações em suporte eletrônico e digital. A política deve contemplar, também, a manutenção e salvaguarda desses suportes tidos como especiais. A existência de diversos recursos informacionais, quer seja em formato impresso, eletrônico ou digital, convivem relativamente de forma harmônica, mas não estão isentos de sofrerem ações do tempo, agentes biológicos e físicos.

A exemplo do papel, um suporte que, a pesar dos avanços tecnológicos, ainda exerce um amplo predomínio na sociedade, por ser um produto de origem orgânica, “é um elemento altamente sensível a calor, umidade, irradiação luminosa, infestação e demais efeitos deteriorantes do meio ambiente” (GOMES, 2006, p. 13).

Nesse sentido, a extensão da vida das coleções, por meio de ações preventivas, e armazenamento adequado, se efetiva no momento em que a biblioteca toma ciência da relevância da preservação e conservação de acervos, por parte dos envolvidos na instituição devendo, para tanto, incluir, em seus processos de planejamento, políticas de salvaguarda que estabeleçam diretrizes, normas, procedimentos que garantam a manutenção do acervo documental, de forma que possa atingir seus objetivos.

Assim como sugere Mesquita (2012, p. 68): "A elaboração de um plano diretor voltado para as coleções, com diretrizes a curto, médio e longo prazo, minimizaria problemas decorrentes de término de mandatos ou de questões políticas".

A inexistência de ações de preservação e conservação tem gerado muita preocupação para as bibliotecas universitárias que lidam com este tipo de acervo, devido a sua degradação e precariedade ambiental, gerando dificuldade no compartilhamento da informação. Para Yamashita e Paletta (2006, p. 173):

> a conservação e a preservação dos acervos garantem o imprescindível acesso à informação tanto em arquivos quanto em outras unidades de informação. O estado em que se encontram os acervos documentais e bibliográficos de instituições públicas e privadas é o que nos leva a enfatizar a importância de se adotar uma política de preservação, que é a melhor garantia contra a deterioração das coleções, sendo, a higienização a primeira ação efetiva para estender a vida útil desses documentos.

A preservação de acervos bibliográficos e documentais requer manutenção sistemática, estabelecimento de ações preventivas, bem como correção de possíveis danos que o documento possa apresentar. Desse modo, as normas, regras, diretrizes e práticas de preservação e conservação dos acervos documentais, proporciona uma maior e melhor proteção aos documentos, quer no formato físico, quer no digital. Estes, consequentemente, se convertem em um bem de grande relevância histórica, cultural e científico conferindo-lhes uma maior autenticidade, confiabilidade, bem como uma maior durabilidade, de modo a garantir o acesso à informação.

Preservar a memória científica é um processo complexo que exigirá dos gestores, e seus colaboradores da organização, sensibilização no sentido de um olhar mais atento ao valor intrínseco ao patrimônio científico e cultural da instituição.

3.2.2 Política de Indexação

Uma política de indexação estabelece regras, critérios relacionados a atividades de representação temática (classificação) e descritiva (catalogação) dos documentos. Estabelece procedimentos que orientarão uma adequada representação do conteúdo informacional dos documentos, e da descrição do documento que geram pontos de acesso do mesmo, de maneira que o usuário obtenha, por meio de estratégias de busca, maior precisão e relevância na recuperação da informação que necessita.

Rubi (2012, p. 108) afirma que: "A elaboração de uma política de indexação deve ser uma ação desenvolvida no âmbito da administração da biblioteca, representada por uma filosofia que reflita os seus objetivos e que sirva de guia para os bibliotecários". A autora considera que a política de indexação é um importante elemento norteador para tomadas de decisões nas tarefas de determinação dos assuntos, que permite ao bibliotecário indexador realizar seu trabalho de maneira mais racional e objetiva.

De acordo com Carneiro (1985), para se implantar um serviço de indexação, é necessário observar um número considerável de variáveis que, por sua vez, irão afetar sobremaneira, o desempenho do serviço. A autora ressalta que a definição de tais variáveis, juntamente com o estabelecimento de princípios e critérios, guiam a tomada de decisões e estão relacionados aos objetivos da política de indexação, que visa: otimizar os serviços, racionalizar os processos e dar consistência às operações.

A atividade de indexação implica "a preparação de uma representação do conteúdo temático dos documentos" (LANCASTER, 1991, p. 1 - 2). Ao documento são atribuídos termos que servirão de pontos de acesso e que permitirão, por meio de uma busca por assunto, a recuperação e localização do item. O autor destaca que é uma atividade de descrição dos documentos e, por conseguinte, gera a representação destes. Esta atividade envolve a seleção e atende a certos critérios, como o assunto tratado no documento, tipo de documento, língua, origem, que serão inclusos numa base de dados. Vale ressaltar que essa atividade está inserida nos processos de tratamento técnico do acervo e revela-se como um aspecto fundamental no acesso e uso das coleções.

Segundo Galvino (2012, p. 47), a indexação se constitui como "um dos pontos fundamentais no tratamento e recuperação da informação documentária, sendo entendida como a ação de descrever ou identificar um documento em relação ao seu conteúdo".

De acordo com Maciel e Mendonça (2006, p. 27), a função do processamento técnico

> [...] amplia a busca do leitor, se utiliza terminologia adequada e cruzamentos oportunos. É através dela que se estabelecem os catálogos, bases e demais recursos que permitem o rastreamento das informações e dos documentos. Fornece o verdadeiro suporte para a realização das pesquisas documentais, a base da pesquisa científica.

Esse processo é regido por normas, previamente elaboradas, que consistem na análise temática (classificação) e análise descritiva (catalogação) dos documentos.

Para Carneiro (1985, p. 222): "O principal propósito de um sistema de indexação é assegurar da forma mais eficiente e econômica possível, que qualquer documento ou informação seja fornecido ao usuário no momento preciso. " A referida autora ressalta que no estabelecimento de uma política de indexação, é necessário considerar elementos imprescindíveis para se planejar um sistema de recuperação da informação. Tais elementos referem-se:

> - a identificação da organização à qual estará vinculado o sistema de indexação;
> - a identificação da clientela a que se destina o sistema;
> - os recursos humanos, materiais e financeiros (CARNEIRO, 1985, p. 229).

Carneiro (1985, p. 229) considera que um sistema de recuperação da informação implica uma série de decisões, ligadas aos processos envolvidos no sistema e que afetarão seu desempenho. Para a autora, é necessário considerar, na elaboração da política de indexação, os seguintes elementos: cobertura de assunto; seleção e aquisição dos documentos-fonte; processo de indexação – nível de exaustividade e nível de especificidade; escolha da linguagem; capacidade de revocação e precisão; estratégia de busca; tempo de resposta do sistema; forma de saída; avaliação do sistema.

Fujita (2012, p. 24) afirma também que: "A principal justificativa da indexação é a necessidade de recuperação da informação". E destaca que o processo de indexação envolve um conjunto de variáveis, como a especificidade, exaustividade e correção, estas, por sua vez, podem contribuir de forma positiva ou negativa no processo de recuperação da informação.

Nota-se, portanto, que um sistema de indexação de assuntos é uma função de extrema relevância para a biblioteca, ou serviços de informação que, se bem desempenhada, favorecerá o acesso, recuperação e uso da informação. Ligado a este processo está também o adequado armazenamento e arranjo das coleções no espaço físico da biblioteca.

Rubi (2012) ressalta que compete às bibliotecas perceberem a relevância da indexação no processo que envolve o ciclo documentário, e deve-se considerá-la como parte da

administração, em que pese o estabelecimento de parâmetros que possam guiar os indexadores na tomada de decisão, durante o processo de catalogação de assuntos, de forma a minimizar subjetividades e incertezas, e reconhecerem a importância da implantação de uma política de indexação.

Entende-se que a política de indexação, em sua essência, é um instrumento de grande valia para a biblioteca, que por meio de normas e procedimentos, padronização dos processos, resulta na qualidade na representação do conteúdo informacional das coleções, de modo que este possa ser recuperado.

3.2.3 Política de atendimento: circulação e referência

Uma vez que as coleções estão devidamente organizadas, adequadamente armazenadas e prontas para uso, segue-se o momento em que a biblioteca disponibiliza acesso "[...] para o usuário real e virtual e, com ele, as avaliações sobre eficácia de tudo o que foi feito anteriormente [...]" (MACIEL; MENDONÇA, 2006, p. 32). De acordo com as autoras, a relação usuário-biblioteca possibilitará a mensuração da qualidade e eficácia dos serviços.

O serviço de atendimento na biblioteca tem grande relevância, e este, como os demais, está regido por políticas, normas, regras que regulamentam o acesso às coleções, uso dos serviços e produtos, e se constitui, para tanto, de uma atividade fim na organização, e está inserido no processo de dinamização e divulgação das coleções. A política de atendimento tem o propósito de atender às demandas informacionais dos usuários e estabelecer um canal de comunicação eficaz e eficiente, de forma que possibilite frequentes avaliações no sentido de melhorar a qualidade dos serviços.

Neste contexto, está inserido o serviço de referência, constituído de atividades direcionadas a promoção da biblioteca, desde a divulgação dos seus serviços e produtos, à orientação e educação de usuários, disseminação da informação, orientações para acesso e uso do acervo, do sistema de informação, das bases de dados, portais eletrônicos de pesquisa científica e demais outras fontes de informação, implantação de programas de incentivo à leitura, eventos, exposições.

Segundo Accart (2012, p. 303-304), atualmente as bibliotecas, dado ao avanço das tecnologias digitais e redes informacionais, convivem com a existência do serviço de referência presencial (local) e a distância (em linha – por meio da *Internet*). O primeiro, refere-se ao "Serviço de recepção, de informação de orientação e de pesquisa de informações numa biblioteca ou serviço de documentação". O segundo corresponde ao "Serviço em linha

(a partir do sítio da instituição na *Internet*) que oferece os mesmos serviços que um serviço de referência presencial". Também pode ser chamado de balcão virtual de referência à distância. O autor ressalta que é um serviço completo, que apresenta característica que diferem dos outros serviços da biblioteca: como o empréstimo, empréstimo entre bibliotecas, catalogação, classificação e indexação.

O serviço de referência, como tantos outros serviços oferecidos pela biblioteca, requer o profissional bibliotecário especializado e qualificado (bibliotecário de referência) para atuar na orientação ao usuário da informação e melhor utilização dos recursos informacionais. Fonseca (2007, p. 51) destaca que: "Ao bibliotecário compete não mais classificar e catalogar livros – operações realizadas por um serviço central e cooperativo devidamente computadorizado – e sim orientar usuários, fornecendo-lhes a informação que seja do interesse de cada um".

Neste sentido, de acordo com Accart (2012, p. 16): "O profissional de referência domina um conjunto de técnicas, de habilidades". Este deve conhecer o acervo que gerencia, e recursos informacionais, quer seja local, disponíveis em demais serviços e bibliotecas, e outras fontes de informação. Desse modo, o acesso à informação passa a existir a partir de um tema específico, e não se limita mais ao suporte.

Trata-se de um serviço que progrediu bastante, alinhado ao avanço tecnológico, redes digitais informacionais e ao progresso científico, que requereu da biblioteca universitária um redimensionamento nos processos de organização, disseminação, acesso e uso da informação científica, para melhor se adequarem as transformações no campo da ciência e tecnologia, e atenderem as suas demandas.

Vale ressaltar que este serviço pode se diferenciar entre as bibliotecas, mas em sua essência, o processo de atendimento continua voltado às necessidades informacionais específicas dos seus usuários. Na perspectiva de ressaltar a relevância do serviço de referência, Grogan (1991, p. 22) afirma que:

> O trabalho de referência, [...] é muito mais do que uma técnica especializada ou uma habilidade profissional. Trata-se de uma atividade essencialmente humana, que atende a uma das necessidades mais profundamente arraigadas de espécie, que é o anseio de conhecer e compreender.

Segundo Grogan (1991, p. 34), o serviço de referência caracteriza-se como a pedra angular da prática bibliotecária e considera um serviço ímpar de assistência efetiva às necessidades informacionais do usuário por "envolver uma relação pessoal, face a face, que o

torna o mais humano dos serviços da biblioteca [...]". Além disso, o esforço despendido não se torna debalde, pois se aplica a resposta de uma necessidade informacional específica do usuário.

Accart (2012, p. 32) destaca no serviço de referência a política de referência, que é um instrumento que faz parte da política de informação da biblioteca, e se constitui a partir da missão, objetivos e metas da instituição. Ele apresenta três objetivos estabelecidos pela política de referência:

- O serviço de referência reflete a imagem da instituição [...] "deve, em especial, cuidar, no que diz respeito ao lugar físico, de sua localização estratégica, da organização do espaço, e de sua sinalização"[...]. Importante manter uma coleção com fontes de informação impressas e digitais, contar com profissionais qualificados, com capacidade para relacionar-se bem;
- O serviço de referência deve constituir-se como polo de excelência na recepção, orientação e pesquisa. Refletindo-se na excelência da qualidade na instituição, que precisa contar com recursos humanos, financeiros e materiais, primar pela qualidade do serviço, apoiado em qualidades profissionais, humanas e sociais. Dever adotar critérios de qualidade no que tange a recepção, orientação e pesquisa de informação;
- O serviço de informação como agente intermediador das necessidades informacionais e as fontes de informação. Tendo como figura central, o usuário, no serviço de referência (ACCART, 2012).

Como o serviço de referência está voltado para uma atitude de orientação ao usuário, e considerando suas diversas funções, que de acordo com Accart (2012, p. 33), são a "recepção, orientação, informação, pesquisa de informações, capacitação de usuários, etc.", ele sugere que este "é o primeiro ponto de contato com o usuário e representa a instituição. " Desse modo, o bibliotecário de referência busca valer-se de todos os recursos disponíveis para o atendimento às necessidades informacionais expressa pelo usuário.

A circulação é um outro serviço de informação, e está destinado ao controle das coleções no que diz respeito a consultas e empréstimo domiciliar, e entre bibliotecas, dos materiais informacionais. Como nos demais outros serviços da biblioteca, este também possui política de circulação das coleções, com regras, critérios que regulamentam o serviço de circulação dos materiais.

Maciel e Mendonça (2006) apresentam, a seguir, algumas decisões que consideram pertinentes ao processo de circulação dos materiais informacionais que corroboram na efetiva qualidade do serviço:

> - Condições de acesso ao acervo (livre, fechado, restrito a alguns grupos etc.) que seja o mais adequado à clientela da biblioteca, e ao perfil das coleções; Determinação do sistema mais adequado para controle do uso e movimentação das coleções;
> - Estabelecimento de critérios que nortearão o regulamento do serviço de circulação (direitos e deveres do usuário);
> - Organização de coleções em regime de reserva (critérios de circulação diferentes dos estabelecidos no regulamento geral);
> - Adoção do sistema de circulação dirigida para coleção de periódicos;
> - Época e frequência (sic) do levantamento de dados para a expedição de avisos aos leitores em atraso;
> - Determinação e aplicação de penalidade;
> - Período de validade de matrículas;
> - Necessidade de estudo de uso das coleções para subsidiar políticas de desenvolvimento de coleções e desbastamento;
> - Adoção de programas de automação das atividades de circulação.
>
> (MACIEL; MEDONÇA, 2006, p. 38).

Nota-se, para tanto, que os processos envolvidos no serviço de atendimento, devem estar em conformidade com as diretrizes, contempladas na política de modo que estes processos possibilitem disponibilizar a informação científica, e atender às necessidades informacionais da comunidade universitária e da sociedade, cumprindo, a biblioteca universitária, sua missão de prestar suporte informacional aos programas de ensino, pesquisa e extensão, constituídos como o tripé da universidade.

4 SEGURANÇA DA INFORMAÇÃO

O cenário contemporâneo se apresenta como a “era do big data, em que volumes maciços de informação são gerados, armazenados, manipulados e compartilhados o tempo todo, entre todas as entidades que possamos imaginar [...]” (SÊMOLA, 2014, p. 20). Neste contexto, situam-se as organizações, que evidenciam um elevado grau de dependência da informação e das TIC.

Assim sendo, a informação torna-se um recurso indispensável nas organizações, quer sejam públicas ou privadas, que usam a mesma nos seus processos de tomada de decisões. Desse modo, as Instituições de Ensino Superior, enquanto promotoras do conhecimento e responsável pelo patrimônio documental, geram novos conhecimentos, exigindo cuidados especiais com este patrimônio.

Manoel (2014, p. 1) refere-se ainda a informação como “o resultado do processamento de dados, gerando algum tipo de conhecimento. Essa informação só é importante ou valiosa se fizer diferença para quem a manipula [...]”. Conforme o autor, a informação é um ativo da organização, que deve ser protegido, tanto quanto os bens físicos, pois ela torna-se fator de impacto em maior ou menor grau, constituindo-se elemento essencial na produção do conhecimento e desafio para as organizações na agregação de valor aos negócios e sua existência. O TCU (2012, p. 10) propõe que: “A informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico”.

Conforme Manoel (2014, p. 5): “A informação é um ativo valioso para as organizações e devem ter a sua adequada proteção, a fim de proporcionar melhores oportunidades competitivas no mercado em que atuam”. Para o autor, o maior dos desafios das organizações é transformar a informação em conhecimento que possa agregar valor aos negócios corporativos. Nota-se que, sendo a informação um ativo de valor, torna-se “um recurso crítico para a realização do negócio e a execução da missão da organização. Portanto, sua utilização deve ter regras e procedimentos”. (FONTES, 2006, p. 2) O estabelecimento das regras e procedimentos, se converte em instrumento de proteção da informação e minimização dos riscos aos processos gerenciais da organização:

> A informação é um componente representativo na sociedade do conhecimento, a qual surgiu como resultado do fenômeno conhecido como explosão informacional, distinguida pelo aumento quantitativo e acelerado

> nos processos de produção e disseminação da informação (BELARMINO; ARAÚJO, 2014, p. 7).

Sêmola (2014, p. 31) define ativo informacional como "tudo o que manipula direta ou indiretamente a informação, inclusive ela própria". Também se consideram como ativos "os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso" (BRASIL, 2015, p. 14). "Ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes" (ABNT NBR ISO/IEC 27002:2013, p. 04).

Atualmente, muitas organizações enfrentam um grande desafio que são os riscos à Segurança da Informação, e estes geram consequências danosas que refletem na responsabilidade corporativa, perda da credibilidade e trazem danos financeiros. Uma das principais prioridades na gestão das organizações tem sido a garantia da segurança da informação (BULGURCU; CAVUSOGLU; BENBASAT, 2010, tradução nossa).

> A segurança da informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas (FONTES, 2006, p. 11).

Na visão de Sêmola (2014, p. 4), a Segurança da Informação refere-se à "área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". O autor considera que esta área abrange, de forma mais ampla, as práticas relacionadas à gestão de riscos incidentes que podem ter implicações na consecução dos princípios básicos da segurança, a saber, a confidencialidade, integridade e disponibilidade.

De acordo com Bulgurcu, Cavusoglu e Benbasat (2010, p. 524, tradução nossa) o "sucesso em segurança da informação pode ser alcançado quando as organizações investem tanto em técnica e recursos sócio-organizacionais". Considera-se que os indivíduos envolvidos na organização são o elo mais fraco e por sua vez sujeitos aos ataques, relacionados ao uso da informação, quanto ao uso dos sistemas de informação. Silva e Stein (2007, p. 49) afirmam que: "As organizações estão cada vez mais cientes dos riscos de ataques a suas informações privilegiadas, porém, os indivíduos comuns e em alguns casos, até

mesmo órgãos do governo tendem a acreditar que é improvável que eles sejam alvo de ataque". Neste sentido, faz-se necessário perceber que:

> A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma companhia, é muito menos importante depois que elas são formalmente publicadas), porém a segurança da informação permanece importante em algumas etapas de todos os estágios (ABNT NBR ISO/IEC 27002, 2013, p. 6).

Ainda que as organizações lancem mão de aparatos tecnológicos na tentativa da redução dos riscos e de ameaças potenciais aos seus ativos, isto poderá não ser suficiente, pois a Segurança da Informação não está restrita ao uso dos recursos computacionais e redes digitais, mas abrange todas as informações produzidas e disseminadas nas organizações e recursos humanos.

No Brasil, em 2000, foi publicado o Decreto n. 3.505/2000, como marco da SIC (Segurança da Informação e Comunicação e SegCiber (Segurança Cibernética). Tal decreto institui a Política de Segurança da Informação para os órgãos e entidades da Administração Pública Federal (APF) e cria o Comitê Gestor da Segurança da Informação (CGSI), cuja atribuição é de assessoramento da Secretaria-Executiva do Conselho de Defesa Nacional (CDN), de modo que sejam executadas as diretrizes da política, avaliação e análise relacionadas aos objetivos de que trata o decreto. Esse decreto dá início ao Marco do Governo Brasileiro no panorama da SIC e SegCiber, que institui outros marcos legais, normativos e institucionais relativos à segurança da informação (BRASIL, 2015).

Nota-se que o governo federal tem empreendido esforços no enfretamento dos desafios atuais, em face da grande interconectividade global que, apesar desses esforços, gera riscos e ameaças às infraestruturas tecnológicas da informação e de redes, com considerável aumento de incidentes de fraudes, roubos de dados e ataques, que afetam a sociedade como um todo. Para tanto, é instituída a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (APF) – 2015/2018, versão 1.0 (desdobrada da Instrução Normativa GSI/PR n.° 01/2008), como instrumento de apoio aos órgãos e entidades governamentais com o objetivo da melhoria da "segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais" (BRASIL, 2015, p. 11).

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) coordena e integra a SIC e SegCiber, e tem como finalidade a apresentação de diretrizes

estratégicas no planejamento de segurança da informação e comunicação e segurança cibernética na esfera da APF. A presente "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal – 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008, coordenada e integrada pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR, tem a finalidade de apresentar as diretrizes estratégicas para o planejamento de Segurança da Informação e comunicações e de segurança cibernética no âmbito da APF, objetivando a articulação e a coordenação de esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento da área no Governo e a mitigação dos riscos aos quais encontram-se expostas as organizações e a sociedade (BRASIL, 2015).

A SIC e SegCiber se consolidam como uma função estratégica de Estado, como instrumentos de preservação e manutenção das infraestruturas críticas dos países, abrangendo as áreas de: energias, água, finanças, telecomunicações, transportes, informação, bem como os direitos do cidadão, a privacidade e soberania. Ressalta-se, ainda, além da responsabilidade do Estado brasileiro, a importância do setor privado, no que corresponde a SIC e SegCiber, que provêm serviços ao Governo e sociedade, detendo parte das infraestruturas de telecomunicações e redes de comunicações digitais (BRASIL, 2015).

Segue Quadro 8 explicativo dos conceitos adotados na "Estratégia de Segurança da Informação e Comunicação e de Segurança Cibernética na Administração Pública Federal" para melhor compreensão.

Quadro 8 – Conceitos adotados na Estratégia de Segurança da Informação, Comunicação e de Segurança Cibernética

a) Segurança da Informação e Comunicações (SIC)	Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
b) Segurança Cibernética (SegCiber)	A arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas.
c) Ativos de Informação	São os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
d) Infraestruturas Críticas	São as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

Fonte: Adaptado para Quadro de Brasil (2015).

A segurança da informação tornou-se uma abordagem necessária que foi ganhando rapidamente prioridade tanto nas organizações da administração pública, quanto nas da iniciativa privada, que tem sido potencializada pelo acelerado avanço das TIC, a "explosão da informação" e a expansão dos meios de comunicação. Desse modo, percebe-se que a informação tem seu papel de destaque nas organizações, pois se configura como um recurso de mobilização dos processos organizacionais e gerador de desenvolvimento. Desse modo, caracteriza-se como um recurso estratégico, crucial na garantia da sobrevivência das organizações. Nota-se, portanto, que a informação é utilizada pelas pessoas e ainda que esta, possa vir a se encontrar em ambiente tecnológico (digital), sua segurança se processa por meio dos indivíduos no ambiente convencional.

Atualmente, estas organizações dependem cada vez mais das tecnologias digitais e da informação, nos seus processos decisórios, no intuito de garantir continuarem desenvolvendo-se e manterem-se competitivas. A proteção da infraestrutura tecnológica, patrimonial, e os fluxos de informação, na rede digital, bem como no que diz respeito aos controles de acesso físicos e lógicos, torna-se uma necessidade imperativa para o ambiente organizacional.

Nesta perspectiva, destaca-se as iniciativas do Tribunal de Contas da União - TCU (2012) na abordagem da Segurança da Informação, que no intuito de avaliar a segurança da informação (na gestão e uso da TI na APF) no âmbito da administração pública, lança em 2007 levantamento em Governança de TI, com a finalidade de avaliação da qualidade que os órgãos públicos dão no tratamento das informações sob sua responsabilidade. Utilizou-se à época, como critério de avaliação da governança em TI, a norma 17799:2005 (substituída atualmente pela 27002) quanto à Segurança da Informação. Esse levantamento teve como base questionário com 39 perguntas, aplicado a 255 órgãos e entidades da APF. Essa ação possibilitou conhecer a situação crítica que estes órgãos apresentam em relação à segurança da informação.

A partir de então, o TCU (2012), através do acórdão 1.603/2008-Plenário, recomenda orientação acerca da importância da Gestão da Segurança da Informação (GSI), na promoção de ações, através de normatização que possibilite o estabelecimento ou aperfeiçoamento de: continuidade do negócio, gestão de mudanças, gestão de capacidade, classificação da informação, gerência de incidentes, análise de riscos, gerenciamento da Segurança da Informação, Política de Segurança da Informação (PSI) e controle de acesso.

Ressalta-se que outros dois levantamentos foram realizados (2010 e 2012), mas já se utilizando a ISO/IEC 27002, baseados em questionários mais abrangentes. O levantamento de 2010 resultou no Acórdão 2.308/2010-TCU-Plenário e constatou-se que não houve melhoras

com relação aos indicadores de Segurança da Informação, em comparação ao levantamento de 2007. O de 2012 (Acórdão 2.585/2012-TCU-Plenário) apresentou evidências que expressaram o não cumprimento das recomendações dos Acórdãos. Os três levantamentos realizados, evidenciaram, junto às instituições pesquisadas, fragilidades no que corresponde a abordagem da Segurança da Informação na APF. Tais levantamentos resultaram em publicação que objetiva apresentar "boas práticas em segurança da informação" a pessoas que interagem em ambientes informatizados "desde profissionais de TI envolvidos com segurança de informações até auditores, usuários e dirigentes preocupados em proteger o patrimônio, os investimentos e negócios da instituição, em especial, os gestores da Administração Pública Federal" (TCU, 2012, p. 7).

Apresenta-se, também, o CERT (Centro de Estudos, Resposta e Treinamento de Incidentes de Segurança no Brasil), que se alinha a ações de tratamento de incidentes ligados à segurança de redes de computadores conectados à *Internet* brasileira. Desse modo, "Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato" (CERT.br). Nota-se que, com a expansão da *Internet*, e o volume exponencial de informações e recursos, aumentou o número de pessoas e instituições conectadas, emergindo desse fato problemas relacionados a incidentes que se apresentam em forma de ataques a computadores e sistemas de informação conectados à rede. Conforme Quadro 9.

Quadro 9 - Descrição das categorias de incidentes reportados ao CERT.br

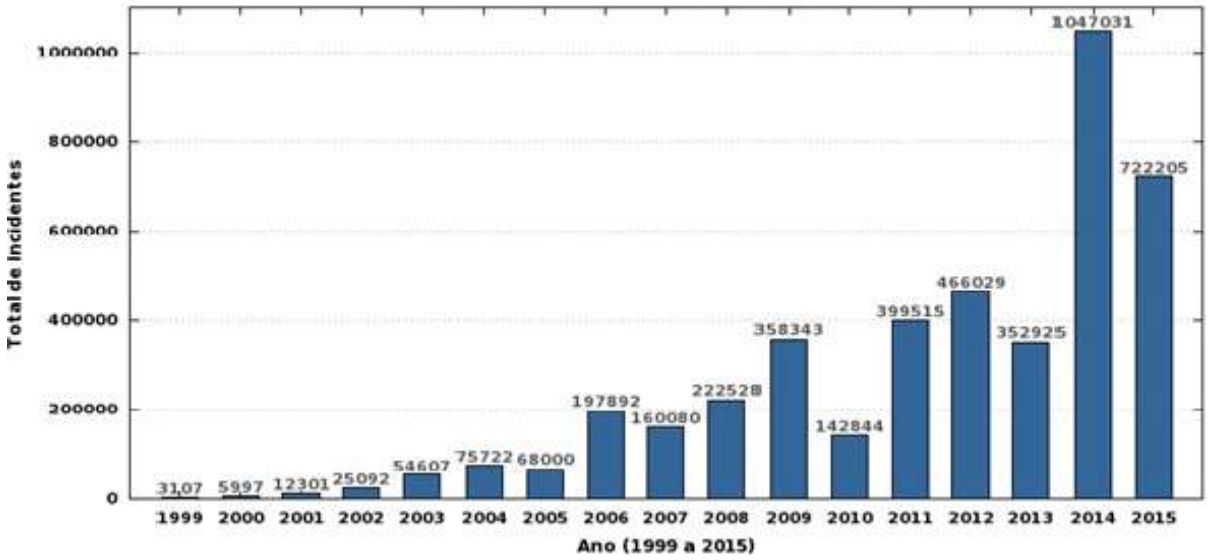
Descrição das categorias de incidentes reportados ao CERT.br	
worm	Notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
dos	(DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
invasão	Um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.
web	Um caso particular de ataque visando especificamente o comprometimento de servidores *Web* ou desfigurações de páginas na Internet.
scan	Notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
fraude	Segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

outros	Notificações de incidentes que não se enquadram nas categorias anteriores.

Fonte: Adaptado para Quadro de CERT.br (2016).

Em 2015, o CERT.br, recebeu 722.205 notificações ligadas a incidentes na rede, distribuídos nas categorias: Ataques a servidores *WEB,* Ataques de Navegação de Serviços, Tentativas de Fraude, Varreduras e Propagação de Códigos Maliciosos, Computadores Comprometidos e outros. Vale ressaltar que esse total é 31% menor que em 2014 (CERT.br). Tais incidentes recaem sobre a Segurança da Informação nas Instituições, bem como às pessoas conectadas à rede, resultando em danos que podem impactar de forma negativa negócios corporativos, sistemas de informação institucionais e privados, bem como à privacidade dos indivíduos. A seguir, apresenta-se a estatística das notificações de incidentes reportados ao CERT.br:

Figura 2 – Estatística de incidentes reportados ao CERT.br



Fonte: CERT.br (2015).

Um incidente considerado como um megaciberataque, foi o ocorrido em 12 de maio de 2017, que atingiu, pelo menos, 74 países. De acordo com o CERT.Br (2017, documento eletrônico sem paginação), foram registradas mais de 57 mil invasões *hackers "*a Sistemas de comunicação de empresas e serviços públicos em diferentes países – como Alemanha, Brasil, Espanha, Filipinas, Japão, Rússia e Turquia, entre outros[...]" em que na tela dos computadores "mensagens aparecem pedindo o pagamento em *bitcoins* (moedas virtuais) equivalentes a US$ 300 (R$ 940) para reativar o sistema — valor que subiria com o passar do

tempo". Tipo de ataque classificado como *ransomware*, e ocorre no momento que um usuário, sem se dar conta, baixa um arquivo infectado por vírus, e toda a rede é contaminada.

Na visão da *Information Systems Audit and Control Association* (ISACA) – Associação de Auditoria e Controle de Sistemas de Informação (2012), a Segurança da Informação na organização se baseia no princípio da garantia da proteção da informação "contra a divulgação a usuários não autorizados (Confidencialidade), a modificação imprópria (integridade) e não-acesso quando necessário (disponibilidade) ".

> • Confidencialidade significa preservar restrições autorizadas de acesso e divulgação, incluindo meios para proteger a privacidade e informações confidenciais.
> • Integridade significa proteção contra modificação de informações impróprias ou destruição, e inclui a garantia de informações não-repúdio e autenticidade.
> • Disponibilidade significa garantir o acesso oportuno e de confiança e uso da informação (ISACA, 2012, p. 18, tradução nossa).

Desse modo, entende-se a necessidade da GSI como prática que se aplica na garantia dos seus princípios básicos "integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição" (TCU, 2012).

Para Beal (2004, p. 83), a Segurança da Informação (SI) está relacionada às etapas do fluxo informacional, portanto, inserida na gestão da informação que está "voltada para a coleta, o tratamento e a disponibilização da informação que dá suporte aos processos organizacionais" para o alcance dos objetivos institucionais. Segundo a referida autora, a segurança da informação tem como objetivo a garantia da proteção da informação com base nos seguintes requisitos:

> **Sigilo** (proteção contra divulgação indevida), **integridade** (proteção contra a modificação não autorizada de informação), **autenticidade** (garantia de que a informação seja proveniente da fonte à qual ela é atribuída), **disponibilidade** (garantia de que as informações e serviços importantes estejam disponíveis para os usuários quando requisitados) e **irretratabilidade da comunicação** (proteção contra a alegação por parte de um dos participantes de uma comunicação de que a mesma não ocorreu) (BEAL, 2004, p. 52).

Segundo Araújo (2009, p. 41), a obtenção da segurança da informação se dá pelo estabelecimento de processos de implementação de uma série de controles, expressos através de políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*. E ressalta que tais controles se aplicam aos vários grupos das 10 seções da norma ISO IEC

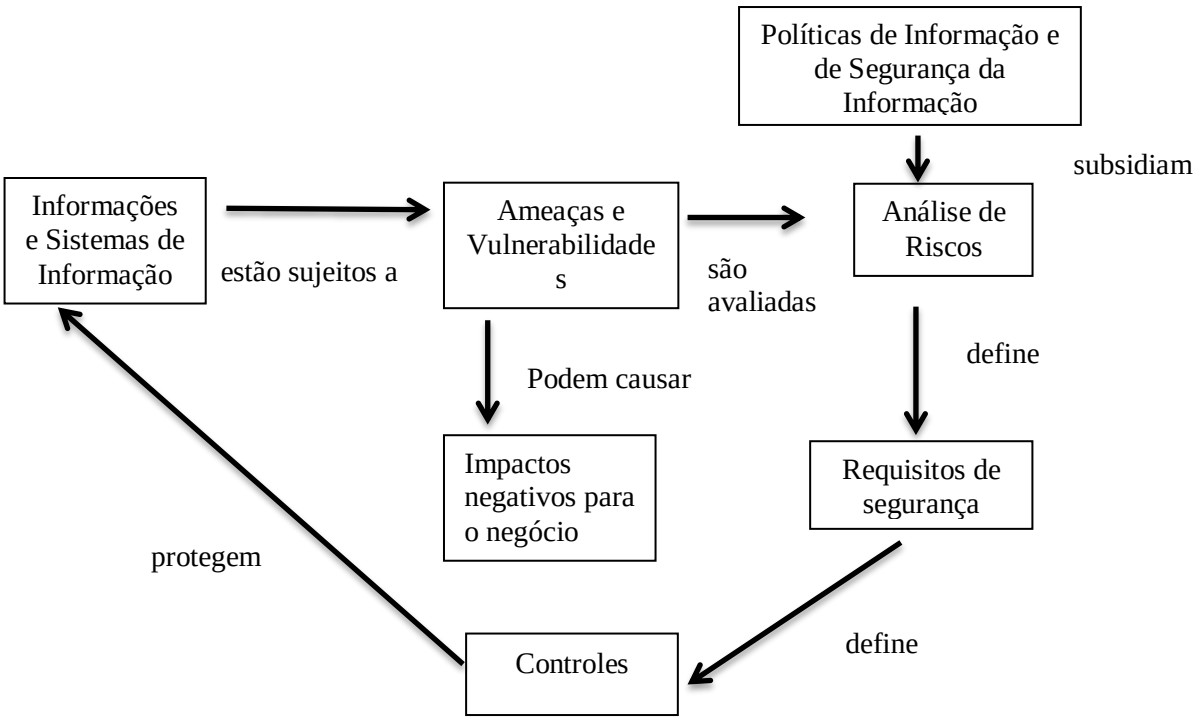
27001, estes controles, por sua vez, são estabelecidos para que a organização possa garantir que sejam atendidos os objetivos em Segurança da Informação.

O autor considera, ainda, que o cenário da SI é agravado por vários fatores, devido à dependência que as organizações têm com relação aos sistemas de informação e serviços, o que as tornam ainda mais vulneráveis às ameaças, em que pese a expansão da interconexão das redes, quer seja pública ou privada, fato este que favoreceu o aumento do compartilhamento de recursos informacionais, o que dificultou o controle de acesso, pois os sistemas de informação, em sua maioria, não foram pensados na perspectiva da segurança.

4.1 GESTÃO DE SEGURANÇA DA INFORMAÇÃO (GSI) E SISTEMA DE GESTÃO DA INFORMAÇÃO (SGSI)

Nota-se que a proteção da informação como um todo, bem como da infraestrutura tecnológica, e a conscientização da necessidade dessa proteção, está inserida na área da GSI e torna-se um imperativo no contexto das organizações. A seguir, na Figura 3, a autora apresenta um esquema com a visão geral dos principais elementos da gestão da segurança da informação:

Figura 3 – Principais elementos da Gestão da Segurança da Informação



Fonte: Beal (2004, p. 53).

De acordo com a Instrução Normativa GSI/PR nº 01 (BRASIL, 2008) a Gestão de Segurança da Informação e Comunicações refere-se a

> ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações (BRASIL, 2008).

Nesse sentido, as normas, diretrizes, procedimentos, se constituem em um conjunto de elementos de grande relevância no processo de geração, armazenamento, uso e disseminação da informação por parte de seus usuários no âmbito da organização. Sem esses elementos, a GSI torna-se inviável, impossibilitando à organização obter resultados positivos e significativos, pois é preciso um entendimento sobre o que seja a SI, para que se possa planejar estratégias de ações na proteção dos ativos de informação.

Fontes (2006, p. 11) apresenta os princípios básicos da proteção da informação, acrescido de outros. Neste sentido, a proteção da informação pressupõe o cumprimento desses princípios que devem ser cumpridos e possam garantir a SI.

Quadro 10 - Princípios básicos da proteção da informação

Disponibilidade	A informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.
Integridade	A informação deve estar correta, ser verdadeira e não estar corrompida.
Confiabilidade	A informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia.
Legalidade	O uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contatos, bem como com os princípios éticos seguidos pela organização e desejados pela sociedade.
Auditabilidade	O acesso e uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.
Não repúdio da auditoria	O usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Fonte: Adaptado para quadro de Fontes (2006, p. 11).

A informação é encontrada em diversos suportes, quer sejam físicos ou digitais, é compartilhada por meios eletrônicos ou via correio convencional, e mesmo no ambiente convencional da organização, desse modo recomenda-se medidas adequadas de proteção.

Assim, como afirma Fontes (2006, p. 10): “Para que a proteção da informação seja eficaz no dia-a-dia da organização, os conceitos e os regulamentos de segurança devem ser compreendidos e seguidos por todos os usuários”. Isto se aplica pela adoção da norma ISO/IEC 27001 Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos (ABNT NBR ISO/IEC 27001, 2013), que foi criada para o provimento de requisitos necessários para o estabelecimento, implementação, manutenção e melhoramento de um Sistema de Gestão de Segurança da Informação (SGSI). Esta norma está alinhada com as entidades de padronização e normatização internacionais ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*). Tais requisitos são genéricos e aplicáveis a todas as organizações, independentemente de seu tipo, porte ou natureza de seus negócios. A propósito:

> A adoção de um SGSI é uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. São esperados que todos estes fatores de influência mudem ao longo do tempo (ABNT NBR ISO/IEC 27001, 2013, p. 4).

Segundo Ferreira e Araújo (2008, p. 54) o SGSI ou *Information Security Management System* (*ISMS*) “é o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação”.

O SGSI é, portanto, um instrumento necessário para a organização, que deve ser encarado como parte integrada aos processos organizacionais, e considerada em sua estrutura administrativa global, de modo que a SI possa ser considerada no planejamento, controles e sistemas de informação, de maneira que possibilite o atendimento aos requisitos de segurança da informação. Assim sendo:

> O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados (ABNT NBR ISO/IEC 27001, 2013, p. 4).

Na perspectiva de um melhor entendimento do contexto organizacional, das necessidades e expectativas dos interessados, que implicam no SGSI e SI, tem-se que “A organização deve determinar as questões internas e externas que são relevantes para o seu

propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação" (ABNT NBR ISO/IEC 27001, 2013, p. 5).

Neste contexto, se posiciona a GSI, que possui normas técnicas destinadas à segurança em tecnologia da informação, e código de práticas em gestão da segurança da informação, elaborado pela NBR ISO/IEC 27002:2013, da Associação Brasileira de Normas Técnicas (ABNT).

Conforme NBR 27001(ABNT NBR ISO/IEC 27001, 2013) no planejamento do SGSI é necessário que a organização determine questões externas e internas, as necessidades e expectativas das partes interessadas, para a consecução de ações que possibilitem identificar os riscos e oportunidades. São fatores relevantes na SI:

> Pela inclusão de uma variedade de processos de melhoria contínua, um SGSI permite que os responsáveis tenham ferramentas para monitorar e controlar seus sistemas de Segurança da Informação, minimizando, assim, o risco do negócio e garantindo que a segurança cumpra o objetivo estratégico da organização com conformidade legal (MANOEL, 2014, p. 112).

No escopo da normatização e direcionamento na área de SI, no que se refere ao Sistema de Gestão da Segurança da Informação (SGSI), a Norma complementar 02/IN01/DSIC/GSIPR/2008 (BRASIL, 2008), estabelece a metodologia de gestão de segurança da informação e comunicações baseada no processo de melhoria contínua, denominado ciclo **"PDCA"** *(Plan-Do-Check-Act)*, referenciado pela norma ABNT NBR ISO/IEC 27001:2006. Esta metodologia deve ser "complementar aos primeiros processos de Gestão de Segurança da Informação e Comunicações, previstos na IN 01 GSI, de 13 de junho de 2008, a serem implementados pelos órgãos e entidades da Administração Pública Federal, direta e indireta".

Segundo Manoel (2014, p. 59), o ciclo *PDCA* teve sua origem na década de 1929, cujo idealizador foi Walter Andrew Shewhart (inventor do controle estatístico da gestão de qualidade). Tendo como disseminador e responsável pela melhoria contínua dos processos produtivos nos Estados Unidos, William Edward Deming, na década de 1950. Este modelo serviu de referência na melhoria contínua dos sistemas de gestão no mundo, de maneira que sua aplicação possibilitou por muito tempo as melhorias no campo da SI.

A partir da evolução do mercado, e aprendizado dos profissionais de SI, clientes, fornecedores, esse modelo evoluiu naturalmente para um modelo de gestão de *Plan – Do – Check – Lern*, sendo que *Act* é substituído por *Learn* (aprender). O autor ressalta a relevância da aprendizagem nesse ciclo, bem como em toda a esfera da organização e assevera que o

conhecimento é fator determinante das diretrizes a serem seguidas, que perpassam pela execução, verificação ou auditoria. Assim: “Sem aprender não há como planejar, sem planejar não há como executar, sem executar não há como verificar e auditar, e sem verificar e auditar não há como aprender [...]” (MANOEL, 2014, p. 60). O Quadro 11 mostra o modelo *PDCA* aplicado aos processos do SGSI:

Quadro 11 - Etapas do PDCA e suas definições

Plan (planejar) (estabelecer o SGSI)	Estabelecer política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente a política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria do SGSI.

Fonte: ABNT NBR ISO IEC 27001 (apud FONTES, 2012, p. 35).

O Quadro 12 explicita o planejamento de SGSI que contempla os risco e oportunidades na segurança da informação:

Quadro 12 – Planejamento de SGSI

Ações para contemplar riscos e oportunidades	**Avaliação de riscos de segurança da informação**
a) assegurar que o Sistema de Gestão da Segurança da Informação pode alcançar seus resultados pretendidos; b) prevenir ou reduzir os efeitos indesejados; e c) alcançar a melhoria contínua. A organização deve planejar: a) as ações para considerar estes riscos e oportunidades; 1) integrar e implementar estas ações dentro dos processos do seu sistema de gestão da segurança da informação; e 2) avaliar a eficácia destas ações.	A organização deve definir e aplicar um processo de avaliação de riscos de segurança da informação que: a) estabeleça e mantenha critérios de riscos de Segurança da Informação que incluam: 1) os critérios de aceitação do risco; e 2) os critérios para o desempenho das avaliações dos riscos de Segurança da Informação; b) assegure que as contínuas avaliações de riscos de Segurança da Informação produzam resultados comparáveis, válidos e consistentes; c) identifique os riscos de Segurança da Informação: 1) aplicando o processo de avaliação do risco de Segurança da Informação para identificar os riscos associados com a perda de confidencialidade,

	integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação; e 2) identifique os responsáveis dos riscos. d) analise os riscos de segurança da informação: 1) avalie as consequências potenciais que podem resultar se os riscos identificados em 6.1.2 c) 1) forem materializados 2) avalie a probabilidade realística da ocorrência dos riscos identificados em 6.1.2 c) 1); e 3) determine os níveis de risco; e) avalie os riscos de segurança da informação: 4) compare os resultados da análise dos riscos com os critérios de riscos estabelecidos em 6.1.2 a); e 5) priorize os riscos analisados para o tratamento do risco.
Tratamento de riscos de Segurança da Informação. A organização deve definir e aplicar um processo de tratamento dos riscos de segurança da informação para: a) selecionar, de forma apropriada, as opções de tratamento dos riscos de segurança da informação, levando em consideração os resultados da avaliação do risco; b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação; c) comparar os controles determinados em 6.1.3 b) acima com aqueles do Anexo A a e verificar que nenhum controle necessário tenha sido omitido; d) elaborar uma declaração de aplicabilidade que contenha os controles necessários (ver 6.1.3 b) e c), e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles do anexo a; e) preparar um plano para tratamento dos riscos de segurança da informação; f) obter a aprovação dos responsáveis pelos riscos do plano de tratamento dos riscos de segurança da informação, e a aceitação dos riscos residuais de segurança da informação;	**Objetivo de Segurança da Informação e planos para alcançá-los** A organização deve estabelecer os objetivos de segurança da informação para as funções e níveis relevantes. Os objetivos de segurança da informação devem: a) ser consistentes com a política de segurança da informação; b) ser mensurável (quando aplicável); c) levar em conta os requisitos de segurança da informação aplicáveis, e os resultados da avaliação e tratamento dos riscos; d) ser comunicados; e e) ser atualizado, conforme apropriado. A organização deve reter informação documentada dos objetivos de segurança da informação. Quando do planejamento para alcançar os seus objetivos de segurança da informação, a organização deve determinar: a) o que será feito; b) quais recursos serão necessários; c) quem será responsável; d) quando estará concluído; e) como os resultados serão avaliados.

Fonte: Adaptado para quadro de ABNT NBR ISO/IEC 27001 (2013).

Neste contexto de abordagem do processo de SGSI, destaca-se, ainda, a *Information Systems Audit and Control Association* – Associação de Auditoria e Controle de Sistemas de Informação (ISACA), entidade líder mundial na área de fornecimento de "conhecimento, certificações, comunidade, advocacia e treinamento em garantia e segurança de sistemas de

informação (SI), governança corporativa e gestão de TI, bem como risco e conformidade de TI" (ISACA, 2012).

O ISACA elaborou o *COBIT* (*Control Objectives for Information and Related Technology* - Objetivos de Controle para Informações e Tecnologia Relacionada), um modelo corporativo que permite às organizações, na governança e gestão de TI, de estrutura de controles internos, a partir do entendimento e gerenciamento de riscos que estejam associados ao uso de TI. Este modelo, atualmente na versão COBIT5, permite que as organizações possam atingir seus objetivos associados à governança corporativa e gestão de TI, através de processos e habilitadores no apoio à criação de valor para a organização. Considera-se, ainda, que cada organização possui objetivos diferentes, de maneira que o modelo permite ser personalizado e adequar-se ao contexto organizacional, através de cascata de objetivos, em que os objetivos corporativos são traduzidos em alto nível para objetivos de TI específicos e gerenciáveis, de forma que possam ser mapeados na prática de processos específicos. (ISACA, 2012, p. 15)

Quadro 13 – Princípios do COBIT 5

1º Princípio: Atender às Necessidades das Partes Interessadas
Organizações existem para criar valor para suas Partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos.
2º Princípio: Cobrir a Organização de Ponta a Ponta
- O COBIT 5 integra a governança corporativa de TI organização à governança corporativa; - Cobre todas as funções e processos corporativos; O COBIT 5 não se concentra somente na 'função de TI', mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo por todos na organização; - Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, de ponta a ponta, ou seja, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização.
3º Princípio: Aplicar um Modelo Único Integrado
Há muitas normas e boas práticas relacionadas a TI, cada qual provê orientações para um conjunto específico de atividades de TI. O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como um modelo unificado para a governança e gestão de TI da organização.
4º Princípio: Permitir uma Abordagem Holística
Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização.

Fonte: Adaptado para quadro de ISACA (2012).

Neste modelo, são trabalhados quatro princípios, a saber: 1) atender às necessidades das partes interessadas, 2) cobrir a organização de ponta a ponta, 3) aplicar um modelo único integrado, 4) permitir uma abordagem holística. Um conjunto de habilitadores (elementos que

venham a auxiliar na consecução dos objetivos corporativos) é definido pelo COBIT5, no apoio a organização, na implementação de sistema gestão e governança de TI. São sete as categorias definidas pelo modelo: Princípios, Políticas e Modelos, Processos, Estruturas Organizacionais, Cultura, Ética e Comportamento, Informação, Serviços, Infraestrutura e Aplicativos, Pessoas, Habilidades e Competências.

Para Isaca (2012, p. 15):

> A informação é um recurso fundamental para todas as organizações e a tecnologia desempenha um papel significativo desde o momento que a informação é criada até o momento em que ela é destruída. A tecnologia da informação está cada vez mais avançada, tornando-se pervasiva nas organizações e nos ambientes sociais, públicos e corporativos.

Nota-se que a função básica da SI é a proteção dos ativos de informação, de maneira que os riscos sejam minimizados a níveis toleráveis. É uma área também responsável na elaboração do plano de continuação dos negócios (FERREIRA, ARAÚJO, 2008). Numa visão mais ampla, Sêmola (2014, p. 5) considera a SI "como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação".

Nesta perspectiva, entende-se que, pela não observância e cumprimento às normas, regras, procedimentos relacionados à SI, advêm problemas, gerados por incidentes de segurança que incidem na garantia dos princípios básicos de SI, a saber: integridade, disponibilidade, acessibilidade, confidencialidade e autenticidade da informação, por meio da exploração das vulnerabilidades existentes na organização no que concerne à proteção da informação em ambiente convencional (organização) e nas redes digitais (*Internet*, sistemas de informação, etc.).

É necessário considerar que os incidentes de SI não se restringem ao âmbito dos sistemas informacionais e redes digitais, mas se encontram no ambiente convencional da organização, em que pese atividades ligadas à geração, tratamento, uso e disseminação da informação conforme já abordado em capítulo anterior.

Conforme Bonilla e González (2012), no mercado contemporâneo, as organizações devem basear-se no uso constante de sistemas de informação nos seus processos corporativos na tomada de decisões, o que faz emergir a necessidade de proteção dessa infraestrutura tecnológica que possa garantir sua permanência e competitividade nos negócios. Por vezes, algumas organizações dispõem de poucos recursos para investir em tecnologias, o que não justifica deixar de se investir em segurança.

Nota-se, que o investimento em SI é fator primordial para o sucesso das organizações, pois diante do cenário de massificação do uso das redes digitais, e sistemas de informação, cresceu o número de serviços baseados em informação, de maneira que as organizações precisaram redimensionar seus processos para lidar com o manejo desse recurso, que se tornou relevante para o seu desenvolvimento.

De acordo com Bonilla e Gonzáles (2012, p. 7, tradução nossa), paralelo a esses acontecimentos, "surgiram indivíduos que realizam atividades ilegais com o objetivo de invadir os fluxos de informação privados e confidenciais, fazendo que essas redes se convertam em um ambiente inseguro". Para os autores, isso implica que as organizações, bem como as pessoas que nelas atuam, não estão isentas dos riscos de ataques internos e externos, pois apresentam, por vezes, vulnerabilidades que afetarão a integridade, confidencialidade e disponibilidade das informações, até que se tenha o conhecimento ou sistema de detecção dessas ameaças e possa se implementar ações de controle desses incidentes de segurança. Diante do exposto, é importante destacar que:

> [...] na sociedade da informação, com a difusão da Internet e o desenvolvimento das Tecnologias da Informação e Comunicação (TIC), as empresas se utilizam cada vez mais da rede mundial de computadores como principal canal para geração de negócios, ampliando, dessa forma, a possibilidade de incidentes no ciclo de vida da informação (criação, manuseio, armazenamento, transporte e descarte), podendo comprometer os resultados organizacionais (SILVA; ARAÚJO; AZEVEDO, 2013, p. 38).

Ressalta-se que incidentes de Segurança da Informação decorrem das vulnerabilidades, que são fragilidades, exploradas pelas ameaças que, por meio dos riscos, possibilitam as ações maliciosas de atacantes. O incidente está ligado a "uma atividade através da utilização de recursos de processamento e do acesso às informações que afeta, em qualquer instância, a confidencialidade, a integridade ou a disponibilidade" de informações ou ativos de informação (FERREIRA; ARAÚJO, 2014, p. 117). Para os autores, qualquer evento que seja adverso, confirmado ou mesmo sob suspeita, pode estar relacionado à segurança de sistemas ou redes de computadores e pode ser definido como incidente de segurança.

Os riscos relacionados à SI, evoluem e se intensificam, e evidenciam a ação de invasores cada vez mais sofisticados e qualificados no uso das ameaças e tecnologias do futuro, enquanto que as organizações, numa batalha geralmente ineficaz, ainda se fiam em estratégias de segurança do passado em um cenário expresso pela expansão da superfície de

ataque, incluindo parceiros, clientes, fornecedores e outros grupos, em que se evidencia o crescente volume de dados que fluem pelos canais digitais do ciberespaço (PWC, 2014).

De acordo com a Pesquisa Global de Segurança da Informação 2016 (PWC, 2016), com o permanente aumento das ameaças, torna-se uma das grandes preocupações de gestores das organizações e governos, o conhecimento e gerenciamento de riscos relacionados à segurança cibernética, na adoção de tecnologias inovadoras, do tipo segurança em nuvens, autenticação avançada na redução de riscos e melhorias nos programas cibernéticos (PWC, 2016).

Segundo o Relatório Anual da Rede Nacional de Ensino e Pesquisa (RNP), o ano de 2013 destacou-se no Brasil e no mundo, no âmbito da Segurança da Informação, como o ano em que mais se evidenciaram notícias que trouxeram discussões sobre a segurança de informações trafegadas na *web* e aos riscos aos quais pessoas e dados corporativos estão expostos, ataques de negação de serviço distribuído (DDoS *Distributed Denial of Service*), *botnets*[1], incidentes relacionados a roubo e vazamentos de informações sobre programas de vigilância norte-americanos, como o caso sobre as revelações do ex-analista da NSA, Edward Snowden e exploração de vulnerabilidades dos serviços essenciais das redes NTP e DNS (RNP, 2013 p. 5, documento eletrônico).

A partir de uma análise dos dados gerais das notificações de incidentes reportadas ao Centro de Atendimento a Incidentes de Segurança (CAIS), em 2013, evidenciou-se uma diminuição de 20% sobre o total de incidentes em comparação ao ano de 2012. O CAIS registrou, no ano de 2013, 106.724 incidentes, em comparação com 2012, que teve registros de 133.439 incidentes. A redução tem ênfase nos ataques relacionados às categorias Fraude, com queda de 42,8%, e Código Malicioso, com queda de 23,8%.

Tal diminuição se dá pela melhoria no processo de triagem que o CAIS tem investido, na aplicação de recursos e processos de tratamento das notificações, realizando um trabalho contínuo com ações voltadas à conscientização junto à comunidade sobre segurança da informação, detecção e tratamento de incidentes, bem como o crescente esforço das comunidades acadêmicas no aprimoramento da segurança em suas instituições (RNP, 2013 p. 8).

Conforme o CAIS em Resumo, em 2015, no segundo quadrimestre, foram geradas 157.317 notificações, com leve tendência de redução para 13% em comparação ao

[1] É uma rede de *bots*, um conjunto de dispositivos em rede (computadores, *tablets*, *smartphones* e outros) infectados com *bots* e controlados pelo atacante com direcionamento. (RNP, 2013 p. 8).

quadrimestre anterior. Para as notificações de incidentes foram 76% da categoria Código Malicioso e 9% na categoria Tentativa de Intrusão.

Nesse sentido, com vistas a diminuir gradualmente o número de notificações de vulnerabilidades, o CAIS, juntamente com equipes de segurança das instituições mais afetadas, tem executado projetos, através de ações conjuntas no tratamento das causas-raízes das vulnerabilidades, que impactam sobremaneira a rede acadêmica e de pesquisa (RNP, 2015). A Figura 4 apresenta as notificações de incidentes de SI nas instituições acadêmicas no ano de 2015, reportados ao CAIS.

Figura 4 - Notificações incidentes de Segurança da Informação

Fonte: CAIS em Resumo (2015).

Diante do exposto, Fontes (2012, p. 6) afirma: “A segurança da informação é um processo da organização e deve considerar a informação tanto no ambiente convencional quanto no ambiente de tecnologia”. Nesse processo, tanto o ambiente convencional, em que se evidencia o predomínio das informações em papel, quanto o ambiente pessoal, em que as informações se encontram na mente dos indivíduos, devem ser levados em conta. Esse processo existe para que a organização, em suas atividades estratégicas, táticas e operacionais, possa utilizar os recursos suportados pelas informações, de maneira confiável, e deve estar alinhado aos objetivos da organização, estes alcançados por meio de políticas e padrões.

Neste sentido, Fontes (2012, p. 9) ressalta que:

> O processo de segurança da informação somente terá sucesso se a sua implantação for uma decisão estratégica da organização e consequentemente a direção apoie explicitamente o desenvolvimento, a implantação e a manutenção deste processo de proteção da informação.

Neste contexto, é preciso considerar aspectos relevantes que implicam sobremaneira no planejamento de um modelo de Gestão da Segurança da Informação e que estão diretamente relacionados à "definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades" (SÊMOLA, 2014, p. 6).

De acordo com Sêmola (2014, p. 7), o modelo de GSI expressa um sentido mais amplo e deve considerar em primeiro plano os desafios do negócio corporativo como um todo. Esse modelo ressalta a importância de uma orientação na direção de uma autonomia dos conceitos autenticidade e conformidade (outrora referenciada como legalidade). Afirma, ainda, que a autenticidade tem sua origem nos precursores confidencialidade e integridade, e dada sua relevância no contexto atual, cumpre seu papel de sinalizar para o compromisso dos aspectos relacionados à informação e seus envolvidos, no processo de troca. Já a conformidade (*compliance*), componente do GRC (gestão da governança, risco e conformidade), tem como papel a garantia de que se faça cumprir as obrigações da organização, que envolve o compromisso que vai dos "*stakeholders* (investidores, empregados, credores, agências reguladoras etc.) a aspectos legais e regulatórios relacionados à administração das empresas" (SÊMOLA, 2014, p. 8). Para o autor, a conformidade possibilita a ampliação das fronteiras da legalidade, considerada um dos aspectos mais relevantes da segurança da informação.

Nesse sentido, dependendo dos objetivos que a organização queira alcançar, é preciso considerar os elementos essenciais relativos à prática de segurança da informação. Adiante, como reforço aos aspectos conceituais relacionados à GSI, quanto aos elementos relevantes associados à SI, apresenta-se o seguinte quadro, para uma melhor compreensão:

Quadro 14 – Conceitos considerados relevantes na abordagem da Segurança da Informação

Conceito	**Definição**
Autenticação	Processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação de elementos.
Conformidade	Processo de garantia do cumprimento de obrigações empresariais com *stakeholders* (investidores, empregados, credores etc.) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios éticos e de conduta estabelecidos com a alta direção das mesmas. Faz parte do tripé do GRC – modelo de gestão da governança, dos riscos e da conformidade empresariais.
Aspectos associados	
Autorização	Concessão de permissão para o acesso às informações e funcionalidades das aplicações aos participantes de um processo de troca de informações

	(usuário ou máquina), após a correta identificação e autenticação dos mesmos.
Autenticidade .	Garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e de que a mensagem ou informação não foi alterada após o seu envio ou avaliação. Diz respeito também, a um termo [utilizado normalmente na certificação digital – com utilização de recursos de criptografia[2] para atribuição de um rótulo de identificação].
Auditoria	Processo de coleta de evidências de uso dos recursos existentes, a fim de identificar as entidades envolvidas em um processo de troca de informações, ou seja, origem, destino e meios de tráfego de uma informação.
Severidade	Gravidade do dano que determinado ativo pode sofrer à exploração de uma vulnerabilidade por qualquer ameaça aplicável.
Relevância do ativo	Grau de importância de um ativo para a operacionalização de um processo de negócio.
Relevância do processo de negócio	Grau de importância de um processo de negócio para o alcance dos objetivos e sobrevivência de uma organização.
Criticidade	Gravidade referente ao impacto em relação ao negócio causado pela ausência de um ativo, pela perda ou redução de suas funcionalidades em um processo de negócio ou pelo seu uso indevido e não autorizado.
Irretratabilidade	Característica de informações que possuem a identificação do seu emissor, que o autentica como autor de informações por ele recebidas.

Fonte: Adaptado para quadro de Sêmola (2014, p. 10).

Entende-se que estes aspectos estão associados ao panorama evidenciado pelo avanço das TIC, expresso num contexto de fatores que apresentam por vezes ameaças (naturais, involuntárias e voluntárias) estas, por sua vez, exploram, através dos riscos, as vulnerabilidades ou fragilidades (Físicas, Naturais, de *Hardware, de Software*, Mídias, Comunicação e Humanas) que estão associadas aos ativos de informação das organizações, permitindo que um incidente de segurança - evento decorrente de uma ameaça - ocorra e gere impactos, que afetem de maneira negativa os princípios de segurança da informação: confidencialidade, integridade e disponibilidade (SÊMOLA, 2014).

Entende-se que há um número variado de vulnerabilidades, que não oferecem risco, se isoladas. No entanto, se estão ligadas a um agente causador (ameaças) ou condições que favoreçam a exploração das vulnerabilidades, é bem provável que venha a ocorrer o risco. Vale ressaltar que, a vulnerabilidade de maior significância no contexto da segurança, ainda é o elemento humano. Pois, não basta o desenvolvimento de tecnologias sofisticadas, se o fator humano não estiver em foco, como coparticipante no desenvolvimento de cultura de segurança da informação, por meio de programas de conscientização e educação.

[2] "Ciência e arte de escrever mensagens em forma cifrada ou em código [...]" (CERT.Br, p. 67).

A seguir, no Quadro 15, apresenta-se a definição dos elementos associados a vulnerabilidades que, por suas vezes, implicam diretamente na prática de segurança da informação e que devem ser considerados na GSI.

Quadro 15 – Elementos associados à Segurança da Informação

Ameaças	
Conceito	**Definição**
Ameaças	São agentes ou condições que causam acidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade. Quanto a sua intencionalidade, classificam-se em:
Tipos de Ameaças	
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 *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.
Vulnerabilidades	
Conceito	**Definição**
Vulnerabilidades	São fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade. [...] por si só, não provocam incidentes, pois são elementos passivos, necessitando de um agente causador ou condição favorável, que são as ameaças. A seguir exemplos de vulnerabilidades:
Tipos de Vulnerabilidades	
Físicas	Instalações prediais que não atendem às boas práticas ou normas e regulamentações vigentes; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em ambientes com ativos ou informações estratégicas; controle de acesso deficiente em locais contendo informações confidenciais ou sensíveis etc.
Naturais	Ambientes com equipamentos eletrônicos próximos a locais 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.
Hardware	Computadores são suscetíveis à poeira, umidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados, com falhas ou flutuações no suprimento energético ou aumento excessivo na temperatura ambiente.
Software	Erros na codificação, instalação ou configuração de sistemas e aplicativos podem acarretar acessos indevidos, vazamento de informações, perda de dados e de trilhas de auditoria ou indisponibilidade do recurso quando necessário.
Mídias	Discos, fitas, relatórios e impressos podem ser perdidos ou danificados; falhas de energia podem causar panes em equipamentos, podendo danificar trilhas lógicas de dados; discos rígidos usualmente têm vida útil; a radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
Comunicação	A comunicação telefônica é vulnerável a escutas (acesso indevido) ou problemas na infraestrutura física ou lógica que impeçam de ser estabelecida.
Humanas	Falta de treinamento ou de conscientização das pessoas, falta de avaliação psicológica adequada ou verificação de antecedentes (*backgraund check*) que identifique objetivos escusos ou problemas anteriores, ou mesmo má-fé

	ou o descontentamento de um funcionário, entre outros, podem levar ao compartilhamento indevido de informações confidenciais, à não execução de rotinas de segurança ou erros, omissões etc. que ponham em risco as informações.
Conceito	**Definição**
Risco	Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios.
Impacto	Abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócios.
Incidente	Fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.
Medidas de Segurança	
Conceito	**Definição**
Medidas de segurança	São as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, reduzir essas vulnerabilidades, limitar a probabilidade ou impacto de sua exploração, minimizando ou mesmo evitando os riscos. São referenciadas também como controles.
Características das medidas de segurança	
Preventivas	Têm como objetivo evitar que os incidentes venham a ocorrer. Visam garantir a segurança por meio de mecanismos que estabeleçam a conduta e a ética na instituição. (Ex.: políticas de segurança, instruções e procedimentos de trabalho, campanhas e palestras de conscientização de usuários, especificações de segurança, equipamentos de controle de acesso, ferramentas para implementação da política de segurança (*firewall*, antivírus, configurações adequadas de roteadores e dos sistemas operacionais.).
Detectivas	Visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. (Ex.: análise de riscos, sistemas de detecção de intrusão, alertas de segurança, câmeras de vigilância, alarmes, etc.
Corretivas	Ações voltadas à correção de uma estrutura tecnológica e humana para que se adapte às condições de segurança estabelecidas pela instituição ou voltadas à redução dos impactos: equipes para emergências, restauração de *backup*, plano de continuidade operacional, plano de recuperação de desastres.

Fonte: Adaptado para quadro de Sêmola (2014, p. 13).

Ainda no âmbito da segurança da informação, e principalmente da segurança patrimonial, tem-se no aspecto relacionado a controles de acesso, a abordagem da teoria do perímetro que, segundo Sêmola (2014, p. 43), trata-se de "estrutura de segmentação de ambientes físicos [...] considerada estratégia militar de defesa e também se aplica ao cenário atual das empresas [...]". Para o autor, é uma estrutura que permite que se vá além dos aspectos físicos e possa ser aplicado na segmentação de ambientes lógicos. E afirma que a "segmentação inteligente dos ativos" é o grande segredo na obtenção do melhor retorno dos mecanismos de garantia dos níveis de proteção da informação, o que possibilita aplicação

adequada dos controles, com níveis dosados de proteção, de forma que possa atender às necessidade e demandas de segurança.

> Além do perímetro estar associado à compartimentalização de espaços físicos e lógicos, ele também cumpre o importante papel de alerta e de mecanismo de resistência distribuído por áreas, a fim de permitir que tentativas de acesso indevido e invasão gerem sinais de alerta e se deparem com a resistência que propiciará tempo para que medidas contingenciais sejam tomadas antes que a ação avance ainda mais em direção ao alvo (SÊMOLA, 2014, p.59).

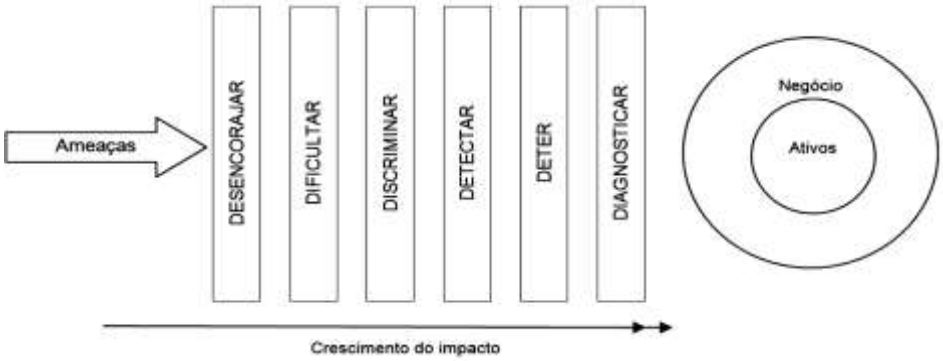
De acordo com Sêmola (2014, p. 54) considerando a amplitude e complexidade da área de segurança, os desafios são comumente estudados por camadas ou fases, de maneira a tornar mais claro o entendimento de cada uma das camadas. A essa divisão dá-se o nome de barreiras de segurança, que são seis. Cada uma dessas barreiras tem uma expressiva relevância no objetivo de redução dos riscos, e é necessário um dimensionamento adequado que direcione a uma interação e integração corretas. É um modelo conceitual que implementa a teoria do perímetro e segmenta perímetros físicos e lógicos, oferece níveis complementares e crescentes de resistência e proteção. Adiante, o autor define cada uma das seis barreiras:

> **Barreiras da Segurança da Informação:**
>
> **Barreira 1: desencorajar**
> Tem a função de desencorajar as ameaças. Que por sua vez, podem sofrer desmotivação ou perda de interesse e estímulo na tentativa de quebra da segurança através de mecanismos físicos, tecnológicos ou humanos (ex.: câmera de segurança, aviso de alarmes, divulgação da política de segurança, treinamento de funcionários, com informações sobre práticas de auditoria e monitoramento de acesso aos sistemas, nessa fase, já são efetivos.
>
> **Barreria 2: dificultar**
> Essa barreira complementa a anterior através da adoção efetiva dos controles que dificultarão o acesso indevido. (ex.: dispositivos de controle de acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético).
>
> **Barreira 3: discriminar**
> Cerca-se de recursos que permitem identificar e gerir os acessos, definindo perfis e autorizando permissões.(ex.: processos de avaliação e gestão do volume de uso dos recursos, como e-mail, impressora ou até mesmo o fluxo de acesso físico aos ambientes.
>
> **Barreria 4: detectar**
> Age de forma complementar às suas antecessoras. Deve munir a solução de segurança de dispositivos que realizem, alertem e instrumentem os gestores da segurança na detecção de situações de risco, seja em uma tentativa de invasão, seja em uma possível contaminação por vírus, o descumprimento da

> política de segurança da empresa ou cópia e envio de informações sigilosas de forma inadequada.
>
> **Barreia 5: deter**
> Representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento dessa barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. (ex.: medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas.
>
> **Barreria 6: diagnosticar**
> Essa fase tem o sentido especial de representar a continuidade do processo de gestão de segurança da informação. Mesmo sendo a última barreira, é o elo entre a primeira barreira, criando um movimento cíclico e contínuo. É a barreira de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa. (SÊMOLA, 2014, p. 64)

Segundo Sêmola (2014, p. 74), um diagnóstico preliminar malconduzido, desprovido de metodologia e instrumentos, impossibilita uma precisão maior no processo de levantamento e análise de riscos, o que acarretará distorção no entendimento da situação de segurança com a situação desejada, aumentando, por sua vez, a probabilidade de um dimensionamento inadequado das barreiras, em que se percebe a distribuição dos investimentos de maneira desproporcional, ineficaz. Resultando na não correspondência entre o retorno no investimento e as expectativas da empresa que, por sua vez, não alcançará nível de segurança que se adéque as suas atividades. A Figura 5 apresenta um diagrama representativo das barreiras de segurança:

Figura 5 - Diagrama representativo das barreiras de segurança



Fonte: Sêmola (2003, p. 27).

A seção seguinte discorre sobre a segurança da informação, considerando seus aspectos históricos e conceituais, com vistas a uma melhor compreensão da evolução dos padrões de segurança da informação.

4.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: ASPECTOS HISTÓRICOS E CONCEITUAIS

Conforme Manoel (2014), as Normas ISO/IEC 27001 e 27002 advêm da ISO 17799 que, por sua vez, originou-se do BS7799 – (*British Standard* – Padrão Britânico). Essas normas são consideradas as primeiras normas internacionais como código de práticas em Segurança da Informação utilizadas no mundo por diversas organizações.

O autor ressalta que o primeiro órgão internacional a dar atenção especial à elaboração e divulgação de uma norma de Segurança da Informação, cuja fundação remonta a 1987, foi o DTI (*Departamento of Trade and Industry*) através da sua área comercial CCSC (*Commercial Computer Security Center*), no Reino Unido. Dentre as responsabilidades desse departamento, uma delas era auxiliar os fornecedores de produtos de segurança de TI na elaboração de critérios e requisitos para avaliação em SI, como forma de certificação das empresas inglesas ligadas a esse setor.

A partir de então, foi criado o ITSEC (*The Information Technology Security Evaluation Criterian*) e o código de boas práticas no apoio à implementação de ações em SI, e executadas através de controles de SI. Em 1995, o *British Standards Institution* publica, após período de consulta pública, a norma BS7799:1995, com a função de estabelecer-se como um

National Satandards Body (Corpo Nacional de Padrões) semelhante a função exercida pela ABNT no Brasil.

Com a evolução tecnológica, surge a necessidade de uma auditoria sobre a prática da norma pelas organizações. Cria-se, então, um código de práticas, como recomendações que tratavam da implantação dos controles de Segurança da Informação – BS7799:1995-1(código de práticas) e BS7799-2 (certificação – conjunto de controles essenciais). Essas publicações geraram proposta para a *International Organization for Standardization* (ISO) de se homologar uma norma ISO que fosse equivalente e que não se restringisse ao Reino Unido, mas que fosse válida internacionalmente. No ano de 2000 é publicada a ISO/IEC 17799:2000.

A partir desses acontecimentos, a ISO evoluiu o código de práticas em SI, gerando publicações que culminaram na série de padrões ISO/IEC 27000, com fim de auxiliar as organizações na padronização da norma em nível mundial, com a implantação e manutenção em SI, através de um código de boas práticas. Em 2005, a ABNT (Associação Brasileira de Normas Técnicas) traduz e publica, no Brasil, a norma ABNT NBR ISO/IEC 27002:2005 Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão de Segurança da Informação (tradução da antiga ISO/IEC 17799, 2005) e, em 2006, traduz e publica a. ABNT NBR ISO/IEC 27001:2006 Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos (substituta da BS17799:2002-2 – referente ao processo de certificação dos SGSI). Em 2013, novas versões da ISO/IEC 27001 e ISO/IEC 27002, são publicadas (MANOEL, 2014). Essas duas normas citadas são parte da família ISO/IEC 27000, que segundo a ABNT (2013) descreve a visão geral e o vocabulário do Sistema de Gestão da Segurança da Informação e referencia as normas da família do Sistema de Gestão da Segurança da Informação (incluindo a ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005), com termos e definições relacionados.

A Segurança da Informação tem sua abrangência em parte no ambiente da tecnologia da informação, de modo que este ambiente de tecnologia, está inserido no contexto organizacional, de forma que a proteção da informação e definição de diretrizes, ou seja, políticas e normas, torna-se um imperativo, para que as regras possam, de maneira estratégica e operacional, direcionar a existência desta proteção (FONTES, 2012).

> A necessidade de políticas internas de segurança da informação varia entre organizações. Políticas internas são especialmente úteis em organizações maiores e mais complexas onde aqueles que definem e aprovam os níveis esperados de controle são segregados daqueles que implementam os controles, ou em situações onde uma política se aplica a muitas pessoas ou funções diferentes na organização. Políticas de segurança da informação

> podem ser emitidas em um único documento, ‘política de segurança da informação’ ou como um conjunto de documentos individuais, relacionados (ABNT NBR ISO/IEC 27002, 2013, p. 9).

Para Beal (2004, p. 54): “A existência de uma política declarada de informação ajuda a organização de muitas formas, inclusive quanto à preservação dos princípios éticos de uso dos dados corporativos”. Nota-se que, a informação, precisa receber um tratamento adequado que perpasse pelo estabelecimento de políticas e regras, uma vez que, trata-se de um recurso tão importante quanto os demais existentes na organização. Nesta perspectiva, tem-se que:

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos (ABNT NBR ISO/IEC 27002, 2013, p. 4).

A partir desta perspectiva, entende-se que é o desenvolvimento de PSI na organização que, alinhada a sua missão e objetivo, passam a delinear ações estratégicas voltadas à segurança com vistas a mitigar os riscos e ameaças aos ativos de informação, no sentido de garantir que as informações geradas, processadas, armazenadas e disponibilizadas no âmbito das instituições, mantenham a integridade, a confidencialidade e a disponibilidade das informações.

Nesta mesma direção da proteção da informação, destaca-se a Norma ISO/IEC/ABNT 27002 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de Segurança da Informação (ABNT NBR ISO/IEC 27002, 2013) que está estruturada para dar suporte às atividades de GSI, fornecendo diretrizes às organizações, na prática da gestão da segurança da informação, e inclui a seleção, implementação e gerenciamento de controles considerando os ambientes que oferecem risco à segurança da informação. Essa norma traz recomendações quanto à elaboração, implementação e análise crítica da política de segurança da informação, que define de que maneira a organização precisa se posicionar com relação às categorias de controle da área de segurança. Os controles dizem respeito, como sugere Fontes (2012, p. 24), aos “elementos que definem o que a norma considera importante para um processo de segurança da informação na organização e devem ser os elementos considerados [...]” na PSI da organização (FONTES, 2012, p. 24). Desse modo:

> A política de segurança de informações deve conter princípios, diretrizes e regras genéricos e amplos, para aplicação em toda a instituição. Além disso, ela deve ser clara o suficiente para ser bem compreendida pelo leitor em foco, aplicável e de fácil aceitação. A complexidade e extensão exageradas da PSI pode levar ao fracasso de sua implementação. Cabe destacar que a PSI pode ser composta por várias políticas inter-relacionadas, como a política de senhas, de *backup*, de contratação e instalação de equipamentos e *software*s (TCU, 2012, p. 12).

A PSI, por ser um instrumento que define o curso de ação a ser seguido, contribui para a garantia do acesso à informação no âmbito das Instituições de Ensino Superior e, neste contexto, se insere a Biblioteca Universitária, sendo esta responsável pela difusão do conhecimento e depositária de conteúdos informacionais de inestimável valia para a pesquisa científica, para a aprendizagem e para a geração do conhecimento.

> A elaboração de uma política de segurança da informação (PSI) representa um passo fundamental no estabelecimento de um sistema de gestão de segurança da informação eficaz. A PSI é o documento que registra os princípios e as diretrizes de segurança adotados pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos (BEAL, 2008, p. 43).

Beal (2008) ressalta ainda que a PSI é um instrumento que formaliza aspectos relevantes quanto à proteção, controle e monitoramento dos ativos de informação, pois traça as linhas mestras para a implementação da SI, de maneira que incita à direção da organização, ao comprometimento com a proteção da informação e a criação de uma base de colaboração com os processos de identificação e tratamentos de riscos, junto a todos os integrantes. Bonilla e González (2012, p. 9, tradução nossa) reforçam ainda que:

> As políticas de segurança são uma demonstração do que pode ou não pode se fazer dentro da empresa, por isso deve contemplar, sem limitação:
> - O nome do proprietário da política e o responsável pela sua realização;
> - O grupo de pessoas que devem cumprir;
> - Apresentar a política, ter um procedimento claro e um objetivo;
> - Deve estabelecer sanções pelo descumprimento das políticas, o que lhe dará mais validade.

De acordo com Ferreira e Araújo (2008, p. 86), a PSI "deve capacitar a organização com instrumentos jurídicos, normativos e processuais. Esses instrumentos devem abranger as estruturas físicas, tecnológicas e administrativas [...]" de maneira que as informações

corporativas estejam em conformidade com os princípios de confidencialidade, integridade e disponibilidade.

A PSI "define um conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação" (FERREIRA; ARAÚJO, 2008, p. 36).

Neste sentido, estes autores compreendem:

> Deve-se utilizar uma visão metódica, criteriosa e técnica em seu desenvolvimento e elaboração, de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades e [...] na elaboração das políticas com o perfil da empresa e dos negócios que ela pratica (FERREIRA; ARAÚJO, 2008, p. 36).

É necessário observar que a PSI precisa expressar os anseios daqueles que são responsáveis pelas decisões que envolvem o destino dos recursos da organização, bem como dos que têm acesso e fazem uso da informação (FERREIRA; ARAÚJO, 2008). Assim: "A política de segurança da informação precisa refletir a preocupação da cúpula estratégica da organização, e, portanto, deve contar com a participação desta no processo de elaboração". (BEAL, 2008, p. 43)

Desse modo, a PSI se constitui um instrumento fundamental de "orientação e apoio às ações de gestão da segurança", e assume uma abrangência ampla, que está dividia como se percebe na citação:

> - **Diretrizes:** Possuem papel estratégico e devem expressar a importância que a organização dá aos ativos de informação, além de comunicar aos funcionários seus valores;
> - **Normas:** Segundo nível da política que detalha situações, ambientes, processos específicos e oferece orientação para o uso adequado das informações;
> - **Procedimentos:** Está presente na política em maior quantidade por seu perfil operacional. Descrição detalhada sobre como atingir os resultados esperados (FERREIRA; ARRAUJO, 2008, p. 86).

Nota-se, portanto, que a PSI tem papel de destaque na determinação de diretrizes e normas, em que se evidenciam aspectos relevantes na sua implementação. Ressalta-se que sua elaboração deve se antepor às ocorrências dos incidentes relacionados à segurança, ou após ocorrerem, de modo que reincidências possam ser evitadas, pois se constitui importante ferramenta na prevenção de problemas legais e instrumento de aderência a processos de

controle da qualidade (FERREIRA; ARAÚJO, 2014). Adiante, os autores apresentam os aspectos relevantes relacionados à implementação da PSI:

> - Estabelecimento do conceito de que as informações são um ativo importante da organização;
> - Envolvimento da Alta Administração com relação à Segurança da Informação;
> - Responsabilidade formal dos colaboradores da empresa sobre a salvaguarda dos recursos da informação, definindo o conceito de irrevogabilidade;
> - Estabelecimento de padrões para a manutenção da Segurança da Informação (FERREIRA; ARAÚJO, 2008, p. 36).

A ISO IEC 27002 (2013) em sua estrutura aponta as seguintes recomendações no que se refere à elaboração e implementação de política de segurança da informação:

> Controle
>
> Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
>
> Diretrizes para implementação
>
> Convém que no mais alto nível a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.
>
> Convém que as políticas de segurança da informação contemplem requisitos oriundos da:
> a) estratégia do negócio;
> b) de regulamentações, legislação e contratos;
> c) do ambiente de ameaça da segurança da informação, atual e futuro.
>
> Convém que a política de segurança da informação contenha declarações relativas a:
>
> a) definição da segurança da informação, objetivos e princípios para
> b) orientar todas as atividades relativas à segurança da informação;
> c) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
> processos para o tratamento dos desvios e exceções
> (ABNT NBR ISO/IEC 27002, 2013, p. 8).

A ISO IEC 27002 (2013), recomenda ainda para um nível mais baixo, a estruturação de políticas de tópicos específicos que sirvam de apoio à PSI, uma vez que estas exigem implementação de controles de segurança e são estruturadas na direção das necessidades de

grupos de interesse, e abrange tópicos específicos dentro da organização (ABNT/NBR/ISO/IEC, 2013).

> Exemplo de políticas com tópicos específicos:
> a) controle de acesso;
> b) classificação e tratamento da informação;
> c) segurança física e do ambiente;
> d) tópicos orientados aos usuários finais:
> 1) uso aceitável dos ativos;
> 2) mesa Limpa e Tela Limpa;
> 3) transferência de informações;
> 4) dispositivos móveis e trabalho remoto;
> 5) restrições sobre o uso e instalação de software;
> e) backup;
> f) transferência da informação;
> g) proteção contra *códigos maliciosos*;
> h) gerenciamento de vulnerabilidades técnicas;
> i) Controles criptográficos;
> j) segurança nas comunicações;
> k) proteção e privacidade da informação de identificação pessoal;
> l) relacionamento na cadeia de suprimento
> (ABNT NBR ISO/IEC 27002, 2013, p. 8).

Beal (2008) assevera que a PSI não pode ser um documento estático e para a efetivação de sua continuidade, é necessário o estabelecimento de mecanismos que possam garantir uma constante atualização, seu conteúdo periodicamente revisado, de forma que possa ser um instrumento de resposta a mudanças que se apresentam por meio de ameaças provenientes dos ambientes interno e externo, das vulnerabilidades inerentes aos ativos de informação e necessidades de negócio. A autora ressalta que não importa que processo seja adotado na produção da PSI, é fundamental que seja certificado, por parte dos dirigentes da organização, se sua versão final possui coerência com as diretrizes da organização, ou seja, sua missão, visão, valores e objetivos.

Para elaboração da PSI, é importante considerar que o seu foco seja nas questões de princípios, de modo que ela possa ter uma ampla abrangência, ou seja, não deve adentrar em questões técnicas, estas, por sua vez, devem ser tratadas nas normas internas, nas rotinas e procedimentos específicos.

No documento da PSI, em sua introdução, recomenda-se contextualizar a problemática da SI no que diz respeito ao contexto dos riscos, reforçando a relevância na proteção da informação e recursos computacionais, a necessidade de sua proteção contra ameaças, com ações de prevenção de elementos que possam intervir negativamente e causar destruição,

alteração indevida ou sua divulgação não autorizada. A atribuição das responsabilidades precisa ser clara, e deve estender-se a todos os níveis da organização.

Deve-se fazer um delineamento das responsabilidades nos aspectos de implementação, verificação da conformidade, auditoria e avaliação da segurança, de maneira que possam ser estabelecidas as orientações necessárias para que sejam implementadas todas as medidas de proteção.

O conteúdo da política de segurança da informação varia de acordo com as características da organização, seu porte, área de atuação, e outros. O documento da PSI deve abranger aspectos que considera relevantes na sua elaboração, caso necessário (BEAL, 2008, p. 44). O Quadro a seguir explicita tais aspectos:

Quadro 16 – Aspectos a serem considerados na elaboração da PSI

Organização da segurança	Definições sobre a estrutura de gestão adotada para administrar as questões de segurança da informação, com indicação de quem é responsável e presta contas pela segurança em todos os níveis da organização e quais as linhas hierárquicas existentes entre as funções de segurança.
Classificação e controle dos ativos	Orientações sobre realização de inventário dos ativos informacionais, formas de classificação da informação considerada crítica e responsabilidades pela manutenção dos controles necessários para protegê-la.
Aspectos humanos da informação	Definições sobre a política de segurança de pessoal (processos de admissão e demissão, requisitos de segurança aplicáveis a funcionários e prestadores de serviço, treinamento em segurança). Diretrizes do comportamento esperado em relação ao uso dos diversos tipos de recursos computacionais disponíveis (tais como e-mail, Internet, Intranet, sistemas de informação etc.) e em caso de ocorrência de uma quebra de segurança.
Segurança do ambiente físico	Diretrizes para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis do negócio contra acesso não autorizado, dano ou interferência.
Segurança do ambiente lógico	Diretrizes para garantir a operação correta e segura dos recursos computacionais e proteger a integridade dos serviços.
Segurança das comunicações	Diretrizes para a proteção de dados e informações durante o processo de comunicação.
Prevenção e tratamento de incidentes	Diretrizes para a prevenção, detecção, notificação, investigação e tratamento de incidentes de segurança, bem como para a emissão de relatórios a eles relacionados.
Desenvolvimento/aquisição, implantação e manutenção de sistemas	Diretrizes para o uso de controles de segurança em todas as etapas do ciclo de vida dos sistemas, incluindo o padrão mínimo de segurança a ser aplicado a todos os sistemas corporativos, e orientações a respeito do uso da avaliação de risco para a identificação dos sistemas que irão merecer medidas extras de proteção.
Gestão de continuidade do	Recomendações para que a organização se prepare para

negócio	neutralizar as interrupções às atividades organizacionais e proteja os processos críticos na ocorrência de uma falha ou desastre.
Conformidade	Diretrizes para a preservação da conformidade com requisitos legais (tais como proteção de direitos autorais e da privacidade), com as normas e diretrizes internas (incluindo o tratamento de informação proprietária) e com os requisitos técnicos de segurança. Procedimentos a serem adotados em caso de violação da política de segurança, e descrição das punições a que estão sujeitos os infratores (as quais podem ir de uma simples advertência a demissão e ação judicial).

Fonte: Adaptado para quadro de Beal (2008, p. 44).

Acenando para avaliação constante com vistas à melhoria e qualidade da PSI, a ISO IEC 27002 traz no item 5.1.2 (ABNT NBR ISO/IEC, 27002, 2013) recomendações que versam sobre a "análise crítica da política de segurança da informação, e criação da função do gestor de segurança da informação, que alinhada à Administração superior da organização se encarregará, a partir de programas de conscientização, treinamento, educação de comunicar a política aos funcionários e partes externas, de maneira que a PSI possa ser explícita, entendida e acessível a todos os seus usuários, não deixando margem para alegações de desconhecimento, quando da ocorrência de incidentes de segurança. A seguir são apresentadas as recomendações da NBR ISO IEC 27002 sobre a avaliação crítica da PSI:

> Controle
>
> Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
>
> Diretrizes para implementação
>
> Convém que cada política de segurança da informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança da informação.
>
> Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança da informação da organização e tenha um enfoque para gerenciar a segurança da informação em resposta às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente de tecnologia.
> Convém que a análise crítica das políticas de segurança da informação leve em consideração os resultados da análise crítica pela direção.
>
> Convém que seja obtida a aprovação da direção para a política revisada. (ABNT NBR ISO/IEC 27002, 2013, p. 10).

Segundo Beal (2008, p. 59) a informação, considerada do ponto de vista de seu conteúdo, se divide em três categorias: informação pessoal, informação de segurança nacional e informação de negócios, embora nas organizações não exista uma padronização para a classificação das informações.

Das questões relacionadas a controle da segurança da SI, a ISO 27002 (ABNT NBR ISO/IEC 27002, 2013, p. 23) trata ainda do assunto relacionado à gestão de ativos (item 8), que traz recomendações referentes à classificação e controle dos ativos de informação. Este processo tem como objetivo: "Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos". Recomenda-se, para tanto, "[...] que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido." (ABNT NBR ISO/IEC 27002, 2013, p. 23).

"Os inventários de ativos ajudam a assegurar que a proteção efetiva ocorra, e podem igualmente ser exigidos para outras finalidades, tais como a saúde e segurança, razões de seguro ou financeiras (gestão de ativos)" (ABNT NBR ISO/IEC 27002, 2013, p. 23).

No que se refere à classificação da informação, a ISO/IEC 27002 (ABNT/NBR/ISO/IEC 27002, 2013, p. 25) considera: "Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada". Objetivando: "Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização".

> A classificação da informação é processo de estabelecer o grau de importância das informações mediante seu impacto no negócio, ou seja, quanto mais estratégica e decisiva para a manutenção ou sucesso da organização, maior será sua importância. A classificação deve ser realizada a todo instante, em qualquer meio de armazenamento (FERREIRA; ARAÚJO, 2008, p. 78).

Na classificação da informação, é importante considerar a existência de regras cuja principal delas é a "determinação de proprietários para todas as informações, sendo este o responsável por auxiliar na escolha do meio de proteção. (FERREIRA; ARAÚJO, p. 78)

Para as informações cujo armazenamento se dê em qualquer espaço, precisam estar alinhadas aos critérios de classificação, e seu grau de sigilo possua uma identificação, que possa logo ser reconhecido (FERREIRA; ARAÚJO, 2008). O Quadro 17 apresenta um modelo de inventário dos ativos de informação que pode ser utilizado pela organização.

Quadro 17 – Inventário dos ativos de informação

NATUREZA DO ATIVO	ATIVOS DE INFORMAÇÃO
Informação	• Banco de dados e arquivos magnéticos • Documentos de sistemas e manual do usuário • Material de treinamento • Procedimentos operacionais de recuperação • Planos de continuidade
Documentos em papel	• Contratos • Documentação da empresa • Relatórios confidenciais
Software	• Aplicativos • Sistemas operacionais • Ferramentas de desenvolvimento • Utilitários do sistema
Físico	• Servidores, *desktops* e *notebook* • Impressoras e copiadoras • Mídias magnéticas • Gerador, nobreak e ar-condicionado • Móveis, prédios e salas
Pessoa	• Empregados, estagiários, terceiros e fornecedores
Serviço ou atividade	• Computação (aplicação de *patches*, *backup*) • Comunicação (ligações telefônicas, videoconferências) • Utilidades gerais

Fonte: Ferreira e Araújo (2008, p. 78).

Os autores ressaltam, ainda, que para um conjunto de informações armazenadas em um mesmo espaço, e que possuam níveis diferentes, o critério adotado será a classificação de todo o espaço, de forma que a informação possa ser classificada no mais alto nível.

Tanto os procedimentos como as políticas podem e devem ser adaptadas as necessidades e características de cada organização. Não seria diferente com as bibliotecas que sendo unidades de informação tem aspectos próprios do seu funcionamento e gestão, e estão sujeitas a diferentes tipos de ameaças a seus ativos informacionais.

4.3 SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS

Por ser um organismo considerado em constante desenvolvimento, numa evocação à 5ª Lei de Ranganathan, a biblioteca atua como uma organização que abriga registros do conhecimento em diversos suportes, expresso em coleções que vai de obras consideradas raras, quer por sua edição esgotada, quer pelo tempo de publicação, e outros, a obras em

formato digital, que cobrem diversas áreas do conhecimento, bem como, demais recursos informacionais que a biblioteca disponibiliza através de bases de dados, portais eletrônicos de pesquisa. Sem, no entanto, deixar de estar conectada com os avanços tecnológicos, de que tanto depende.

Este fator acaba por atrair a atenção de indivíduos sequiosos de obter a posse de tais materiais (burlando as regras de circulação), ou mesmo invadindo o sistema de informação da biblioteca, que, por meio de ações maliciosas, se aproveitam das vulnerabilidades que possivelmente possam existir na segurança. Isto tem sido tema de preocupação de gestores de bibliotecas, museus, arquivos e demais unidades de informação, que lidam com estes registros do conhecimento, que requerem ações que venham a garantir a segurança das coleções, bem como do ambiente destas organizações que lidam com a informação, quer seja em suporte físico, eletrônico ou digital.

Dessa forma, para a salvaguarda do acervo físico se utiliza, por exemplo: o guarda-volumes (para os usuários), as regras para o controle de acesso restrito aos acervos raros, as publicações periódicas científicas impressas, a restrição de acesso a acervos sobre artes (e outros tipos de materiais que possam vir a sofrer danos, extravios), a instalação de sistemas antifurto (sistemas de segurança eletrônicos) para acervos bibliográficos, com etiquetas (autocolantes e metálicas), ativadores (para magnetização), desativadores (para desmagnetização) e detectores (painéis ou portais de controle da saída indevida de materiais).

Conforme Lima (1995, p. 126): “Os melhores resultados de pesquisa sobre eficiência de sistemas de segurança eletrônicos para bibliotecas mostram que as perdas nas coleções podem ser reduzidas de 70 a 98%”. E ressalta que isto vai depender, é claro, da área protegida e a combinação com outros fatores de segurança, tais como a eficiência de funcionários no atendimento aos alarmes, colocação e ativação de etiquetas no controle de novas aquisições, prevenção de possíveis remoções ou desativações de etiquetas por parte de usuários mal intencionados, eficiência na segurança em instalações da biblioteca, como portas de controle de carga e descarga de materiais, entrada de funcionários, saídas de emergência, proteção de janelas e outros. Outro aspecto positivo é a abolição dos constrangimentos na verificação de bolsas, pertences pessoais de usuários ao saírem do interior da biblioteca (LIMA, 1995).

No entanto, Manini e Greenhalgh (2016), asseveram que a criação de sistemas de segurança contra roubo e furto não deve se limitar à instalação de câmeras de vigilância, alarmes e reforços na estrutura física de contenção. Mas isto tem sua implicação na institucionalização, por meio de documentos formais, de normas e regras, e o respeito que os participantes na instituição deverão ter às mesmas.

Quanto às bases de livros digitais, cada editor possui suas regras específicas para o direito de uso (no *download*, impressão) e controles de acessos, de acordo com as normas de direitos autorais. O sistema de informação que a biblioteca utiliza para o gerenciamento do acervo e atividades administrativas, também possui regras de uso e controle de acesso, com sistema de senhas (que nem sempre são criadas de forma segura), restrições e permissões específicas com perfis de usuários para operacionalização das atividades gerenciais do acervo (aquisição, catalogação, classificação, indexação, relatórios, estatísticas, disseminação da informação, pesquisa).

Roubos de livros, sobretudo os raros, peças de museu, documentos de arquivos, invasão a sistemas de informação, extravio de obras, foram sempre uma constante nas instituições que possuem unidades de informação. Já na Idade Média, nos mosteiros, como forma de impedir que livros valiosos fossem roubados por estudiosos, os abades costumavam prendê-los com correntes. Na contemporaneidade, obras raras estão em ameaças constantes, o que demonstra fatos como o roubo de livros em 2002, na Biblioteca da Suécia, e em 2012, na Biblioteca Girolamini, em Nápoles, de grande proporção, que foram motivos de uma conferência em 2015, na Biblioteca Britânica, como a participação de Bibliotecários, Livreiros e Antiquários, sob o ameaçador tema *The Written Heritage of Mankind in Peril* (Herança escrita da humanidade em perigo). Ressalta-se que esses dois roubos foram praticados por funcionários (OPINIÃO&NOTÍCIA, 2015).

Nota-se que o alvo são, em sua maioria, obras raras, documentos raros, peças valiosas, entre outros. A ação dos atacantes tem seu foco no elo mais fraco da corrente: as vulnerabilidades, como se trata em Segurança da Informação e segurança como um todo. O que denota a problemática da segurança que, muitas vezes, deixa a desejar, quer seja pelo pouco orçamento, ou descaso por parte de gestores que não acreditam que possam ocorrer riscos e ameaças à segurança de seus acervos e sistemas de informação.

No Brasil, temos relatos de roubos de obras valiosas, como o roubo de 24 livros raros datados do século 16 a 20, do Museu Nacional do Rio de Janeiro (ESTADÃO, 2004). Outro fato foi o roubo de 22 livros raros do Instituto de Botânica, na Zona Sul de São Paulo, por uma quadrilha (em fevereiro de 2012). Alguns dos exemplares foram estimados em US$ 60 mil dólares, por livreiros estrangeiros. Na ocasião: “Duas viaturas seriam deslocadas para levar até o instituto os 11 volumes de Flora fluminensis, cinco de Sertum palmarum brasileinsium, dois de Le Bambusées e exemplares de Graminearum genera, Herbarium amboinense, Plantarum brasiliae e Flora brasílica” (ESTADÃO, 2012). Estes fatos denotam a

ponta do *iceberg* da complexidade da segurança em Bibliotecas, Museus, Arquivos e outras Unidades de Informação.

No que se refere ao acervo de livros raros, a BC da UFPB possui uma coleção de livros raros, que atualmente encontra-se em processo técnico, mas não possui plano de segurança específico para este tipo de acervo. Manini e Greenhalgh (2016) asseveram que a maioria das instituições, que possuem acervo de livros raros, dificilmente contemplam em seus manuais, políticas, técnicas de análise bibliológica (descrição minuciosa do acervo, análise das características intrínsecas e extrínsecas da produção da obra), realização de inventários, ou mesmo regulamentos que possam estruturar rotinas de segurança para estas obras.

Deve-se considerar que, além das ameaças locais ou internas à segurança da informação, no que se refere aos acervos que se apresentam no edifício da biblioteca, faz-se necessário observar, a segurança de rede *web* que de acordo com Williams (2001, p. 13, tradução nossa) "é o processo de configuração de hardware de rede, computadores, software, e o ambiente físico para minimizar o risco de ataque a esses recursos", ou seja, é o processo de proteção da rede e *softwares*, de forma que se possa reduzir as chances de riscos à SI, e usuários (internos e externos) não estejam suscetíveis às ameaças digitais. Isto se aplica, para tanto, aos Sistemas de Informação das bibliotecas, bem como suas Bases de Dados e *sites*, que, por sua vez, podem ser alvos de ameaças externas (usuários, *hackers*, fornecedores), ou internos (funcionários), diante do contexto de conectividade da *Internet* em que a biblioteca está inserida, o que vai exigir medidas de segurança, na rede através, da implementação de Políticas de Segurança da Informação que possam minimizar potenciais perdas de dados, ataques aos sistemas de gerenciamento da informação e servidores locais e gastos financeiros com a manutenção da rede. Diante desse cenário, é evidente que

> controlar e reduzir incidentes tecnológicos e de segurança, dentre outros fatores, torna-se extremamente importante com a finalidade de assegurar a operação da rede em níveis aceitáveis de desempenho, além de manter os seus equipamentos de informática com softwares e aplicativos especializados, visando facilitar a comunicação e otimizar o fluxo da informação e do conhecimento, permitindo, assim, o aumento da eficiência e das condições de excelência das informações armazenadas no sistema utilizado pelas bibliotecas, seja no campo da pesquisa, do ensino, da extensão, da prestação de serviços de referência ou da gestão institucional (LIMA; ARAÚJO, SANTOS; BARBOSA, SANTOS, 2017, sem paginação).

Outro fator que merece ser observado com maior ênfase, é a segurança dos processos gerenciais da biblioteca que, precisam estar alinhados aos aspectos de SI, uma vez que, a proteção da informação, deve envolver a organização como um todo, considerando as dimensões pessoa, processo, tecnologia.

Nota-se, para tanto, que no ambiente da biblioteca, são muitas e constantes as ameaças potenciais e reais, que vão desde ameaças ambientais e físicas, ameaças lógicas, a ameaças relacionadas aos processos gerenciais e recursos humanos, sendo esta última, a mais crítica, considerando ser o fator humano, "o elo mais fraco" na segurança, uma vez que este não esteja fortalecido, capacitado para lidar com os problemas relacionados a SI. Neste contexto, além dos fatores de risco, devem ser considerados os usuários internos (funcionários) que, por desconhecimento, insatisfação, ou ignorar as medidas de segurança (quando expressas formalmente em políticas), acabam por fazer mau uso dos recursos informacionais, recursos de redes *web*, e causam danos a acervos, sistemas de informação, sistemas operacionais, estações de trabalho e outros. Quanto aos usuários externos, estes mal-intencionados, ou simplesmente por pura curiosidade, ou por não atentarem às políticas, com suas regras de uso da biblioteca, podem se posicionar como ameaças e comprometerem os serviços e produtos da biblioteca, através da exploração de possíveis vulnerabilidades em sua segurança.

Embora a biblioteca tenha suporte tecnológico, nem sempre se fazem presentes em sua rotina boas práticas, no que se refere à segurança da informação, seja no ambiente convencional ou virtual. Isto reforça a necessidade imperativa de planejamento direcionado à proteção da informação com foco em políticas de segurança, quer seja para seus processos gerenciais, quer seja para seus acervos, para seu Sistema de Informação, estações de trabalho e redes de acesso à *Internet*, uma vez que não há uma segurança absoluta, o que implica na constante renovação, reavaliação de tais políticas, na minimização dos riscos associados à segurança, de forma que a biblioteca esteja alinhada aos princípios básicos da SI: integridade, disponibilidade, acessibilidade, para que possa continuar na utilização eficaz dos recursos e garantia do acesso à informação. Nesta perspectiva, observa-se que:

> As BUS precisam e devem elaborar documentos que visem o estabelecimento de normas gerais de utilização dos equipamentos e recursos computacionais destinados à pesquisa, ao ensino, à extensão e as atividades administrativas das IES, afim de que as ameaças sejam evitadas e/ou amenizadas (LIMA; ARAÚNJO, SANTOS; BARBOSA, SANTOS, 2017, sem paginação).

Uma vez planejado o processo de Segurança da Informação, sua implantação, execução e controle vão exigir a necessidade de uma mudança na cultura organizacional que, segundo Manini e Greenhalgh (2016) diz respeito “ao modo de se fazer as coisas nas organizações, baseado no aprendizado partilhado para superação dos problemas e na relação entre crenças e costumes de cada pessoa [...]”. Entende-se que é primordial o engajamento de toda a equipe no processo de proteção dos bens existentes na biblioteca, seja de que natureza for, de maneira que possam estar habilitados a detectar os riscos e ameaças à segurança, e tomar decisões acertadas para a salvaguarda do patrimônio informacional, cultural e científico.

4.3.1 Construção de Política de Segurança da Informação para biblioteca

No ambiente organizacional de uma biblioteca universitaria, é necessário um entendimento dos riscos e dos ativos informacionais, bem como do processo de gerenciamento dos mesmos, uma vez que esta se diferencia de outras organizações por ter como atividades fins o acesso e disseminação da informação.

Neste sentido, tem-se que, no processo de desenvolvimento da PSI, é pertinente considerar que, de acordo com Höne e Eloff (2002, p. 405, tradução nossa): “O estilo de escrita da política deve refletir a cultura organizacional para assegurar a aceitação do documento pelos usuários da organização”. Para Hare (2001), na linha do que propõem Höne e Eloff (2002), faz-se necessário considerar a cultura da organização para o desenvolvimento de Política de Segurança da Informação. Compreende-se que isto converge para o processo de identicação das ameaças, riscos e vulnerabilidades a que a organização está exposta, quanto à SI, conforme a utilização de métodos destinados a identificação destes elementos.

Hare (2001) assevera que o ambiente organizacional é um espaço em que as pessoas, não só se reunem para cumrprirem suas atribuições de trabalho, mas um espaço de socialização e interação de ideias sobre sua vida profissional e pessoal. Nesta perspectiva, a política de segurança da informação torna-se um instrumento essencial de qualquer organização, pois identifica a maneira como os seus membros deverão se comportar. Desse modo, a política estabelecerá o que é relevante para a organização e as definições da forma de trabalho proposta pela PSI, estabelecendo as responsabilidades que poderão ser específicas aplicadas a toda a organização ou setores.

De acordo com Hare (2001), para a política são usados: padrões para o estabelecimento de medida comum, e que sejam aceitas pelas pessoas que seguirão esses

padrões na implementação da política; procedimentos que fornecem os detalhes, o passo a passo, o modo como será implementada e seguida; e as diretrizes que identificarão o que a gestão gostaria que fosse realizado.

Entende-se que, como afirma Flowerday e Tuyikeze (2016 p. 170, tradução nossa): “O processo de desenvolvimento e implementação de uma política eficaz de segurança da informação não é direto, mas é impulsionado por várias questões, como exigências regulatórias, complexidade das novas tecnologias e ameaças externas e internas”. Nota-se, para tanto, que a PSI precisa estar adequada ao contexto, missão, objetivos, metas da organização, portanto, deve ser clara, compreensível (roteiro inteligível), concisa, exequível, implementável, explícita quanto aos seus objetivos, necessidades. E deve submeter-se a avaliações e revisões periódicas, para garantia de sua atualização.

A literatura da área de PSI apresenta considerações sobre boas práticas que viabilizam a proteção dos ativos de informação e trazem, também, diversos modelos que norteiam a elaboração de Política de Segurança da Informação.

A partir dessas considerações, foi possível identificar princípios essenciais que devem compor uma Política de Segurança da Informação que, conforme Höne e Eloff (2002), são princípios que seguem padrões internacionais e trazem a descrição das regras gerais relacionadas à segurança da informação no âmbito organizacional. Tais princípios explicam o comportamento adequado ou inadequado dos usuários na organização, relativamente aos vários tópicos e conceitos. Esses princípios poderão estar ligados estritamente à cultura da organização ou às regulamentações que regem suas atividades, enquanto outros poderão se aplicar a todas as organizações, em suas políticas de segurança da informação. Como são princípios passíveis de mudanças, à medida que a tecnologia avança, importa uma revisão periódica. A seguir, o Quadro 18 apresenta sugestão de elementos essenciais em uma PSI:

Quadro 18 - Elementos a serem considerados em uma PSI

Elementos	Características
Necessidade e abrangência da segurança da informação	Breve declaração introdutória enfatizando a dependência da organização da Segurança da informação. Esta declaração introdutória também fornece informações sobre a razão pela qual a política é necessária na organização.
Objetivos da Segurança da Informação	Os objetivos da segurança da informação em uma organização devem ser descritos brevemente para informar o leitor sobre o objetivo específico da gestão da segurança da informação na organização. Estes objectivos devem estar claramente ligados à estratégia geral da empresa, às suas metas e objectivos e à natureza da sua actividade .
Definição de Segurança da	Uma política de segurança da informação é geralmente

Informação	direcionada a uma audiência diversa para quem a segurança da informação pode ser um conceito estranho e novo. Portanto, é crucial que a política contenha uma definição breve e compreensível de segurança da informação para garantir uma compreensão uniforme do conceito em toda a organização.
Compromisso da Gestão com a Segurança da informação	Declaração de compromisso é a declaração singularmente mais importante em uma política de segurança da informação. Sem esta afirmação, qualquer atividade tentada pelo pessoal de segurança da informação não será eficaz e não será levada a sério em toda a organização. A declaração de compromisso de gestão pode forçar os funcionários a prestar atenção à segurança da informação e demonstra a intenção da administração de fazer um sucesso dela na organização.
Aprovação da Política de Segurança da Informação (Assinatura)	A assinatura de aprovação também pode ser vista como a assinatura de endosso e deve normalmente ser a do mais alto signatário possível na organização. Esta assinatura deve ser exibida em uma posição proeminente como mais um sinal do compromisso da alta gerência com a segurança da informação.
Objetivo da Política de Segurança da Informação	O objetivo ou objectivo da política de segurança da informação não deve ser confundido com as declarações introdutórias sobre a necessidade de segurança da informação numa organização. Essas declarações descrevem as razões para o desenvolvimento de uma política de segurança da informação e, possivelmente, estarão ligadas a questões de conformidade legal. Os principais objetivos da política em si são assim descritos nesta seção.
Princípios de Segurança da Informação	Os princípios de segurança da informação descrevem as regras gerais relacionadas à segurança da informação dentro de uma organização.
Papéis e responsabilidades	Este é um dos componentes mais importantes da política de segurança da informação, uma vez que esta parte diz ao leitor exatamente o que é esperado dele / ela em termos de segurança da informação na organização. As funções e responsabilidades devem abranger todos os aspectos da segurança da informação, bem como as responsabilidades individuais de todas as partes que utilizam os recursos de informação da organização.
Violação da Política de Segurança da Informação e Ação Disciplinar	A declaração sobre violações da política de segurança da informação é uma declaração muito poderosa, pois garante que ações disciplinares podem ser tomadas contra um usuário se a política não for adotada. É muito importante que esta declaração esteja diretamente relacionada à política disciplinar geral da organização.
Monitoramento e Revisão	Esta declaração trata da necessidade de monitorizar e rever frequentemente a aplicabilidade e eficácia dos controlos de segurança da informação implementados dentro da organização. Sem essa afirmação, não há continuidade forçada para a melhoria da implementação da segurança da informação na organização.
Declaração e reconhecimento do Usuário	Este não é um elemento comum encontrado em uma política de segurança apresentado como um apêndice ou um documento separado. No entanto, é um elemento muito útil, pois é tipicamente redigido como uma versão abreviada da política de segurança da informação e direcionado completamente para os usuários da organização. Os usuários são, então, mais propensos a ler toda a seção e ter uma melhor compreensão do que é esperado deles. Ao assinar uma declaração de usuário sobre o trabalho antes

	do acesso à informação eletrônica ser concedida, o usuário reconhece sua responsabilidade em relação à segurança da informação. A declaração do usuário e o reconhecimento também devem ser lidos e assinados novamente todos os anos, de forma anual, para lembrá-los de suas responsabilidades individuais na proteção dos ativos de informação dentro da organização.
Referências cruzadas	A política de segurança da informação nunca deve ser escrita isoladamente e terá de ser Apoiado por outras políticas, padrões, procedimentos e processos relevantes. Esses documentos aplicáveis devem ser referenciados na política para garantir que o leitor obtenha uma visão completa de todos os controles e medidas de segurança da informação utilizados na organização. Muitas vezes, as organizações também são obrigadas a implementar certos controles e medidas, conforme determinado pela legislação e regulamentos do país. Estes Então também precisam ser referenciados na política.

Fonte: Adaptado para quadro de Höne e Eloff (2002, tradução nossa).

Destaca-se, também, como exemplo de modelo, a Política de Segurança da Informação do Estado de Oklahoma (OMES IS, 2015, tradução nossa), cuja intenção é proteger os ativos de informação do Estado, por meio do Gabinete de Serviços de Informação de Gestão e Serviços Empresariais (OMES IS), que tem a responsabilidade de dar a conhecer as diretrizes, procedimentos, normas e boas práticas aplicadas a todas as agências estatais. E estas têm, por sua vez, a obrigatoriedade de tornar cientes todos os funcionários do Estado, bem como contratados, e todas as organizações que lidam com a informação, da importância da proteção dos ativos de informação do Estado. Essa política foi criada para reger todos os aspectos relacionados a *hardware*, *software*, comunicações e formação. Traz as definições de informação, ativos de informação, o proprietário da informação, bem como a responsabilidade da informação quanto à confidencialidade, às implicações relacionadas ao mau uso dos recursos informacionais, entre outros aspectos pertinentes à proteção da informação.

Para tanto, nota-se que esta PSI traz, em seu conjunto, elementos específicos e, de acordo com a área de responsabilidade das entidades que a utilizam, com abrangência a todas as agências estatais. Estes elementos em destaque, bem como o referencial teórico e os dados da aplicação da metodologia, servirão de orientação para a elaboração da PSI que esta pesquisa propõe. O Quadro 18 apresenta os elementos da PSI do Estado de Oklahoma (OMES IS, 2015, tradução nossa), com base na qual foram escolhidos alguns elementos que nortearão a construção da minuta da PSI/BC, com adaptações. O Quadro 19 apresenta um resumo destes elementos:

Quadro 19 – Elementos norteadores que subsidiam a composição de uma PSI

Introdução	Explicita o que o documento estabelece, a descrição dos procedimentos, diretrizes e boas práticas para a criação e manutenção de um ambiente seguro para o armazenamento e disseminação da informação. Ressalta a importância de que todos os envolvidos na organização devem estar cientes da política, dos procedimentos, orientações e boas práticas em segurança da informação, bem como, o comprometimento na proteção da informação. Destaca que os requisitos de segurança representam os níveis mínimos de segurança exigidos, um guia para o desenvolvimento de plano de segurança e políticas adicionais, caso seja necessário.
Informação	A gestão da informação requer um conjunto de procedimentos, orientações e boas práticas que forneçam orientação e direção no que tange à segurança da confidencialidade, integridade e disponibilidade das informações. Todo o conteúdo informacional armazenado é propriedade da organização e a mesma é a principal responsável pela garantia da autenticidade, integridade e precisão das informações. O objetivo da organização é proteger a informação de danos inadvertidos ou intencionais, bem como a divulgação ou utilização não autorizada de acordo com as normas de classificação e diretrizes processuais.
Gestão de incidentes	Responsabilidades e procedimentos de gestão de incidentes devem ser estabelecidos para garantir uma resposta rápida, eficaz e ordenada para a segurança incidentes. Os procedimentos devem ser estabelecidos para cobrir todos os tipos possíveis de incidentes de segurança.
Questões de Pessoa/Problema de utilizadores	A conscientização do pessoal da política de segurança da informação, dos procedimentos, das diretrizes, boas práticas, bem como a adesão à política é da responsabilidade da organização. Utilização de computador pessoal: os computadores da organização são de uso para atividades relacionadas com o trabalho. Todos os utilizadores têm acesso a computadores para tarefas relacionadas com o trabalho e esse uso e deve permanecer em conformidade com as políticas estabelecidas. Uso de Email: Usado de forma adequada, o e-mail é um canal de comunicação às pessoas, assim, facilitando o contato de negócios. No entanto, esta conveniência também leva os usuários a experimentarem ou aproveitarem essa mídia, de forma inadequada, resulta em e-mails de indesejáveis. Seu uso indevido pode comprometer a integridade de sistemas, segurança da informação e outros serviços.

Segurança física e do ambiente	A organização é responsável pela documentação, execução, monitoramento e teste de um plano de segurança física para ativos de informação e de telecomunicações. Este plano de segurança física avaliaria os riscos de potenciais perdas.
Continuidade dos negócios	Um plano de contingência fornece o plano organizacional documentado para mitigar os riscos de interrupção de negócios e minimizar o impacto de qualquer interrupção do serviço. Seu objetivo é manter-se em alerta, pronto para sustentar os processos de uma organização durante e após uma importante interrupção imprevista nos serviços causada por desastres e falhas de segurança.
Gerenciamento de mídias removíveis	Estabelecimento de procedimentos operacionais apropriados para proteção de documentos, mídia de computador (fitas, discos, cassetes, etc.), dados de entrada / saída e documentação do sistema contra danos, roubo e acesso não autorizado.
Controle de *software* malicioso	Implementação de controles de detecção e prevenção para proteção contra softwares maliciosos e procedimentos adequados de conscientização dos usuários, atentando para conformidade com os seguintes procedimentos: licenças de software; proteção na obtenção de arquivos e software; atualização regular de software; revisões periódicas de software e e conteúdo de informações de sistemas; verificação de arquivos em mídias eletrônicas de origem duvidosa ou sem autorização; verificação de anexos de correio eletrônico e downloads; atribuição de responsabilidades com a proteção contra vírus em sistemas; treinamento em usos e outros
Cumprimento de segurança	A organização deve assegurar que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam documentados e executados corretamente. Todas as áreas dentro da organização podem estar sujeitas a uma revisão periódica para garantir o cumprimento dos procedimentos e padrões de segurança. Estes devem incluir o seguinte: (A) sistemas de informação; (B) fornecedores de sistemas; (C) proprietários de ativos de informações e informações; (D) agências de hospedagem de recursos de informações e informações, e (E) usuários.
Gestão de risco	O gerenciamento de risco engloba avaliações de risco, mitigação de riscos, avaliação e avaliação. O processo de avaliação de risco inclui identificação e avaliação de riscos e impactos de risco e recomendação de medidas de redução de risco. A mitigação do risco refere-se a priorizar, implementar e manter as medidas adequadas de redução de risco recomendadas pelo processo de avaliação de risco. Através de um processo de avaliação contínua, organização é responsável por determinar se o risco se encontra em um nível aceitável ou se os controles de segurança adicionais devem ser implementados para reduzir ainda mais ou eliminar o risco residual.
Controle de acesso	Controles de acesso físico e lógico são necessários para garantir a integridade das informações e dos ativos físicos.

***Back Up* de Informação**	As cópias de backup de informações e software essenciais de negócios devem ser realizadas regularmente. Devem ser fornecidas facilidades de backup adequadas para garantir que todas as informações e software essenciais do negócio possam ser recuperados após um desastre ou falha na mídia. Os arranjos de backup para sistemas individuais devem ser testados regularmente para garantir que eles atendam aos requisitos dos planos de continuidade de negócios.
Proteção da informação	Os registros importantes de uma organização devem ser protegidos contra perda, destruição e falsificação. Alguns registros podem precisar ser mantidos de forma segura para atender aos requisitos legais ou regulamentares, bem como para apoiar atividades comerciais essenciais. O período de tempo e o conteúdo da informação para retenção podem ser estabelecidos por leis ou regulamentos federais e estaduais.

Fonte: Adaptado para quadro da Política de Segurança da Informação do Estado de Oklahoma (2015).

Broderick (2006), numa abordagem sobre desenvolvimento de sistema de gerenciamento de segurança da informação (ISMS), em que trata de normas de segurança e regulamentos de Segurança, expõe um mapeamento de requisitos de segurança que inclui os padrões da norma ISO 27001 e COBIT. Entende-se que, a partir deste mapeamento, pode-se extrair elementos básicos, alinhados aos padrões internacionais de segurança da informação, conforme mostra Quadro 20, que apresenta os elementos de segurança da informação relacionados ao desenvolvimento de PSI:

Quadro 20 – Elementos de Segurança da Informação relacionados ao desenvolvimento de PSI

Elementos de Segurança da Informação	
Política de segurança	• Definir o plano estratégico de TI Determinar a direção tecnológica • Comunicar os objetivos e a direção da gerência • Monitorar o processo
Organização da Segurança da Informação	• Definir a arquitetura de informações • Definir a organização e os relacionamentos de TI • Monitorar do processo
Gestão de ativos	• Avaliar os riscos • Determinar a direção tecnológica • Gerir a qualidade • Monitorar o processo

Segurança de recursos Humanos	• Gerir recursos humanos • Educar e treinar usuários • Monitorar o processo
Segurança Física e Ambiental	• Gerenciamento de instalações • Avaliar os riscos • Desenvolver e manter processos • Gerenciar alterações • Monitorar o processo
Gestão de comunicações e operações	• Adquirir e manter infra-estrutura tecnológica • Desenvolver e manter procedimentos • Determinar a direção tecnológica • Monitorar o processo
Controle de acesso	• Comunicar os objetivos e a direção da gerência • Definir e gerenciar níveis de serviço • Gerenciar serviços de terceiros • Gerenciar o desempenho ea capacidade • Garantir a segurança dos sistemas • Educar e treinar usuários • Ajudar e aconselhar os clientes • Gerenciar a configuração • Gerenciar problemas e incidentes • Monitorar o processo
Aquisição, desenvolvimento e manutenção de sistemas de informação	• Identificar soluções automatizadas • Adquirir e manter software aplicativo • Adquirir e manter infra-estrutura tecnológica • Desenvolver e manter procedimentos • Instalar e credenciar sistemas • Gerenciar alterações • Monitorar o processo
Gerenciamento de incidentes de segurança da informação	• Educar e treinar usuários • Ajudar e aconselhar os clientes • Gerenciar a configuração • Gerenciar problemas e incidentes • Monitorar o processo

Continuidade dos negócios	• Determinar a direção tecnológica • Definir e gerenciar níveis de serviço • Gerenciar serviços de terceiros • Gerenciar o desempenho ea capacidade • Garantir a segurança dos sistemas • Gerir operações • Monitorar o processo
Conformiade	• Garantir a conformidade com os requisitos externos • Monitorar o processo • Avaliar a adequação do controle interno • Obter garantias independentes • Fornecer auditoria independente

Fonte: Adaptado para quadro de Broderick (2006).

Ferreira e Araújo (2008, p. 44) destacam, ainda, alguns itens que podem ser relevantes para o sucesso da PSI. Nota-se que esses itens são comuns aos autores já referenciados, no entanto sua aplicação é única, adequando-se à realidade de cada organização, a saber:

- Formalização dos processos e instruções de trabalho;
- Utilização de tecnologias capazes de prover segurança;
- Atribuição formal de responsabilidades e das respectivas penalidades;
- Classificação das informações;
- Treinamento e conscientização constantes.

Os autores ressaltam, a propósito, a possibilidade de se desmembrar a segurança da informação em 4 grandes aspectos:

- **Segurança computacional:** conceitos e técnicas utilizados para proteger o ambiente informatizado contra eventos inesperados que possam causar qualquer prejuízo;
- **Segurança lógica:** prevenção contra acesso não autorizado;
- **Segurança física:** procedimentos e recursos para prevenir acesso não autorizado, dano e interferência nas informações e instalações físicas da organização;
- **Continuidade de negócios:** estrutura de procedimentos para reduzir, a um nível aceitável, o risco de interrupção ocasionada por desastres ou falhas por meio da combinação de ações de prevenção e recuperação. (FERREIRA; ARAÚJO, 2008, p. 45)

Entende-se que todos estes elementos se revestem de um direcionamento a uma adequada proteção da informação, tanto no meio convencional, quanto no meio tecnológico, e requerem, dos participantes da organização um esforço conjunto na aderência aos regulamentos de segurança, de maneira que os impulsionem a uma cultura de boas práticas em SI, que abranja as dimensões pessoa, processos e tecnologia.

5 DESENVOLVIMENT O E ANÁLISE DOS DADOS

Discorre como ocorreram os procedimentos de coleta e análise dos dados. O resultado destes é substancial para o processo de construção da PSI, que envolve diversas atividades, sendo a Análise e Avaliação de Riscos, uma delas, instrumento relevante, para a identificação das ameaças, vulnerabilidades e riscos, e que contribui na identificação dos seus controles.

5.1 APLICAÇÃO E ANÁLISE DO FRAAP

Para assegurar a clareza e entendimento das questões, realizou-se primeiramente um pré-teste, no dia 07/04/2017, na sala LTI (ambiente do Prof. Wagner), às 14:30, com alunos da Disciplina Gestão da Segurança da Informação do Mestrado Profissional em Gestão nas Organizações Aprendentes da UFPB. Por se tratar de alunos que já estão inteirados com as questões que envolvem a Segurança da Informação (SI), pode-se perceber uma tendência a percepção da importância da SI em uma biblioteca universitária, conhecimento da PSI da UFPB, percepção dos problemas que envolvem a SI. Na identificação e classificação das ameaças, percebeu-se uma semelhança, no que se refere a preocupações que convergem mais para as ameaças físicas do que as ameaças relacionadas a SI nas práticas gerenciais, expressa pelos participantes da pesquisa. Com o resultado satisfatório do pré-teste, aplicou-se os instrumentos de coleta: FRAAP e o questionário.

5.1.1 Pré-FRAAP

Para a realização do Pré-FRAAP, foi criado um grupo no *WhatsApp* como canal de comunicação junto aos participantes da pesquisa. Anteriormente, houve uma conversa informal com cada participante, explicando o objetivo da pesquisa, os instrumentos de coleta de dados, definição de conceitos que orientariam a Análise e Avaliação de Riscos para a construção de uma Política de Segurança da Informação. Os participantes foram informados acerca do que se trata a pesquisa, os objetivos e a finalidade da Análise e Avaliação de Riscos. Esta etapa foi determinante na elaboração dos requisitos para a realização das atividades de Análise e Avaliação de Riscos que serão descritas em seguida.

5.1.2 Sessão FRAAP

A Sessão FRAAP ocorreu na sala da Direção da Biblioteca Central da UFPB, no dia 11/04/2017, com início às 13:40 horas e término às 16:40 horas (três horas de duração), tendo como participantes oito bibliotecários gestores.

Na ocasião da reunião dirigida, foi apresentada a pesquisa, conceitos sobre Segurança da Informação, ativo, vulnerabilidades, ameaças, riscos, probabilidade, impacto, de maneira que os participantes pudessem se inteirar dos elementos relacionados à SI. Após essa explanação, seguiu-se para a aplicação do método.

Os participantes receberam uma folha de papel A4 e caneta, foram orientados a escreverem as ameaças à Segurança da Informação no ambiente da BC. Após a identificação das ameaças, foi feita a classificação considerando o nível de probabilidade e nível de impacto. Foi solicitado que cada participante expusesse uma única ameaça por vez, num processo cíclico de identificação das ameaças, até que não restasse mais nenhuma ameaça a ser elencada.

Cada participante listou em média cinco ameaças. Foi realizado um breve debate sobre estas ameaças, em seguida, foi solicitado o preenchimento de um *check-list* contendo uma lista de possíveis ameaças, sugeridas por Peltier (2005) e os participantes classificaram-nas atribuindo um valor (1 = Baixo, 2 = Médio, 3 = Alto), quanto ao nível de probabilidade e nível de impacto. Na ocasião, aplicou-se também o questionário de 23 questões que contemplam as categorias: pessoa, processos e tecnologias. Vale ressaltar que este *check-list* foi usado como elemento complementar na intenção de obtenção de mais informações que pudessem ser úteis na análise dos resultados.

5.1.3 Resultados FRAAP

Foi identificado um conjunto de 15 ameaças, dentre as quais 9 Ameaças Físicas, 2 Ameaças Lógicas, e 4 Ameaças Processos, sugerindo revisão dos princípios: Integridade, Confidencialidade e Disponibilidade. Importante considerar que, durante o processo de classificação, ocorreram ameaças semelhantes que, em comum acordo com os participantes, foram aglutinadas ao grupo das ameaças correspondentes (Quadro 21).

Quadro 21 – Identificação das ameaças e princípios a serem observados

Ameaça Nº	Ameaças	Princípios
Ameaças Físicas		
1	**Cabeamento de rede exposto** (Estrutura lógica**)**	Disponibilidade
2	**Vazamento de água / falha de encanamento/goteira** **(**Instalações hidráulicas necessitando reparos, goteiras, chuva)	Disponibilidade
3	**Falha de rede elétrica** **(**Problemas parte elétrica - instalações elétricas precárias)	Disponibilidade
4	**Ausência de manutenção predial** (Estrutura física precária; ausência de controle de pragas (cupins e morcegos).	Disponibilidade
5	**Falta de câmeras de segurança** (Inexistência de segurança física e predial)	Integridade/confidencialidade
6	**Ameaças ambientais** (Fungos, incêndio, falta de climatização, animais peçonhentos (entrada); umidade elevada, falha de ar-condicionado).	Disponibilidade
7	**Falta de Higienização do acervo**	Disponibilidade
8	**Controle de acesso físico** (Ausência de controle de acesso físico aos setores; falta de controle na identificação dos usuários; falta de segurança em todos os andares do prédio)	Integridade/confidencialidade
9	**Sinalização precária na Biblioteca**	Disponibilidade
Ameaças Lógicas		
10	**Invasão de hacker** (Ataques a bases de dados)	Integridade
11	**Falta de backup** (Cópias de segurança)	Integridade
	Ameaças – Processos	
12	**Falta de capacitação no uso das TICs** (treinamento)	Disponibilidade/integridade/confidencialidade
13	**Obsolescência tecnológica (**falta de troca de equipamentos nas datas corretas; falta equipamentos de qualidade).	Disponibilidade
14	**Ruídos na comunicação** (Conversas paralelas - problemas de comunicação)	Confidencialidade
15	**Falta de pessoal - chave** (Escassez de recursos humanos capacitado/qualificado para exercer as funções/atividades)	Integridade

Fonte: Dados da pesquisa (2017).

O processo de classificação das ameaças (Quadro 22) para a identificação dos riscos se deu a partir de uma abordagem qualitativa, considerando-se as características e análise da pesquisa em pauta. Para tanto, o nível de exposição ao risco foi identificado mediante a probabilidade de ocorrência da ameaça e o consequente impacto à organização, considerando-se as definições para Nível de Probabilidade e Nível de Impacto (Quadro 2 e 3).

Quadro 22 – Classificação das Ameaças quanto ao Nível de Probabilidade e Impacto

Ameaças	Probabilidade	Impacto
Falta de pessoal - Chave (Escassez de recursos humanos capacitados/qualificado para exercer as funções/atividades	Alta	Alto
Falta de capacitação no uso das TICs	Alta	Alto
Vazamento de água / falha de encanamento/goteira (instalações hidráulicas necessitando reparos, goteiras, chuva)	Alta	Alto
Falha de rede elétrica (Instalações elétricas precárias)	Alta	Alto
Ausência de manutenção predial (Estrutura física precária; ausência de controle de pragas -cupins e morcegos).	Alta	Alto
Ausência de câmeras de segurança (Inexistência de segurança física e predial)	Alta	Alto
Ameaças ambientais (fungos, incêndio, falta de climatização, animais peçonhentos (entrada); umidade elevada, falha de ar-condicionado).	Alta	Alto
Falta de Higienização do acervo	Média	Médio
Controle de acesso físico (Ausência de controle de acesso físico aos setores; falta de controle na identificação dos usuários; falta de segurança em todos os andares do prédio;	Alta	Alto
Ruídos na comunicação (Conversas paralelas – Problemas de comunicação)	Alta	Médio
Sinalização precária na Biblioteca	Média	Alto
Invasão de hacker (Ataques a bases de dados)	Média	Alto
Falta de backup (Cópias de segurança)	Média	Médio
Cabeamento de rede exposto (Estrutura lógica**)**.	Alta	Alto
Obsolescência tecnológica (Falta equipamentos de qualidade).	Média	Médio

Fonte: Dados da pesquisa (2017).

Ocorreu um breve debate, gravado com permissão dos participantes, no momento da classificação das ameaças quanto ao nível de probabilidade de sua ocorrência e seu impacto. Observou-se em suas falas que, alguns participantes, deram maior ênfase a problemas de infraestrutura física, bem como segurança física, do ambiente e ameaças ambientais. Quanto às ameaças relacionadas a processos e lógicas, mesmo não tendo sido enfatizadas, foram citadas, como significativas, mas não com tanta ênfase com relação as citadas acima.

Segundo informações do participante 1, há algum tempo atrás, foi detectado a instalação de um robô em uma determinada Base de Dados de Periódicos Científicos. O participante 1 informou que, durante um final de semana, foi baixado um volume exponencial de artigos de uma das revistas mais caras da área de química. Segundo ele, isto ocorreu já

duas vezes. Informou que na época do ocorrido, a Capes entrou em contato com a UFPB, informando que poderia perder o acesso ao Portal de Periódicos, se não identificassem.

Esse fato chama à atenção para a questão da importância que a Biblioteca precisa dar em sua gestão de suas bases digitais, no sentido de assegurar, junto aos seus fornecedores, sistemas anti-robôs, para aprimorar a segurança da informação.

O participante 2, expunha que as ameaças relacionadas à Falta de pessoal - chave (pessoal capacitado, treinamento, falta de capacitação no uso das TICs, etc.), expressa bem a realidade da Biblioteca (durante o período de realização da pesquisa), não só no que diz respeito a escassez de pessoal, mas a necessidade de pessoal capacitado para exercer as atividades.

Com relação a problemática do uso das TICs, foi tema recorrente nas falas. O participante 2 afirmou que "o dano pode ser seríssimo", pois "o trabalho não anda, a informação é processada de forma errada, enviada de forma errada...".

No que se refere à obsolescência tecnológica, um dos participantes relatou que há recursos tecnológicos, mas é insuficiente, poderia ter mais, pois, em alguns casos, estes já sofrem de obsolescência.

Ao abordar o tema da segurança física e controle de acesso, o participante 4 relatou sobre a entrada de dois indivíduos suspeitos. Posteriormente, descobriu-se que se tratava de dois assaltantes. Este fato evidência o nível de risco à que a Biblioteca está exposta, quando não são estabelecidas medidas de prevenção da segurança, e isto vale, não só para a segurança física, mas a segurança lógica também.

A ABNT NBR ISO/IEC 27002 (2013, p. 46), recomenda o estabelecimento de perímetros de segurança, que "sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis". Estes perímetros referem-se a barreiras de segurança, conforme apresentado por Sêmola (2014) em que, segundo o autor, cada barreira expressa-se de maneira relevante, objetivando a redução dos riscos. Para tanto, é necessário um redimensionamento adequado que seja direcionado a uma correta interação e integração desse processo.

Nesse sentido, Beal (2008, p. 81) afirma que: "Uma barreira corresponde a qualquer obstáculo colocado para prevenir um ataque, podendo ser física (cerca elétrica, parede), lógica (processo de *logon* para acesso a uma rede) ou uma combinação de ambas (autenticação de indivíduos por dispositivo biométrico)".

Os participantes ressaltaram também a ausência de câmeras de segurança no acervo, e a sinalização precária da biblioteca, sobretudo para o acesso a pessoas com necessidades

especiais. Um dos participantes incluiu a falta de higienização, como uma ameaça, tanto a falta de higienização predial, além do acervo como um todo. Os demais participantes ratificaram esse problema, embora não considerassem de alto impacto, mas de médio impacto nas atividades da BC.

O Participante 1, ao abordar a questão da obsolescência tecnológica, comentou sobre a necessidade de equipamentos atualizados. Uma vez que se trabalha com bases de dados que oferecem imagens em alta definição, em 3D, isso implica na boa qualidade dos equipamentos e programas, que possam atender de maneira satisfatória as demandas da Biblioteca Central. O participante 4 afirmou que "no contexto do participante 1, seria mais impactante a obsolescência tecnológica", mas para o seu contexto de trabalho, o impacto da obsolescência seria médio, no entanto, considera que em se tratando do contexto da biblioteca como um todo, torna-se alto. Este debate entre os participantes demostra o entendimento que os pontos tratados devem ser vistos como um todo, de forma que cada gestor participante estava ciente e atento as necessidades dos demais colegas.

Sobre a questão da cópia de segurança, o participante 1 relatou fato recorrente, de equipamentos levados para manutenção e não se fazia *backup* das informações contidas no mesmo. Comentou que é evidente a durabilidade dos equipamentos ser mínima, mas ressaltou a importância de um entendimento de que se está lidando com informação, com armazenamento de informação, acesso à informação, o que implica a necessidade de se trabalhar com bons equipamentos.

Beal (2008, p. 81) assevera que: "A proteção do ambiente e dos ativos físicos de informação, tanto como no [...] ambiente lógico, [...] exige a combinação de medidas preventivas, detectivas e reativas." Isto vai se aplicar à elaboração de PSI adaptada às necessidades da organização, como instrumento de mitigação dos riscos, conforme já abordado nesta pesquisa.

A partir de fevereiro de 2017, durante o desenvolvimento desta pesquisa, a Biblioteca Central passou para uma nova gestão. Na perspectiva de empreender esforços para implementar restruturações, estratégias operacionais, foram formadas comissões para atender as demandas das atividades. O participante 3, ressaltou a relevância da pesquisa em pauta, como um instrumento gerador de melhorias para a Biblioteca, o que foi referendado por todos os envolvidos.

De posse das informações acerca da probabilidade e impacto das ameaças aos ativos de informação da BC, efetuou-se a soma dos valores dos níveis Alto (3), Médio (2) e Baixo (1), para identificação do nível de risco.

Foi necessário definir uma escala em que se atribuiu de 2-3 (Baixo), 4 (Médio) e 5-6 (Alto). Segue o Quadro 23:

Quadro 23 – Análise de risco

Ameaça	Aplicação Sim/Não	Probabilidade 1= Baixa 2= Média 3 = Alta	Impacto 1= Baixo 2 = Médio 3 = Alto	Nível de Risco 5-6(Alto) 4(Médio) 2-3(Baixo)
Falta de pessoal - Chave (Escassez de recursos humanos capacitados/qualificado para exercer as funções/atividades	Sim	3	3	6(Alto)
Falta de capacitação no uso das TICs	Sim	3	3	6(Alto)
Vazamento de água / falha de encanamento/goteira **(**Instalações hidráulicas necessitando reparos, goteiras, chuva)	Sim	3	3	6(Alto)
Falha de rede elétrica **(**Problemas parte elétrica - instalações elétricas precárias)	Sim	3	3	6(Alto)
Ausência de manutenção predial (Estrutura física precária; ausência de controle de pragas (cupins e morcegos).	Sim	3	3	6(Alto)
Ausência de câmeras de segurança (Inexistência de segurança física e predial)	Sim	3	3	6(Alto)
Ameaças ambientais (Fungos, incêndio, falta de climatização, animais peçonhentos (entrada); umidade elevada, falha de ar-condicionado).	Sim	3	3	6(Alto)
Falta de Higienização do acervo	Sim	2	2	4(Médio)
Controle de acesso físico (Ausência de controle de acesso físico aos setores; falta de controle na identificação dos usuários; falta de segurança em todos os andares do prédio	Sim	3	3	6(Alto)
Ruídos na comunicação (Conversas paralelas – Fofocas no ambiente de trabalho (problemas de comunicação)	Sim	3	2	5(Alto)
Sinalização precária na Biblioteca	Sim	2	3	5(Alto)
Invasão de *hacker* (Ataques a sistemas)	Sim	2	3	5(Alto)
Cópias de segurança (Falta de *backup*)	Sim	2	2	4(Médio)

Cabeamento de rede exposto (Estrutura lógica)	Sim	3	3	6(Alto)
Obsolescência tecnológica (Falta equipamentos de qualidade).	Sim	2	2	4(Médio)

Fonte: Dados da pesquisa (2017).

O processo de análise dos níveis de riscos apresentou uma estimativa de 15 riscos considerados 12 Altos e 3 Médios. Com base na Matriz de risco, pode-se identificar as ações necessárias para a identificação dos controles, indicando a letra: A – Ação corretiva precisa ser implementada, conforme Quadro 5 (Matriz de Risco). A seguir, o Quadro 24, apresenta as sugestões de controles para diminuição dos riscos.

Quadro 24 – Sugestão de controles para os riscos

Grupo de Ameaça	Ações
Falta de pessoal – Chave (Escassez de recursos humanos qualificado/capacitado para exercer as funções/atividades).	- Implementar programas de treinamento para usuários (avaliações de desempenho dos utilizadores) concebidos em conformidade com as políticas e procedimentos em vigor para assegurar a utilização adequada da aplicação (PELTIER, 2005); - Na UFPB, há o processo de ingresso por concurso público, para atendimento de escassez de pessoal; - Cursos; - Educação continuada.
Falta de capacitação no uso das TICs	- Implementar programas de usuários (avaliações de desempenho dos usuários) concebidos em conformidade com as políticas e procedimentos em vigor para assegurar a utilização adequada de aplicações(PELTIER, 2005); - A Pró-Reitoria de Gestão de Pessoas (PROGEPE) da UFPB oferece aos seus servidores cursos de capacitação de acordo com as necessidades e demandas. Também são oferecidos cursos em nível *stricto sensu e lato sensu* aos servidores que desejem se qualificar; - Parceria com o Departamento de Computação Científica (DCC) e outros Departamentos.
Vazamento de água / falha de encanamento/goteira (Instalações hidráulicas necessitando de reparos, goteiras, chuva)	- Requisitos de tempo para manutenção serão monitorados e um pedido de ajustamento será comunicado à gerência se a experiência garantir (PELTIER, 2005); - Sistema de chamado para requisição de serviços (Prefeitura Univseritária da UFPB); - Projetos de extensão; - Arquitetura; - Engenharia Elétrica, etc.
Falha de rede elétrica (Problemas parte elétrica - instalações elétricas precárias)	- Requisitos de tempo para manutenção serão monitorados e um pedido de ajustamento será comunicado à gerência se a experiência garantir (PELTIER, 2005); - Sistema de chamado para requisição de serviços (Prefeitura Univseritária da UFPB).
Ausência de manutenção predial (Estrutura física precária;	- Requisitos de tempo para manutenção serão monitorados e um pedido de ajustamento será comunicado à gerência se a experiência garantir (PELTIER, 2005);

ausência de controle de pragas - cupins e morcegos).	- Sistema de chamado para requisição de serviços (Prefeitura Univseritária da UFPB).
Ausência de câmeras de segurança (Inexistência de segurança física e predial)	- Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações (ABNT NBR ISO/IEC 27002, 2013); - Sistema de chamado para requisição de serviços (Prefeitura Univseritária da UFPB).
Ameaças ambientais (fungos, incêndio, falta de climatização, animais peçonhentos (entrada); umidade elevada, falha de ar-condicionado).	- Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentais. (ABNT NBR ISO/IEC 27002, 2013). - Sistema de chamado para requisição de serviços (Prefeitura Univseritária da UFPB).
Falta de Higienização do acervo	- Requisitos de tempo para manutenção serão monitorados e um pedido de ajustamento será comunicado à gerência se a experiência garantir (PELTIER, 2005); - Seção de compras e licitações da Biblioteca Central da UFPB (baseado nos processos e editais de compras anuais da BC) - contratação de serviço de conservação de acervos (Política de Conservação de Acervos).
Controle de acesso físico (Ausência de controle de acesso físico aos setores; falta de controle na identificação dos usuários; falta de segurança em todos os andares do prédio)	- Convém que áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido (ABNT NBR ISO/IEC 27002, 2013); - Planejamento de controles de acessos, buscando parcerias junto às Superintendências – UFPB; - A UFPB utiliza crachá como identificação visível.
Ruídos na comunicação (Conversas paralelas - problemas de comunicação)	- Convém que todos os funcionários da organização e, onde pertinente, partes externas devam receber treinamento, educação e conscientização apropriados, e atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções (ABNT NBR ISO/IEC 27002, 2013); - Oficinas (comunicação – trabalho em equipe); - A Pró-Reitoria de Gestão de Pessoas(PROGEPE) da UFPB oferece aos seus servidores cursos de capacitação de acordo com as necessidades e demandas.
Sinalização precária na Biblioteca	- Solicitar apoio da gestão para garantir a cooperação e coordenação de várias unidades de negócios (PELTIER, 2005); - Trablaho junto aos alunos do Laboratório de Práticas (Curso de Biblioteconomia – UFPB); - Seção de compras e licitações da Biblioteca Central da UFPB (baseado nos processos e editais de compras anuais da BC).
Invasão de *hacker* (Ataques a bases de dados)	- Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos (ABNT NBR ISO/IEC 27002, 2013); - Sistema de chamado – Superintendência de Tecnologia da Informação –STI/UFPB.
Falta de *backup* (Cópias de segurança)	- Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de gestão de cópias de segurança definida (ABNT NBR ISO/IEC 27002, 2013);

	- Sistema de chamado (requisição de serviços) – Superintendência de Tecnologia da Informação –STI/UFPB.
Cabeamento de rede exposto (Estrutura lógica**)**	Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade (ABNT NBR ISO/IEC 27002, 2013); - Sistema de chamado (requisição de serviços) – Superintendência de Tecnologia da Informação –STI/UFPB.
Obsolescência tecnológica (Falta equipamentos de qualidade).	Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade (ABNT NBR ISO/IEC 27002, 2013); - Seção de compras e licitações da Biblioteca Central da UFPB(baseado nos processos e editais de compras anuais da BC).

Fonte: Dados da pesquisa (2017).

A partir deste Quadro, pode-se ter uma visão das possíveis ações que poderão ser implementadas pela organização na direção da busca de melhorias para uma adequada proteção da informação e dos ativos informacionais no ambiente organizacional.

Diante do exposto, é necessário uma conscientização e sensibilização acerca da segurança da informação, com treinamentos, capacitação, orientação junto aos usuários externos e internos, para que se possa tomar conhecimento dos possíveis problemas relacionados à Segurança da Informação, além do planejamento de uma PSI, que, se configura como instrumento relevante, na consolidação de uma cultura de segurança no ambiente organizacional.

5.2 APLICAÇÃO E ANÁLISE DO QUESTIONÁRIO

Observa-se por meio da análise das respostas do questionário, um reflexo da realidade atual da segurança da informação na BC. Embora alguns respondentes expressem certo grau de conhecimento e nível de consciência sobre a necessidade de boas práticas em segurança da informação, evidencia-se a necessidade de ajustes, de maior conscientização e alinhamento de ações que venham a atender às demandas em SI, em caráter de urgência.

Conforme já citado, o questionário foi dividido em três categorias: pessoas, que visou obter informações acerca da percepção e comportamento dos respondentes em relação à SI e; processos e tecnologia, que objetivaram verificar as práticas em SI.

Ressalta-se que, em um dos questionários, um participante deixou de marcar uma questão (9), e em outra (10) marcou duas respostas. Desse modo, essas duas questões foram excluídas da análise. No Quadro 25, apresenta-se a tabulação dos dados obtidos por meio do questionário.

Quadro 25 – Tabulação dos dados do questionário

	N°	Questão	Resposta	Resultado	Percentual %
CATEGORIA 1 - PESSOAS	1	Você possui conhecimento sobre Segurança da Informação	Concordo Indiferente	7 1	87,5% 12,5%
	2	É importante conhecer a Política de Segurança da Informação da UFPB	Concordo fortemente Concordo	5 3	62,5% 37,5%
	3	Você permite a terceiros saberem sua senha de acesso	Concordo fortemente Discorda Discorda fortemente	1 2 5	12,5% 25% 62,5%
	4	Os documentos de trabalho devem ficar à mostra na mesa de trabalho	Concordo Indiferente Discorda	1 4 3	12,5% 50% 37,5%
	5	Para senhas de acesso, deve-se criar senha fortes, de preferência com 8 caracteres, utilizando letras e números	Concordo fortemente Concordo Indiferente	3 4 1	37,5% 50% 12,5%
	6	Ao deixar a estação de trabalho deve-se bloqueá-la	Concordo fortemente Concordo Discordo	3 4 1	37,5% 50% 12,5%
	7	Deve-se utilizar ou armazenar programas não destinados aos objetivos da sua função na Instituição	Concordo Indiferente Discordo Discordo fortemente	1 1 5 1	12,5% 12,5% 62,5% 12,5%
	8	O treinamento em conscientização, educação em segurança da informação, é importante	Concordo fortemente Concorda	5 3	62,5% 37,5%
	9	O estabelecimento de Política de Segurança da Informação em Bibliotecas Universitárias é fator de extrema necessidade	Concordo fortemente Concordo	3 4	42,9% 57,1%
CATEGORIA 2 - PROCESSOS	10	A Biblioteca faz uso de crachá para identificação pessoal dos servidores	Concordo fortemente Concordo	1 6	14,3% 85,7%
	11	Orientações são dadas acerca da manutenção de sua senha de acesso ao Sistema de Informação e a responsabilidade implicada pelo seu mau uso	Concorda Indiferente Discordo Discordo fortemente	3 2 2 1	37,5% 25% 25% 12,5%

	12	A alta administração tem ciência da necessidade que as instituições têm de um programa eficaz em Segurança da Informação	Concordo fortemente Concordo Indiferente Discordo	1 2 3 2	12,5% 25% 37,5% 25%
	13	No ambiente da Biblioteca são estabelecidas políticas de segurança da informação formalizadas	Concordo Indiferente Discordo Discordo fortemente	1 3 3 1	12,5% 37,5% 37,5% 12,5%
	14	Existe classificação das informações de acordo com seu grau de importância	Concordo Indiferente Discordo Discordo fortemente	2 3 2 1	25% 37,5% 25% 12,5%
	15	Existem na Biblioteca Central, procedimentos para garantia da continuidade das atividades, no caso de incidentes na segurança da informação	Concordo Indiferente Discordo	2 3 3	25% 37,5% 37,5%
	16	Existe inventário dos ativos de informação (considerando seu ciclo de vida – criação, processamento, armazenamento, disseminação, desbaste e descarte)	Indiferente Discordo	2 6	25% 75%
	17	Existem controles de entrada física para acessos a somente pessoas autorizadas	Concordo fortemente Discordo Discordo fortemente	1 5 2	12,5% 62,5% 25%
	18	Existe a necessidade de gerenciar as mídias removíveis para prevenir que as informações armazenadas sejam divulgadas sem autorização, modificadas, removidas ou destruídas	Concordo fortemente Concordo Discordo	2 5 1	25% 62,5% 12,5%
	19	A Biblioteca possui controles para proteção física contra desastres naturais, ataques maliciosos e acidentes	Discordo Discordo fortemente	5 3	62,5% 37,5%
CATEGORIA 3 -	20	A atualização do antivírus é feita periodicamente	Concordo Indiferente Discordo Discordo fortemente	2 2 2 2	25% 25% 25% 25%

	21	O antivírus deve ser de licença paga	Concordo Indiferente Discordo	5 2 1	62,5% 25% 12,5%
	22	É necessário o controle para proteção no uso de mídias removíveis (*pen drive, memory cards*)	Concordo fortemente Concordo	3 5	37,5% 62,5%
	23	Deve-se estabelecer restrições para instalação de softwares	Concordo Discordo	7 1	87,5% 12,5%

Fonte: Dados da pesquisa (2017).

Abaixo serão descritas cada uma das categorias e suas respectivas análises, a partir das respostas obtidas por meio do questionário.

5.2.1 Categoria - Pessoas

Na questão 1, sobre o conhecimento em SI, embora 7 (87,5%) dos respondentes demonstrem ter conhecimento sobre SI e 1 (12,5%) seja indiferente, observa-se uma distância entre esse conhecimento e a disposição a boas práticas em SI. Neste mesmo rol de importância se enquadra a questão 2, que diz respeito a conhecer a PSI da UFPB em que 5 (62,5%) concordam fortemente e 3 (37%) concordam e igualmente a questão 8, sobre treinamento e conscientização em SI. Em relação à segurança da informação, a pesar de 7 dos respondentes terem conhecimento e 5 saberem da importância da PSI/UFPB, mas 1 (12,5%) se mostrou indiferente ao assunto em SI, merecendo uma atenção maior, pois pode ser um ponto, suscetível, a questões relacionadas a engenharia social[3] e/ou outros problemas. Conseguinte a isso, a questão 9 trata da importância do estabelecimento de PSI. Nesse bojo, evidencia-se uma tendência bastante favorável do conhecimento, bem como da aceitação de PSI. Embora possa haver uma tendência a atitudes politicamente corretas, no que diz respeito à boas práticas em SI, percebe-se pelas observações empíricas do pesquisador, que ainda não são cumpridos com rigor os requisitos de segurança.

De acordo com o Guia de Referência de Segurança da Informação da Presidência da República, que é o documento normativo em matéria de SI, "os empregados devem entender porque a segurança é importante para a sua organização e para o seu dia-a-dia. Devem saber de que forma as falhas de segurança podem afetar a organização, bem como contra o que se proteger e como se proteger" (BRASIL, 2010, p. 88). Como se trata de profissionais que lidam com a

[3] Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações (CERT.Br., 2012. p.115).

gestão da informação, este cuidado a propósito da SI, corresponde às atribuições e prerrogativas inerentes aos que cumprem estas funções. Ainda assim, é positivo perceber-se um grau de conhecimento e consciência significativos, no sentido de proteção da informação.

Na construção de um "programa de conscientização, é importante não focar apenas no 'o que' e 'como', mas também no 'por quê'". (ABNT NBR ISO/IEC 27002, 2013, p. 21) De acordo com a Norma, importa que haja da parte do funcionário, o entendimento dos objetivos da SI, e seu próprio comportamento no seu impacto potencial, positivo e negativo na organização. Desse modo, "a política de segurança explicita, para todos os usuários que acessam e usam a informação, qual é a filosofia da organização sobre esse recurso, visando assegurar que toda informação da empresa e de seus clientes esteja protegida contra possíveis perdas, danos, destruição e/ou mau uso" (FONTES, 2006, p. 3).

No que se refere a permitir a terceiros saber da senha, questão 3, embora 5 (62,5%) respondentes discordem fortemente e 2 (25%) discordem, 1 (12,5%) permite que conheçam sua senha, o que se torna preocupante, haja vista que, esta abertura, por si só, pode se constituir um ponto de vulnerabilidade, e exposição às ameaças. Também tem relação com a questão acima a 5, referente a construção de senhas fortes, em que 3 (37,5%) concordam fortemente e 4 (57,1%) concordam com a prática do uso de senhas fortes, enquanto que 1 (12,5%) mostrou-se indiferente. Mas, basta um estar indiferente, para que se evidencie a necessidade de que todos estejam cumprindo com rigor, as regras, de modo a se garantir a confidencialidade da senha individual e proteção da informação. No entanto, para que "os controles de senha funcionem, os usuários devem ter pleno conhecimento das políticas de senha da instituição e devem ser orientados e estimulados a segui-las fielmente" (TCU, 2012, p. 20). Isto converge para o estabelecimento de políticas de segurança que possam garantir a confidencialidade, integridade e disponibilidade das informações, bem como, barrar o acesso indevido a sistemas, por pessoas não autorizadas. Pelas observações, não existe norma formalizada e explicitada acerca de construção de senhas fortes.

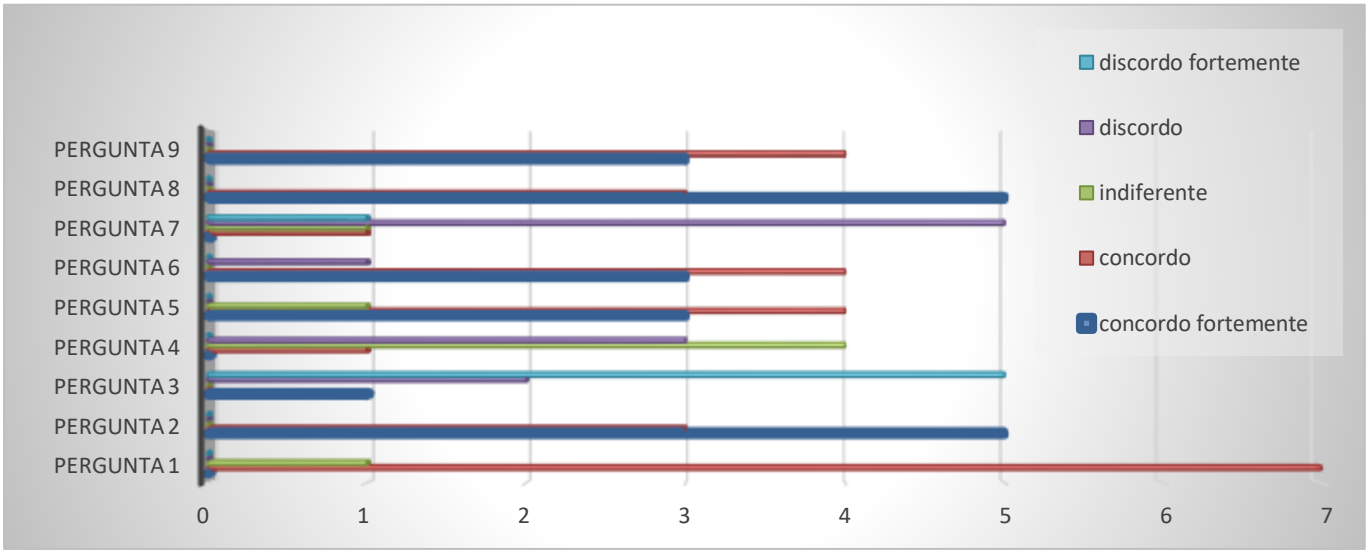
É importante que se assegure a privacidade e proteção das informações de identificação pessoal, em conformidade com legislação e regulamentação pertinente, quando da sua aplicação (ABNT NBR ISO/IEC 27002, 2013).

Na questão 4, "política de mesa limpa", 1 (12,5%) respondente concorda que os documentos fiquem à mostra na mesa de trabalho, 4 (57,1%) são indiferentes, e 3 (37,5%) discordam. O fato de um participante ser favorável que os documentos fiquem à mostra e quatro estarem indiferentes, expressa um desconhecimento dos riscos a que a segurança das informações está exposta, pois "uma política de mesa limpa e tela protegida reduz o risco de

acesso não autorizado, perda e dano da informação durante e fora do horário de trabalho" (ABNT NBR ISO/IEC 27002, 2013, p. 56).

A questão 7, referente à utilização e instalação de programas não pertinentes às atividades da instituição, 1 (12,5%) concorda na instalação e uso, 1 (12,5%) mostrou-se indiferente, enquanto que 5 (62,5%) discordam e 1 (12,5%) discorda fortemente. É expressivo o número dos que não são favoráveis à instalação e uso de programas que não têm pertinência aos objetivos da organização. No entanto, o fato de um mostrar-se indiferente, demonstra a necessidade de uma maior conscientização.

Figura 6 – Gráfico das respostas do questionário – Categoria Pessoas



Fonte: Dados da pesquisa (2017).

Para tanto, a ABNT NBR ISO/IEC (27002:2013, p. 69) corrobora com recomendação de que: "A instalação de *software* não controlado em dispositivos computadorizados pode introduzir vulnerabilidades [...] gerar o vazamento de informações, perda de integridade ou outros incidentes de Segurança da Informação [...]".

Mesmo que a PSI tenha suas variações adaptadas às peculiaridades de cada organização e seu escopo, deverá abranger vários aspectos, cruciais para uma adequada proteção dos ativos de informação. Isto se aplica, sobretudo, aos aspectos humanos da segurança que, de acordo com Beal (2008), a PSI deve trazer em seu conteúdo "definições sobre a política de segurança de pessoal (processos de admissão e demissão, requisitos de segurança aplicáveis a funcionários e prestadores de serviço, treinamento em segurança)".

Nesta categoria pôde-se observar que os respondentes expressam um conhecimento e a noção da importância da SI, ainda que pouco. No entanto, percebe-se que é necessário um

entendimento e maior conscientização assunto, de forma que os princípios relacionados à segurança da informação, possam capacitá-los e incorporar estes princípios à sua vida, quer profissional, quer pessoal.

5.2.2 Categoria – Processos

Na questão 10, referente ao uso de crachás para identificação dos servidores, 1 (12,5%) respondente concorda fortemente e 6 (75%) concordam. Pelas observações *in loco*, percebe-se que nem todos os servidores usam crachás. Mesmo que o número de servidores que não utilizam crachás seja uma minoria, expressa uma não conformidade com as regras estabelecidas quanto ao uso de crachás. Isso corrobora com o entendimento de que a utilização de crachá para a identificação funcional, apesar de tradicional, é um meio ainda eficaz para o controle de acesso físico.

Sobre as orientações quanto ao uso de senha e a responsabilidade implicada no mau uso, na questão 11, 3 (37,5%) respondentes concordam que há orientações, 2 (25%) mostraram-se indiferentes, e 1 (12,5%) discorda fortemente. O fato de ter um que discorda fortemente que não há orientações, evidencia ao menos, um indício de que a difusão dessa informação não é suficientemente clara, a ponto de sanar todas as dúvidas quanto a responsabilidade dos usuários sobre sua senha. Embora possa haver orientações, conforme mostra a resposta, o que se observa é que elas não são explicitadas, formalizadas, ou didaticamente dispostas, de maneira que o usuário tenha ciência das regras. Nesta perspectiva, a ABNT NBR ISO/IEC 27002 (2013, p. 106), recomenda: “Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação pertinente, quando aplicável”. É responsabilidade da Gestão fazer que chegue ao conhecimento de todos os envolvidos na organização, a importância da proteção da informação.

Na questão 12, referente ao conhecimento que a alta administração tem acerca da necessidade que tem a instituição de programas em SI, 1 (12,5%) concorda fortemente que a Alta administração tem ciência, 2 (25%) concordam, 3 (37,5%) são indiferentes e 2 (25%) discordam. Nota-se que há um número expressivo dos que demonstram indiferença, o que acena para o fato do não conhecimento sobre o papel da alta administração frente a SI na organização. Enquanto que, os que discordam, atestam a necessidade de uma aderência de parte da Alta administração à SI, bem como, orientações adequadas sobre proteção da informação a todos os envolvidos na organização.

O sucesso da PSI, dependerá, intrinsecamente, do comprometimento da Alta administração. Quanto maior for seu envolvimento e atuação, nos processos de elaboração e implantação da PSI, maior a chance de a mesma ser efetiva e eficaz. Isto deve ser formalizado por escrito. (TCU, 2012)

Com relação ao estabelecimento de PSI formalizada no ambiente da BC, 1 concorda que há, 3 (37,5%) são indiferentes, 3 (37,5%) discordam e 1 (12,5%) discorda fortemente. Embora o número dos que discordam assemelhe-se aos que são indiferentes, aponta para a evidencia da inexistência de políticas de segurança da informação formalizadas. O que expressa a necessidade da elaboração de diretrizes que venham a nortearem a boas práticas em Segurança da Informação. Nota-se, portanto, que a PSI é o documento necessário para o registro dos "princípios e as diretrizes de segurança adotados pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos" (BEAL, 2008, p. 43).

Quanto à classificação das informações de acordo com seu grau de importância, com relação à questão 14, 2 (25%) concordam que existe, 3 (37,5%) mostraram-se indiferentes, 2 (25%) discordam que existe e 1 (12,5%) discorda fortemente. Nota-se o grupo dos que se mostraram indiferentes ao processo de classificação das informações, apresenta ponderação mais alta. Isto expressa a necessidade de observar se realmente esse tipo de procedimento existe, de fato. O que se observa é que não há um processo formalizado com relação a classificação das informações, embora 2(dois) dos participantes terem concordado parcialmente, o que aponta para uma inconsistência, que precisa de atenção, no sentido de se verificar a relevância desse processo de classificação das informações para a biblioteca. De acordo com ABNT 27002 (2013), a classificação das informações permite "assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização".

Na afirmativa que pondera acerca da existência de procedimentos para a garantia da continuidade das atividades, no caso de incidentes na SI, questão 15, 2 (25%) respondentes concordam que existe, 3 (37,5%) mostraram-se indiferentes e 3 (37,5%) discordam que existe. Estes resultados evidenciam a necessidade de uma atenção maior ao estabelecimento de procedimentos que possam atender a demanda de continuidade das atividades, no caso de incidentes que possam vir a comprometer os serviços.

Para a redução dos riscos que permita garantir a continuidade dos negócios, em um nível aceitável, Beal (2008, p. 137) assevera que "é necessário desenvolver um entendimento claro dos riscos associados a impactos graves (desastres), que levem à redução significativa

ou interrupção dos serviços de informação". Isto se aplica, para tanto, à Análise e Avaliação de Riscos (PELTIER, 2005), abordada nesta pesquisa. Um processo que deve anteceder a elaboração da PSI.

Quanto ao inventário de ativos, questão 16, 2 (25%) mostraram-se indiferentes e 6 (75%) discordam. Uma evidência de que não existe e/ou há inconsistência na elaboração de inventário dos ativos, e nem todos tenham conhecimento. Neste sentido, a ABNT/NBR/ISO/IEC 27002 (2013, p. 23) recomenda que "os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido". É bem expressivo o número dos que discordam da inexistência de inventário de ativos, o que demonstra a necessidade de se estabelecer procedimentos, regras que venham a atender esta demanda.

É necessário ressaltar, que a Política de Segurança da Informação da UFPB (PSI/UFPB), traz em seu Art. 5º, Item III, aspecto que deve ser observado quanto ao requisito de segurança sobre o manuseio e tratamento da informação em que "define padrões e princípios relacionados ao manuseio de informações, o que incluem inventários, administração e propriedade sobre dados, eliminação e remoção de informação, informações disponíveis em mesas de trabalho, telas de computador, material impresso, etc. (RESOLUÇÃO 32/2014, sem paginação).

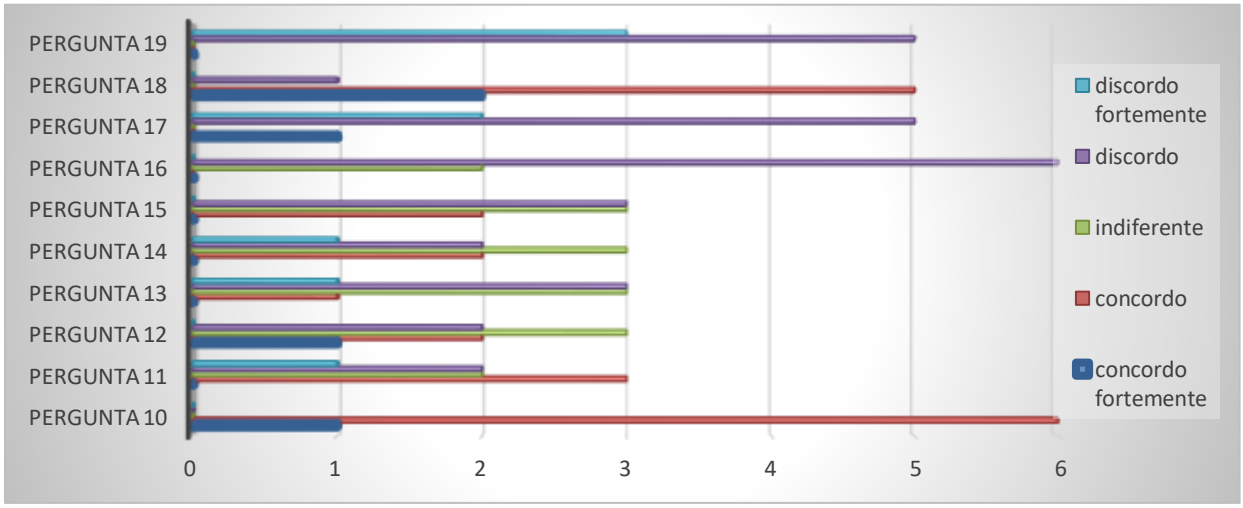
Na questão 17, sobre controle de acesso a pessoas autorizadas, 1 (12,5%) concorda fortemente, 5 (62,5%) discordam que haja esse tipo de controle e 2 (25%) discordam fortemente. Observou-se que o controle de acesso a somente pessoas autorizadas restringe-se a um determinado setor, enquanto que a outros não se aplica. O que requer uma revisão neste controle. A ausência de controles de acessos, ou controles insatisfatórios, torna-se um ponto de vulnerabilidade, que poderá vir a ser explorado por ameaças, caso não estejam adequadamente estabelecidos. Nesta perspectiva, Beal (2008) assevera a necessidade da existência de um conjunto específico de medidas de prevenção, intitulado barreiras de segurança. Neste sentido:

> Uma barreira corresponde a qualquer obstáculo colocado para prevenir um ataque, podendo ser física (cerca elétrica, parede), lógica (processo de logon para acesso a uma rede) ou uma combinação de ambas (autenticação de indivíduos por dispositivo biométrico para concessão de acesso, catraca eletrônica, porta aberta por cartão magnético) (BEAL, 2008, p. 81).

Na questão 18, que trata da existência da necessidade de gerenciamento das mídias removíveis, na prevenção das informações, no sentido da não divulgação sem autorização, modificação, remoção ou destruição, 2 (25%) concordam fortemente que há essa necessidade, 5 (62,5%) concordam e 1 (12,5%) discorda. Nota-se que, mesmo existindo a necessidade, isto implica a consecução de ajustes que possam estar alinhados a regras, procedimentos explícitos e formalizados. O processo de gerenciamento de mídias removíveis, previne que a informação seja divulgada sem autorização, modificada, removida ou mesmo destruída, considerando que os procedimentos estejam em conformidade com a classificação vigente na organização (ABNT NBR ISO/IEC, 27002, 2013).

Na questão 19, sobre a existência de controles para a proteção física contra desastres naturais, ataques maliciosos e acidentes, 5 (62,5%) discordam e 3 (37,5%) discordam fortemente. Isto revela um indício da necessidade de políticas de segurança da informação que atendam à essas demandas e corrobora com o grupo de ameaças físicas classificadas, anteriormente. Segue Figura 7, que apresenta o gráfico das respostas.

Figura 7 – Gráfico das respostas do questionário – Categoria Processos



Fonte: Dados da pesquisa (2017).

Nota-se que, apesar do conhecimento quanto à SI, as práticas em Segurança da Informação ainda são insatisfatórias, precisam ser formalizadas, expressas por escrito, junto aos participantes da organização, de maneira que possa haver um melhor entendimento do seu objetivo maior, por meio de conscientização, de maneira que possam ser efetivadas por todos da organização. O que se observa é que, as preocupações dos gestores, tendem a convergirem, com maior ênfase, para a proteção da informação, no que diz respeito às ameaças relacionadas

a infraestrutura física, segurança física e ambiental, em detrimento da proteção das formas de gestão, dos processos gerenciais, que envolve a capacitação dos recursos humanos, frente às demandas em segurança da informação.

5.2.3 Categoria – Tecnologia

Quanto à periodicidade da atualização do antivírus, questão 20, 2 (25%) concordam que é atualizado periodicamente, 2 (25%) mostraram-se indiferentes, 2 (25%) discordam e 2 (25%) discordam fortemente. A discordância foi expressiva, o que evidencia a necessidade de se rever os processos de atualizações de antivírus, para que os equipamentos, sistemas não estejam expostos a ataques maliciosos, que venham a comprometer as atividades relacionadas ao processamento, disseminação e acesso à informação.

Na questão 21, afirmativa de que o antivírus deve ser pago, 5 (62,5%) concordam, 2 (25%) indiferentes e 1 (12,5%) discorda que o antivírus deve ser pago. Observa-se que há uma tendência maior em que o antivírus seja de licença paga, o que aponta para a preocupação em obter um antivírus, eficaz e eficiente, que possa garantir a proteção contra invasões do sistema.

No intuito de garantir a proteção dos sistemas contra códigos maliciosos que, consequentemente, causam danos que podem comprometer significativamente os sistemas e atividades relacionadas ao processamento da informação, processos de compras e outros, a ABNT NBR ISO/IEC 27002 (2013) recomenda que “sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário”.

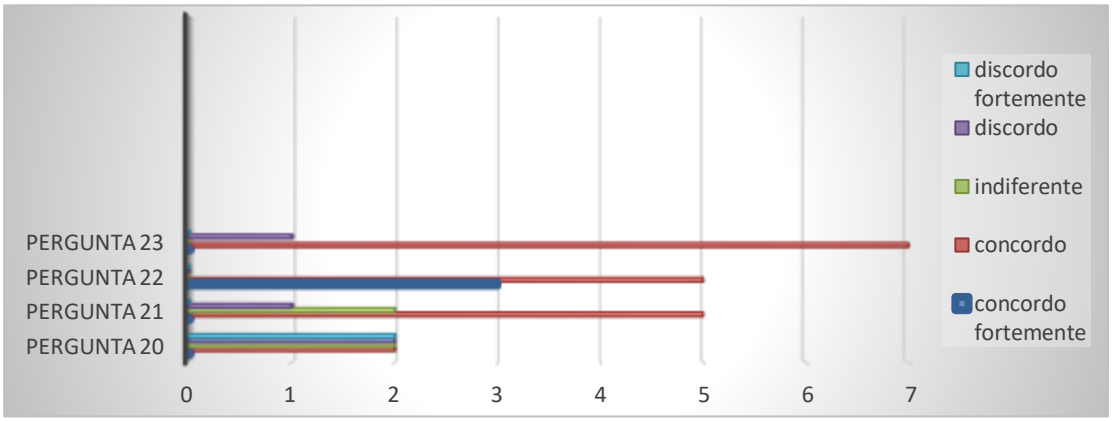
Na questão 22, que trata de controles para a proteção no uso de mídias removíveis, 3 (37,5%) concordam fortemente e 5 (62,5%) concordam, na implementação de controles. Isto reflete a necessidade de políticas específicas de SI. Por fim, na questão 23, 7 (87,5%) concordam que é preciso o estabelecimento de restrições para instalação de software, enquanto que 1 discorda. Assim, a ABNT NBR ISO/IEC 27002 (2013, p. 69) recomenda que “sejam estabelecidas e implementadas regras definindo critérios para a instalação de *software* pelos usuários.”

Com base nos resultados das questões, observa-se que os problemas que, podem ser considerados mais recorrentes são: o estabelecimento de políticas de segurança da informação, que não existe; as práticas em segurança da informação, que são insatisfatórias, e devem estar associadas a uma conscientização, educação em segurança da informação, que

abranja tanto funcionários, quanto pessoal terceirizado da organização; ausência de procedimentos para garantir a continuidade das atividades, no caso de incidentes na segurança da informação; ausência de inventário dos ativos; ausência de controles para proteção física contra desastres naturais, ataques maliciosos, acidentes e controles com restrições de acesso às áreas de processamento da informação e administrativas. Esse conjunto de problemas pode facilitar que ameaças explorem vulnerabilidades, e venham a acarretar danos à organização como um todo.

Isto se aplica ao planejamento de ações que permitam a adoção de medidas preventivas, que possam permitir a redução dos riscos à Integridade, Confidencialidade e Disponibilidade da informação. De acordo com Beal (2008, p. 71): "As pessoas são, acertadamente, consideradas o 'elo frágil' da segurança da informação". De fato, o fator humano é um dos elementos em que se deve dar maior ênfase no processo de planejamento de PSI, pois cada pessoa na organização tem a responsabilidade de proteger a informação e, isso implica, na conformidade com as diretrizes, regras e procedimentos, fator este, preponderante para o sucesso da PSI. Segue Figura 8 que apresenta o gráfico da resposta do questionário – Categoria Tecnologia.

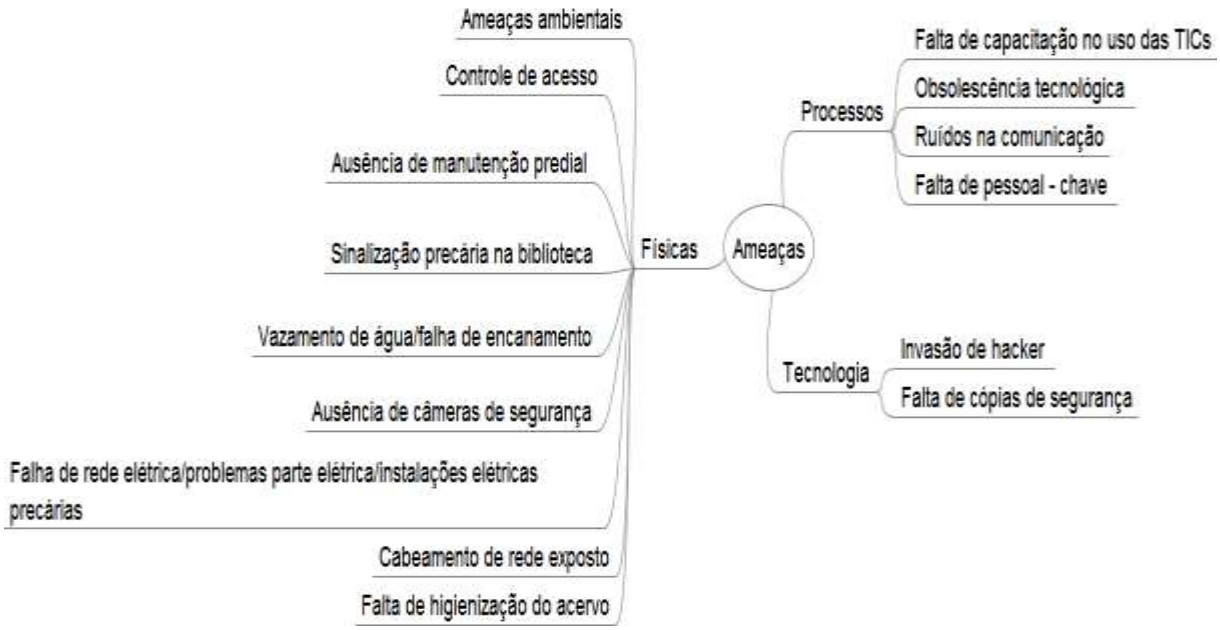
Figura 8 – Gráfico das respostas do questionário – Categoria Tecnologia



Fonte: Elaborado pelo autor, com base nos dados da pesquisa (2017).

A partir da análise e avaliação de riscos, elaborou-se um mapa de ameaças, em que constam as ameaças de probabilidade e impacto altos, considerados pelos participantes da pesquisa, durante o processo de classificação das ameaças, classificadas da seguinte forma: 4 ameaças relacionadas a processos; 9 ameaças relacionadas à segurança física e 2 ameaças relacionadas à tecnologia (Figura 9) totalizando 15 ameaças:

Figura 9 – Mapa de Ameaças



Fonte: Dados da pesquisa (2017). Elaborado pelo *FreeMind*.

O método FRAAP aplicado à pesquisa, recomenda que a partir dos resultados da avalição e análise dos riscos, sejam elaborados planos de ação que possam, efetivamente, diminuir os riscos identificados. Todavia, conforme os objetivos específicos, esses planos foram substituídos pela construção de uma minuta de Política de Segurança da Informação que esteja alinhada à natureza das atividades da BC e possam atender as suas necessidades, de modo a permitir a salvaguardar de seus ativos e recursos informacionais. Com base nos dados da análise e avaliação de riscos e do questionário, foi identificado uma recorrência maior dos riscos relacionados à Ameaças físicas, mas sem, no entanto, eximir as ameaças lógicas.

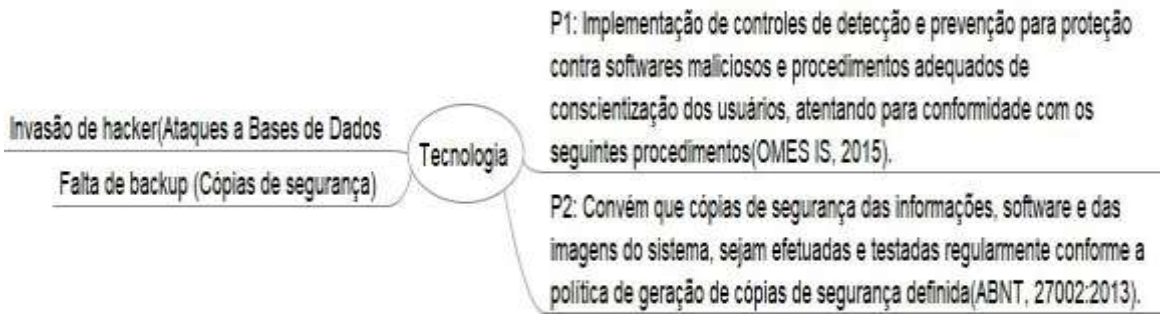
Diante do exposto, observa-se que no âmbito da SI se encontram diversas políticas com regras específicas que vão variar de organização para organização, como já ressaltado anteriormente. A Figura 10 apresenta mapa das ameaças relacionados a segurança física e do ambiente, identificadas com probabilidade e impacto alto e seus respectivos regulamentos de segurança. Onde se lê P, significa proposta para política.

Figura 10 - Ameaças relacionadas à segurança física e do ambiente

Fonte: Dados da pesquisa (2017). Elaborado pelo *FreeMind*.

No conjunto dos regulamentos de segurança da informação, é necessário que estejam explícitas as responsabilidades e obrigações, bem como o poder de autoridade. Na construção dos regulamentos, deve vir explícitos e claros, a definição de padrões e de procedimentos que todos da organização devem seguir. De maneira que estes regulamentos formalizados e publicados, possam permitir aos usuários o conhecimento de como proceder nas situações relacionadas a informação e os recursos informacionais (FONTES, 2012). A Figura 11 apresenta as ameaças relacionadas à tecnologia e respectivos requisitos, conforme identificação em processo anterior.

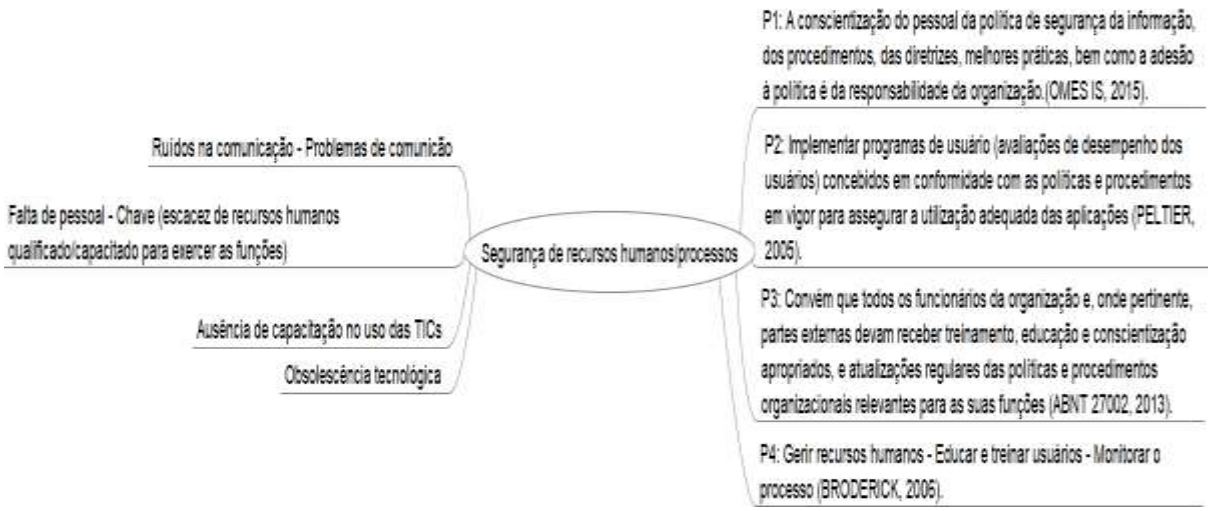
Figura 11 – Ameaças relacionadas à Tecnologia



Fonte: Dados da pesquisa (2017). Elaborado pelo *FreeMind*.

A Figura 12 apresenta as ameaças relacionadas à segurança de recursos humanos, considerando também os processos operacionais. Entende-se que, para uma adequada proteção destes, necessita que os recursos humanos com relação à SI, suas práticas devem estar em conformidade com as normas de segurança.

Figura 12 – Ameaças relacionadas à Segurança de Recursos humanos/processos



Fonte: Dados da pesquisa (2017). Elaborado pelo *FreeMind*.

Nota-se, para tanto, que a Biblioteca está inserida num contexto que, por sua vez, lida com a várias formas de gestão, quer seja, de acervos físicos e digitais (livros digitais, portais eletrônicos de pesquisa, dentre outros serviços), quer seja sistemas de informação e recursos humanos, que exigem a existência de políticas com diretrizes, regras e procedimentos, que

possam garantir o uso adequado e a salvaguarda de seus ativos de informação, bem como de seu patrimônio cultural como um todo.

A partir das informações obtidas com a análise FRAAP, e análise do questionário, percebe-se a existência de um ponto de incongruência, embora se demonstre, por meio das falas, um certo conhecimento da necessidade da proteção da informação. Há, neste caso, uma dificuldade na percepção da proteção da informação de forma integrada, que concebe a segurança da informação abrangendo as dimensões pessoa, processos e tecnologia.

Isto converge também para uma dificuldade de entendimento da necessidade de se proteger as formas de gestão, pois percebe-se que as preocupações dos gestores se direcionam para a proteção dos ativos informacionais, em detrimento da proteção dos processos organizacionais. Entende-se, assim, que é necessário uma conscientização e educação em segurança da informação, de maneira que se possa capacitar os participantes da organização para o desenvolvimento de uma cultura de melhores práticas em SI.

Assim sendo, verificou-se que a Biblioteca Central da UFPB necessita refletir sobre um plano de ação direcionado à segurança da informação, para a garantia de confidencialidade, integridade e disponibilidade com vistas ao desenvolvimento de boas práticas e elaboração de sua política de segurança da informação e salvaguardar das informações gerenciais críticas da organização.

Com os resultados, espera-se contribuir com a Segurança da Informação no âmbito da Biblioteca Central da UFPB com a proposta de minuta para Política de Segurança da Informação, permitindo novas contribuições para o desenvolvimento dos processos de gestão da Biblioteca Universitária.

6 CONSIDERAÇÕES FINAIS

A pesquisa buscou responder a seguinte questão: **Como ordenar elementos de Gestão de Segurança da Informação em uma Política de Segurança para uma biblioteca?**

Os objetivos específicos estabelecidos para o atendimento do propósito desta pesquisa, foram alcançados por meio da construção do referencial teórico, que permitiu conhecer os aspectos concernentes a segurança da informação, possibilitando, para tanto, uma melhor compreensão dos elementos que envolvem os requisitos de segurança da informação e sua aplicação nas bibliotecas.

Um elemento crucial para análise e avaliação dos riscos nesta pesquisa, foi a aplicação da metodologia FRAAP sugerida por Peltier (2005), que possibilitou o mapeamento dos riscos, por meio da realização da identificação das ameaças à segurança da informação nos processos e recursos informacionais no âmbito da Biblioteca Central, o que forneceu subsídios para ordenar os elementos para elaboração de uma minuta de Política de Segurança da Informação, conforme as necessidades da BC.

Entender os riscos e ativos informacionais em uma biblioteca universitária não é uma atividade trivial, pois, diferente de outras organizações, a biblioteca tem com seu "negócio" dar acesso à informação. Sendo a disseminação da informação uma de suas atividades fins. Nesse contexto é comum que o bibliotecário entenda seu acervo como ativos informacionais. Contudo, esta pesquisa deixa claro que o acervo, ainda que um ponto de preocupação nos bibliotecários, não é o único foco de uma PSI para bibliotecas.

A análise e avaliação de riscos identificou ameaças físicas (maior incidência), ameaças relacionadas às formas de gestão (processos operacionais) e as relacionadas a estrutura lógica (TI). Neste processo, foi identificado um conjunto de 15 ameaças, dentre as quais, foram identificadas nove Ameaças Físicas, duas Ameaças Lógicas, quatro Ameaças – Processos, considerando também os recursos humanos envolvidos nestes processos.

Uma vez identificadas as ameaças, foram classificadas mediante os parâmetros de probabilidade de ocorrência e o consequente impacto à organização, considerando as definições para Nível de Probabilidade e Impacto, a partir de uma abordagem qualitativa.

Os resultados permitiram criar uma Matriz de risco, e a partir desta matriz, buscar orientações na literatura especializada para a identificar controles e recomendações como instrumentos de mitigação destes riscos.

Observou-se que os relatos dos participantes da pesquisa, durante a reunião dirigida e no questionário, boa parte admite ter conhecimento em SI, e mesmo demonstrando observação de normas (não formalizadas) quanto ao lidar com a informação e uso dos recursos informacionais. Contudo ficou evidente que estes procedimentos não são institucionalizados, não são realizados por todos de forma rotineira, o que demonstra a necessidade de criação de uma cultura de segurança da informação, por meio de planos de ação direcionados à proteção da informação.

Um fator positivo foi a disposição e cooperação dos participantes da pesquisa durante o processo de aplicação do método para identificação das ameaças à SI no âmbito da biblioteca. Isto sugere uma pré-disposição na percepção da importância de uma PSI em uma biblioteca. Um ponto limitador é que a pesquisa foi realizada somente com gestores, e essa amostra não permite um diagnóstico mais apurado, principalmente em relação ao entendimento dos demais colaboradores da BC/UFPB sobre a SI.

A partir da análise dos resultados da aplicação do método FRAAP, pôde-se identificar pontos de vulnerabilidades, ameaças e riscos que a biblioteca precisa observar no sentido de desenvolver um plano de ação que venham a efetivar melhorias contínuas à proteção da informação e seus ativos, acenando para implementação de políticas que venham a subsidiar programas de segurança da informação. Esta pesquisa permitiu uma visão dos possíveis impactos negativos que podem acontecer aos processos organizacionais quando não observado as práticas em SI e a obtenção do conhecimento necessário para implementação de controles eficazes.

Algo que ainda precisa ser debatido e necessita de tempo para amadurecimento é a necessidade que a biblioteca tem para separar seus processos de gestão interna, processos organizacionais, que geram ativos informacionais necessários para seu funcionamento e da própria universidade e do seu acervo. O grupo que compôs a amostra deste estudo teve dificuldades de separar estes dois elementos, tanto que grande parte das ameaças identificadas como críticas forma relacionadas à parte física da biblioteca.

Por fim, conforme proposto no objetivo geral desta pesquisa foi elaborada uma minuta de Política de Segurança da Informação (Apêndice B), considerando os aspectos: pessoas, processos, tecnologia, e tecendo considerações acerca das responsabilidades dos usuários da política, do uso adequado dos recursos informacionais, o que de fato se deve proteger, ou seja, as diretrizes que a organização deve adotar para que a proteção da informação seja garantida em conformidade com os princípios: integridade, confidencialidade e disponibilidade. A proposta de minuta para Política de Segurança da Informação, possibilita novas contribuições

para o desenvolvimento dos processos de gestão da Biblioteca Universitária com foco na segurança da Informação.

Na política sugere-se um esforço conjunto no sentido do planejamento de medidas preventivas contra possíveis ameaças à segurança da informação como: revisão e melhorias na segurança física e do ambiente; manutenção periódica de equipamentos e estrutura lógica (cabeamento), manutenção de sistemas operacionais; manutenção predial e dos acervos informacionais; orientações quanto a importância do uso de senhas fortes; orientações quanto à proteção das estações de trabalho, quanto à políticas de mesa limpa e tela limpa; revisão no controle de acesso físico, com controles apropriados que assegurem a entrada de somente pessoas autorizadas com permissão de acesso; planejamento de segurança física para áreas de processamento e armazenamento da informação; planejamento de proteção contra ameaças externas e ambientais; treinamento em conscientização e educação em segurança da informação; treinamentos em capacitação no uso das TICs; orientações acerca das responsabilidades que todos os envolvidos na organização tem para com a proteção da informação e uso dos recursos informacionais; criação de uma gestão dos elementos de tecnologia, como canal de comunicação junto a STI, para garantir a manutenção, e se seguir as normas de segurança. Estas são apenas algumas sugestões de ações que possam guiar a biblioteca à SI, por meio de uma PSI institucionalizada e fomentar novas pesquisas em Segurança da Informação em Bibliotecas Universitárias.

REFERÊNCIAS

ACCART, Jean-Philippe. **Serviço de referência**: do presencial ao virtual. Brasília, DF: Briquet de Lemos/Livros, 2012.

ALMEIDA, Maria Christina Barbosa de. **Planejamento de bibliotecas e serviços de informação**. 2. ed. Brasília, DF: Briquet de Lemos/Livros, 2005.

ARAÚJO, Carlos Alberto Ávila de. Políticas de informação em bibliotecas, arquivos e museus. In: GARCIA, Joana Coeli Ribeiro; TARGINO, Maria das Graças (Org.). **Desvendando facetas da gestão e políticas de informação**. João Pessoa, PB: Editora da UFPB, 2015. v. 2

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001. Tecnologia da informação — Técnicas de segurança — Sistemas de Gestão de Segurança da informação — Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

AUN, Marta Pinheiro. A construção de políticas nacional e supranacional de informação: desafio para os Estados nacionais e blocos regionais. **Ciência da Informação**, [S.l.], v. 28, n. 2, aug. 2013. ISSN 1518-8353. Disponível em:<http://revista.ibict.br/ciinf/article/view/841/874>. Acesso em: 22 jul. 2017.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BELARMINO, Valdete Fernandes; ARAÚJO, Wagner Junqueira de. Análise de vulnerabilidades computacionais em repositórios digitais. **Biblios**, n.56, 2014.

BEAL, Adriana. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas Organizações. São Paulo: Atlas, 2008.

_____. **Gestão estratégica da informação**: como transformar a informação e tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004.

BONILLA, Sandra M. ; GONZÁLEZ, Jaime A. Modelo de seguridad de la información. **Ing. USBMed**, v. 3, n. 1, Enero-Junio 2012.
Disponível em: <https://dialnet.unirioja.es/servlet/articulo;jsessionid=BC4799A1BF83D956D28B9E133FDEE6B9.dialnet02?codigo=4692844>. Acesso em: 01 ago. 2016.

BULGURCU, Burcu; CAVUSOGLU, Hasan; BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly**, v. 34, n. 3, p. 523-548, September 2010. Disponível em:<www.periodicos.capes.gov.br > Acesso em: 2 jul. 2016

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015 – 2018**: versão 1.0. Brasília, DF: Presidência da República, 2015. Disponível em:<http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf>. Acesso em: 04 ago. 2016

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Guia de referência para a segurança das infraestruturas críticas da informação**: versão 01 - nov. / 2010. Brasília, DF: Presidência da República, 2010. Disponível em:<http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 04 ago.2016

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa GSI/PR nº 01, 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. Brasília, DF, GSI/PR, 2008. Disponível em:<http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/52-instrucoes-normativas>. Acesso em: 08 ago. 2016.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 02/IN01/DSIC/GSIP. **Metodologia de gestão de segurança da informação e comunicações.** Brasília, GSI/PR, 2008. **Disponível em: <**http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf**>.** Acesso em: 12 ago. 2016.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal. In: **Coletânea de Legislação Relacionada ao Credenciamento de Segurança e ao Tratamento da Informação Classificada na Administração Pública Federal V2.0**. Brasília, DF[documento eletrônico sem data de publicação]. Disponível em: <http://dsic.planalto.gov.br/documentos/NSC/coletanea_legis_NSC.pdf>. Acesso em: 12 ago. 2016.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. Rede Nacional de Ensino e Pesquisa - RNP. **Relatório Anual**: alertas, vulnerabilidades e incidentes de segurança, n.5, set. 2015. Brasília, DF: MCT, 2015.
Disponível em:<https://www.rnp.br/sites/default/files/relatorio_incidentes_2013.pdf>. Acesso em: 16 ago. 2016.

_____. Ministério da Ciência, Tecnologia e Inovação. Rede Nacional de Ensino e Pesquisa - RNP. **CAIS em Resumo**: Incidentes de segurança da informação 2013. Brasília, DF: MCT, 2013.Disponível em: <https://rnp.br/servicos/seguranca/educacao-e-conscientizacao-seguranca>. Acesso em: 16 ago. 2016.

BRASIL. Tribunal de Contas da União. 4. ed. **Boas práticas em segurança da informação**. Brasília, DF: TCU, 2012.

BRODERICK, J. Stuart. ISMS, security standards and security regulations. **Information Security Technical Report**, v. 11, 2006, p. 26 – 31
Disponível em: <www.sciencedirect.com/science/article/pii/S1363412705000750>. Acesso em: 28 maio 2017.

CAETANO, Ana Carolina de Souza; FERNANDES, Geni Chaves. Registros laborais nas bibliotecas universitárias federais: ética, política e acesso a informação. **Inf. Inf**., Londrina, v. 20, n. 3, p. 433 - 456, set. / dez. 2015. Disponível em: <http:www.uel.br/revistas/informacao/>. Acesso em: 19 de abr. 2016

CAPURRO, Rafael; HJORLAND, Birger. O conceito de informação. **Perspectiva em Ciência da Informação**, v.12, n.1, p.148-207, jan. / abr. 2007.
Disponível em:<http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/54/47>. Acesso em: 21 jul. 2016

CARNEIRO, Marília Vidigal. Diretrizes para uma política de indexação. **Revista da Escola de Biblioteconomia da UFMG**, Belo Horizonte, v.14, n.2, p.221-241, set. 1985.
Disponível em: <http://portaldeperiodicos.eci.ufmg.br/reb/>. Acesso em: 20 jul. 2016.

CARVALHO, Isabel Cristina Louzada. **A socialização do conhecimento no espaço das bibliotecas universitárias**. Rio de Janeiro: Interciência, 2004.

CARTILHA de Segurança para Internet: versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil (CGI.br). Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), 2012.

COMÉRCIO de livros raros ameaça a preservação de textos históricos: mercado de livros raros roubados de bibliotecas em razão de medidas de segurança ineficazes foi tema de uma conferência na Biblioteca Britânica. **Opinião & Notícia**, jul. 2015.
Disponível em:<http://opiniaoenoticia.com.br/vida/comercio-de-livros-raros-ameaca-a-preservacao-de-textos-historicos/>. Acesso em: 18 set. 2016.

CUNHA, Murilo Bastos da. Construindo o futuro: a biblioteca universitária brasileira em 2010. **Ci. Inf.**, Brasília, v. 29, n. 1, p. 71-89, jan./abr. 2000.

CUNHA, Murilo Bastos; CAVALCANTI, Cordélia Robalinho de Oliveira. **Dicionário de Biblioteconomia e Arquivologia**. Brasília, DF: Briquet de Lemos/Livros, 2008.

CUNHA, Viviane Lima da. **Tecnologias da Informação e Comunicação na socialização do conhecimento**: um estudo de caso na Biblioteca Central da Universidade Federal da Paraíba. João Pessoa, 2014. [Dissertação].

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: SENAC, 2003.

DIAS, Geneviane Duarte; SILVA, Terezinha Elizabeth da; CERVANTES, Brígida Maria Nogueira. Políticas de informação nas Bibliotecas universitárias: Um enfoque no desenvolvimento de coleções. **Rev. Digit. Bibliotecon. Cienc. inf.,** Campinas, SP, v.1, p. 39-54, jan. / abr. 2013. Disponível

em:<http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/view/572>. Acesso em: 21 abr. 2016

DUARTE, Emeide Nóbrega. Tendências temáticas do GT4 no Enancib 2011**:** rumo à gestão da inovação. **Perspectivas em Gestão & Conhecimento,** João Pessoa, v. 2, Número Especial, p. 4-11, out. 2012.

DUARTE, Zelly. (Org.) **A conservação e a restauração de documentos na era pós-custodial**. Salvador: EDUFBA, 2014. In: GATTI, Daniel Couto. Sociedade informacional e an/alfabetismo digital: relações entre comunicação, computação e internet. EDUSC/EDUFU, 2014.

ESTATÍSTICAS dos Incidentes Reportados ao CERT.br. Ano (1999 a 2015). Comitê Gestor da Internet no Brasil (CGI.br). Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Disponível em:<http://www.cert.br/>. Acesso em: 10 ago. 2016

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação**: guia prático para elaboração e implementação. ed. 2. rev. e ampl. Rio de Janeiro: Ciência Moderna, 2008.

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. 2013. 123 f. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal da Paraíba, João Pessoa, 2013.

FONSECA, Edson Nery da. **Introdução à biblioteconomia**. 2. ed. Brasília: Briquet de Lemos/Livros, 2007.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

_____. **Políticas e normas para segurança da informação**: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

FLOWERDAY, Stephen V.; TUYIKEZE, Tite. Information security policy development and implementation: The what, how and who. **Computers & Security**, v. 61, p. 169-183, 2016.

FRANCE. Ministère de l'Èducation Nationale. **Les politiques documentaires des établessement scolaires**. Rapport à monsieur le ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche. Rapporteur**:** Jean-Louis Durpaire. Raport de l'IGEN n° 2004-037, maio 2004. Disponível em:<http://www.ladocumentationfrancaise.fr/rapports-publics/044000279/index.shtml>**.** Acesso em: 26 jul. 2016.

FUJITA, Mariângela Spotti Lopes. A política de indexação para representação e recuperação da informação. In: LEIVA, Isidoro Gil; FUJITA, Mariângela Spotti Lopes. (Org.). **Política de indexação**. Marília, SP: Cultura Acadêmica, 2012.

GALVINO, Cláudio César Temóteo. **A arte de indexar artigos de periódicos**: a política de indexação da Seção de Periódicos da Biblioteca Central da UFPB. 2012. 90 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal da Paraíba, João Pessoa, 2012.

GOMES, Gláucia; NOGUEIRA, Isabel; ABRUNHOSA, J. J. **Técnicas modernas de preservação & recuperação de acervos bibliográficos.** Nova Friburgo: Êxito Brasil, 2006.

GONÇALVES, Elisa Pereira. 2. ed. **Conversa sobre iniciação à pesquisa científica**. Campinas, SP: Alínea, 2001.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2010.

GIL, Antonio de Loureiro. **Segurança empresarial e patrimonial: segurança dos negócios, plano de contingências, segurança e informática**. São Paulo: Atlas, 1995.

GROGAN, Denis. **A prática do serviço de referência**. Brasília, DF: Briquet de Lemos/Livros, 1991.

HARE, Chris. **Information security policies, procedures, and standards**: essencial code of conduct. Auerbach Publication, 2001. Disponível em*:*< www.ittoday.info/AIMS/DSM/82-10-85.pdf> Acesso em: 16 maio 2017.

HÖNE, Karin; ELOFF, JHP. Information security policy – what do international information security standards say? Elsevier Science. **Computer & Security.** v.21, n.5, Oct 2002. Disponível em:< http://www.sciencedirect.com/science/article/pii/S0167404802005047>. Acesso em: 17 maio 2017.

INFORMATION SYSTEMS AUDITAND CONTROL ASSOCIATION (ISACA). **COBIT 5 for information security**. Rolling Meadows, IL: ISACA, 2012. Disponível em: <http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf>.

_____. **COBIT 5:** Modelo Corporativo para Governança e Gestão de TI da Organização**.** Rolling Meadows, IL: ISACA, 2012.

LANCASTER, F. W. **Indexação e resumos**: teoria e prática. Brasília, DF: Briquet de Lemos/Livros, 1991.

LIMA, Gercina Angela Borém e Oliveira. Sistema de segurança eletrônico para bibliotecas. **R. Esc. Biblioteconomia UFMG**, Belo Horizonte, v.24, n.1, p. 112-128, jan.-jun., 1995. Disponível em:<http://www.brapci.ufpr.br/brapci/index.php/article/view/0000002745/5fe79adc6922b16b471f8d01b>. Acesso em: 18 set. 2016.

LIMA, Juliana Soares *et al*. Segurança da Informação em Bibliotecas Universitárias: a atuação do bibliotecário no planejamento e na implantação de novas políticas institucionais. **RDBCI: Rev. Digit. Bibliotecon. Cienc. Inf.** Campinas, SP, v.15, n.2, AOP, maio/ago. 2017.

LIVROS raros roubados do Instituto de Botânica estavam no lixo. **ESTADÃO,** 2012, São Paulo. Disponível em:<http://sao-paulo.estadao.com.br/noticias/geral, livros-raros-roubados-do-instituto-de-botanica-estavam-no-lixo,857090>.
Acesso em: 06 set. 2016.

MACIEL, Alba Costa; MENDONÇA, Marília Alvarenga Rocha. **Bibliotecas como organizações**. Rio de Janeiro: Interciência, 2006.

MANINI, Miriam Paula; GREENHALGH, Raphael Diego. A relevância da cultura organizacional na implementação de sistemas de segurança contra roubo e furto de livros raros. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 17. 2016, Salvador. **Anais**... Salvador, ANCIB, UFBA, 2016. Disponível em: <http://www.ufpb.br/evento/lti/ocs/index.php/enancib2016/enancib2016/paper/view/3637>. Acesso em: 26 jan. 2017.

MANOEL, Sergio da Silva. **Governança de segurança da informação**: como criar oportunidades para seu negócio. Rio de Janeiro: Brasport, 2014.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia do trabalho científico**: procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos. 7. ed. São Paulo: Atlas, 2013.

_____. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MEGA-ATAQUE virtual derruba sistemas de comunicação ao redor do mundo. **Nic.br**, maio, 2017. Comitê Gestor da Internet no Brasil (CGI.br). Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Disponível em: <http://www.nic.br/noticia/na-midia/mega-ataque-virtual-derruba-sistemas-de-comunicacao-ao-redor-do-mundo/>. Acesso em: 16 maio 2017.

MESQUITA, Simone. Conservação preventiva e reservas técnicas: ainda um desafio para as instituições. In: **Preservação documental**: uma mensagem para o futuro. Salvador: Edufba, 2012.

PASQUARELLI, Maria Luiza Rigo**. Procedimentos para busca e uso da informação**: capacitação do aluno de graduação. Brasília: Thesaurus, 1996.

PELTIER, Thomas R. **Information security risk analisys**. 2. ed. United States: CRC Press, Taylor & Francis Group, 2005.

PWC. **Uma defesa ultrapassada**: Principais resultados da Pesquisa Global de Segurança da Informação 2014 – The Global State of Information Security Survey 2014. PWCBrasil, 2014. Disponível em:<https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acesso em: 16 ago. 2013

RAMOS, Anderson. Conscientização em Segurança da Informação como processo. In: CARBAL, Carlos; CAPRINO, Willian (Orgs.). **Trilhas em segurança da informação**: caminhos e ideias para a proteção de dados. Rio de Janeiro: BRASPORT, 2015.

RICHARDSON, Roberto Jarry. **Pesquisa social**: métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

ROUBADOS 24 livros raros do Museu Nacional do Rio. **ESTADÃO**, 2004, São Paulo. Disponível em:< http://cultura.estadao.com.br/noticias/geral,roubados-24-livros-raros-do-museu-nacional-do-rio,20040506p7225>. Acesso em: 06 set. 2016.

RUBI, Milena Pelsinelli. Política de indexação. In: LEIVA, Isidoro Gil; FUJITA, Mariângela Spotti Lopes. (Org.). **Política de indexação**. Marília, SP: Cultura Acadêmica, 2012.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2.ed. Rio de Janeiro: Elsevier, 2014.

SETZER, Valdemar W. **Dado, informação, conhecimento e competências**. (Versão 25/05/2015). Disponível em: <https://www.ime.usp.br/~vwsetzer/dados-info-html>. Acesso em 20 fev. 2016.

SHAHRI, Ahmad Bakhtiyari. ISMAIL, Zuraini. A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. **Journal of Information Security,** 2012, 3, 169-176. <http://dx.doi.org/10.4236/jis.2012.32020 Published online april 2012>. Disponível em: <http://www.SciRP.org/journal/jis>. Acesso em: 10 mar. 2017.

SILVA, Ângela Maria Moreira. A construção das bibliotecas universitárias no Brasil. **RevIU. Revista Informação & Universidade**, v. 2, n.1, p. 3-23, 2010. Disponível em: <http://revista.ibict.br/cienciadainformacao/index.php/ciinf/article/viewArticle/159>. Acesso em: 26 fev. 2016

SILVA, Denise R. P. da; STEIN, Lílian M. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, v.10, p.43-56, mar. 2007. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410>. Acesso em: 14 jul. 2016

SILVA, Edilene Maria da; GARCIA, Joana Coeli Ribeiro. **Política de informação científica e tecnológica no Brasil:** contribuição para as bibliotecas universitárias. João Pessoa, 10 ENANCIB, 2009. Disponível em:<http://enancib.ibict.br/index.php/enancib/xenancib/paper/viewFile/3268/2394>Acesso em: 22 abr. 2016.

SILVA, Narjara Bárbara Xavier; ARAÚJO, Wagner Junqueira de; AZEVEDO, Patrícia Morais de. Engenharia social nas redes sociais *online:* um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **RICI: R.Ibero-amer. Ci. Inf.,** Brasília, v. 6, n. 2, p. 37-55, ago. / dez. 2013. Disponível em:<http://periodicos.unb.br/index.php/RICI/article/view/9222>. Acesso em: 15 ago. 2016.

SILVEIRA, Nalin Ferreira. Evolução das bibliotecas universitárias: information commons. **Revista ACB: Biblioteconomia em Santa Catarina**, Florianópolis, v.19, n.1, p. 69-76, jan. /jun., 2014.

TARGINO, Maria das Graças. Bibliotecas como preservadoras e disseminadoras da cultura local. In: _____. **Olhares e fragmentos**: cotidiano da biblioteconomia e ciência da informação. Teresina, PI: EDUFPI, 2006.

UNIVERSIDADE FEDERAL DA PARAÍBA. **Resolução 32/2014. Política de Segurança da Informação**. UFPB. 2014. Disponível em:<http://www.ufpb.br/cgti/?q=node/47>. Acesso em: 16 set. 2016.

_____. **Resolução n° 31/2009**. Aprova o regimento interno do Sistema de Bibliotecas da UFPB. Disponível em: <http://www.biblioteca.ufpb.br/Reg_Res.pdf> Acesso em 09 jun. 2013.

United Stats of America. Office of Management and Enterprise Services, Information Services. **Information Security Policy, Procedures, Guidelines**. Oklahoma, USA: Office of Management and Enterprise Services, Information Services. 2015. Discponível em:<https://www.ok.gov/cio/Policy_and_Standards/>. Acesso em: 28 maio 2017

VERGUEIRO, Valdomiro. **Desenvolvimento de coleções**. São Paulo: Polis, 1989.

_____. **Seleção de materiais de informação**: princípios e técnicas. 3. ed. Brasília: Briquet de Lemos, 2010.

VIEIRA, Valter Afonso. **Escalas em marketing**: métricas de resposta do consumidor e de desempenho empresarial. São Paulo: Atlas, 2011.

WEITZEL, Simone da Rocha. **Elaboração de uma política de desenvolvimento de coleções em bibliotecas universitárias**. Rio de Janeiro: Interciência, 2006.

WILLIAMS, Robert L. **Computer and network security in small libraries**: a guide for planning. Texas, USA: Texas State Library and Archives Commission, Austin, 2001.

YAMASHITA, Marina Mayumi; PALETTA, Fátima Aparecida Colombo. **Preservação do patrimônio documental e bibliográfico com ênfase na higienização de livros e documentos textuais**. Rio de Janeiro, v.2, n.2, p. 172-184, ago./dez. 2006. Disponível em: <www.arquivistica.net>. Acesso em: 18 abr. 2012.

APÊNDICE A – Questionário para análise da segurança da informação na Biblioteca Central da Universidade Federal da Paraíba

Este questionário, foi aplicado como levantamento de evidências por meio de análise de risco com foco na Segurança da Informação na Biblioteca Central da UFPB. A estrutura e elaboração do questionário baseia-se no método FRAAP (*Facilited Risk Analisys and Assessement Process*) e em conformidade com a ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança da Informação – Código de Prática para controles de segurança da informação.

Categoria 1 – Pessoas

1) Você possui conhecimento sobre Segurança da Informação:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

2) É importante conhecer a Política de Segurança da Informação da UFPB:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

3) Você permite a terceiros saberem sua senha de acesso:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

4) Os documentos de trabalho devem ficar à mostra na mesa de trabalho:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

5) Para senhas de acesso, deve-se criar senha fortes, de preferência com 8 caracteres, utilizando letras e números:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

6) Ao deixar a estação de trabalho deve-se bloqueá-la:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

7) Deve-se utilizar ou armazenar programas não destinados aos objetivos da sua função na Instituição:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

8) O treinamento em conscientização, educação em segurança da informação, é importante:
Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

9) O estabelecimento de Política de Segurança da Informação em Bibliotecas Universitárias é fator de extrema necessidade:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

Categoria 2 – Processos

10) A Biblioteca faz uso de crachá para identificação pessoal dos servidores:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

11) Orientações são dadas acerca da manutenção de sua senha de acesso ao Sistema de Informação e a responsabilidade implicada pelo seu mau uso:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

12) A alta administração tem ciência da necessidade que as instituições têm de um programa eficaz em Segurança da Informação:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

13) No ambiente da Biblioteca são estabelecidas políticas de segurança da informação formalizadas:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

14) Existe classificação das informações de acordo com seu grau de importância:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

15) Existem na Biblioteca Central, procedimentos para garantia da continuidade das atividades, no caso de incidentes na segurança da informação:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

16) Existe inventário dos ativos de informação (considerando seu ciclo de vida – criação, processamento, armazenamento, disseminação, desbaste e descarte):

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

17) Existem controles de entrada física para acessos a somente pessoas autorizadas:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

18) Existe a necessidade de gerenciar as mídias removíveis para prevenir que as informações armazenadas sejam divulgadas sem autorização, modificadas, removidas ou destruídas:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

19) A Biblioteca possui controles para proteção física contra desastres naturais, ataques maliciosos e acidentes:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

Categoria 3 - Tecnologia

20) A atualização do anti-vírus é feita periodicamente:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

21) O antivírus deve ser de licença paga:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

22) É necessário o controle para proteção no uso de mídias removíveis (*pen drive, memory cards*):

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

23) Deve-se estabelecer restrições para instalação de softwares:

Concordo fortemente( ) Concordo( ) Indiferente( ) Discordo( ) Discordo fortemente( )

APÊNDICE B – Minuta de Política de Segurança da Informação PSI – Biblioteca Central

Universidade Federal da Paraíba

Biblioteca Central

Minuta de Política de Segurança da Informação

João Pessoa – PB
2017

Da introdução

Esta é uma minuta para a instituição de uma Política de Segurança da Informação para Biblioteca Central, da Universidade Federal da Paraíba e estabelece as diretrizes necessárias que guiarão as normas e procedimentos na gestão desta política.

A Política de Segurança da Informação trata-se de documento formal, institucional, destinado ao estabelecimento de diretrizes e normas administrativas referentes à segurança da informação, recursos, serviços e infraestrutura tecnológica (Tecnologia da Informação – TI).

Parte dos pressupostos de que a informação processada, armazenada e disponibilizada na Biblioteca deve ser protegida adequadamente para garantir sua integridade (salvaguarda da informação e processamento), confidencialidade (acesso a somente pessoa autorizada), disponibilidade (acesso autorizado à informação sempre que necessário).

A segurança da informação e sua proteção é de responsabilidade de cada indivíduo que gerencia e/ou acessa os recursos informacionais da Biblioteca, cabendo a estes utilizar a informação da Biblioteca, de acordo com o que está estabelecido na Política de Segurança da Informação da Biblioteca Central.

Do objetivo

O objetivo desta minuta é definir diretrizes que nortearão os indivíduos à prática da Gestão da Segurança da Informação na BC/UFPB

Da abrangência

Esta minuta de política se aplica:

- Aos indivíduos que compõe o quadro interno da BC;
- Ao gerenciamento e uso da informação no ambiente organizacional tanto em formato digital como em formato analógico da Biblioteca.

Da implantação

Cabe a Biblioteca Central coordenar as áreas técnicas, de apoio e de negócios para o desenvolvimento e implantação de projetos, ações, procedimentos, instruções e normativos a fim de possibilitar operacionalização e manutenção desta política. Com Apoio da Superintendência de Tecnologia de Informação (STI) – para tecnologia, e PROGEP – para

treinamento e conscientização/responsabilização dos funcionários; bem como da Prefeitura Universitária – para manutenção e segurança física.

4. Diretrizes e regras

4. 1 O bem informação

A informação é um bem que deve ser protegido, gerenciado de forma adequada, de maneira que sua integridade, disponibilidade, confidencialidade, possam ser garantidas, independente do meio em que a informação esteja armazenada.

4.2 O Gestor da Informação

A gestão da informação implica em um conjunto de diretrizes, procedimentos, orientações e boas práticas para garantir a confidencialidade, integridade e disponibilidade das informações.

Os recursos informacionais deverão ter um Gestor que será designado pela direção formalmente.

O Gestor da Informação é responsável pela gestão e acesso aos recursos informacionais, validação de uso e definição dos demais controles sobre a informação.

4.3 Confidencialidade da informação

Deve ser garantida a confidencialidade das informações em todo seu processo de uso, baseado nos critérios estabelecidos em Norma de classificação da informação, para evitar o acesso indevido às informações confidenciais.

- Os documentos devem ser guardados em armários ou gavetas com chave;
- Gavetas e armários devem permanecer sempre trancados;
- Deve ser feito ativação de tela com bloqueio por senha;
- Atentar para eventuais situações que possam oferecer risco de extravio de informações sigilosas;
- Destruir as mídias magnéticas quando for o momento do descarte;
- O descarte de documentos em papel dever ser feito utilizando fragmentadora com corte transverso.

4.4 Integridade da informação

Deve ser garantida a salvaguarda de toda informação e seus métodos de processamento, para evitar que seja modificada, acessada e destruída indevidamente.

4.5 Disponibilidade da informação

A liberação do acesso à informação aos usuários será autorizada pelo Gestor da Informação, considerando as necessidades do usuário e sigilo da informação para efetivação dos objetivos da biblioteca.

O acesso à informação deve ser garantido ao usuário que necessite da mesma, desde que não venha a comprometer a segurança da informação na biblioteca.

O usuário deve acessar somente as informações e seus ambientes, mediante prévia autorização. A tentativa consciente de acesso aos ambientes não autorizados, será considerada falta grave.

O acesso às informações armazenadas ou processadas em ambiente tecnológico, é de responsabilidade do usuário, sendo individual e intransferível.

Os recursos tecnológicos da biblioteca disponibilizados para os usuários, destinam-se a realização das atividades profissionais.

4.6 Uso de senhas

Todos os usuários devem ser informados da sua responsabilidade pela proteção de suas senhas. Deve-se:

- Seguir as orientações quanto as práticas de uso das senhas;
- Manter confidencialidade sobre sua senha e garantir a não divulgação a quem quer que seja;
- Evitar manter anotações da senha;
- Ao menor sinal de comprometimento do sistema ou da senha, atualizar e/ou alterar a informação de autenticação;
- Criar senhas fáceis de lembrar e difíceis de serem descobertas, usando caracteres diferentes;
- Não utilizar a mesma senha secreta para uso com objetivos pessoais ou profissionais.

4.7 Gestão de ativos

Os ativos de informação e recursos de processamento da informação devem ser identificados, inventariados, classificados e definido as responsabilidades adequadas à sua proteção.

4.8 Classificação da informação

A informação deve ser classificada de acordo com seu valor, requisitos legais, criticidade e sensibilidade, para assegurar que não seja modificada ou divulgada sem autorização.

Sua classificação deve orientar-se pelos níveis de confidencialidade e seguir as orientações da legislação vigente. Para a BC sugere-se os seguintes níveis: ostensiva (informação pública), interna (informação apenas para uso e acesso da BC); e restrita (específica para um determinado setor da BC). A classificação deve considerar quais pessoas, setores organizacionais ou usuários devem ter acesso e quais procedimentos devem ser seguidos na proteção da informação.

4.9 Mesa limpa e tela limpa

Deve ser adotada uma prática de mesa limpa de documentos em papel e mídias removíveis. Deve observar as seguintes recomendações:

- Não deixar informações de fácil acesso na mesa de trabalho ou computador;
- Guardar em local seguro as informações em papel ou mídia de armazenamento eletrônica, fora do horário de expediente;
- Manter computador desligado ou protegido com bloqueio de teclado ou tela, com senhas, quando não estiver em uso;
- Remover de impressoras, os documentos contendo informação sensível ou classificada.

4.10 Gerenciamento de mídias removíveis

Deve-se implementar procedimentos para gerenciamento de mídias removíveis, em conformidade com a política de classificação das informações adotada pela biblioteca.

4.11 Educação em segurança da informação

Deve ser implantado um processo de educação e conscientização dos indivíduos internos e externos, quanto à segurança da informação, no âmbito da Biblioteca, objetivando despertar nos mesmos a percepção da importância de práticas seguras no uso das informações e Tecnologia de Informação da Instituição.

4.12 Gestão de continuidade das atividades

A Biblioteca Central deve garantir a continuidade das atividades essenciais, quando das situações de falhas ou comprometimento de serviços.

Deve ser garantida a proteção dos recursos informacionais, infraestrutura e ambientes físico de realização das atividades operacionais da biblioteca, contra indisponibilidade e deve ser instituído plano de continuidade das atividades.

O desenvolvimento e implementação das medidas preventivas e de continuação das atividades, para situações de incidentes de segurança, devem ser em caráter permanente, e abranger os aspectos pessoas, processos, tecnologia e infraestrutura. Estas iniciativas são de responsabilidade da gestão e deve contar com o apoio das Superintendências da UFPB.

4.13 Correio eletrônico

A conta de *e-mail* disponibilizada pela instituição é de responsabilidade do usuário sendo o mesmo responsável pelas mensagens enviadas. O *e-mail* institucional não deve ser usado para questões pessoais.

As mensagens devem ser de cunho profissional, não comprometer a imagem da instituição, não ser contrário à legislação vigente, bem como aos princípios éticos da instituição.

4.14 Ambiente de *Internet*

As informações acessadas, transmitidas e recebidas pela *Internet* ficam sujeitas ao conhecimento da STI. O uso da *Internet* destina-se ao desempenho das atividades profissionais.

É proibido o uso da *Internet* na realização de atividades que ponham em risco a segurança da informação da Instituição. Os acessos a este ambiente podem ser monitorados pela Biblioteca objetivando a garantia do cumprimento desta PSI.

4.15 Segurança e ética

Ao utilizarem os recursos da instituição, os usuários devem se guiar pela segurança e ética, cientes de que são valores que se completam. Situações que venham a comprometer estes valores deve ser imediatamente reportada a chefia.

4.16 Gestão de incidentes

Quando do funcionamento anormal do sistema de informação, a equipe técnica do STI dever ser imediatamente comunicada para a coibição de eventual comprometimento da segurança das informações.

4.17 Segurança de recursos humanos

Estabelecer as responsabilidades para garantir que funcionários, fornecedores e terceirizados, estejam cientes de suas responsabilidades em conformidade com a segurança da informação na biblioteca.

4.18 Segurança física e do ambiente

Desenvolver e implementar o uso de perímetros de segurança para a proteção de áreas relacionadas ao processamento da informação como as informações críticas ou sensíveis.

A proteção física e do ambiente da Biblioteca é condição precípua para que se possa evitar que ameaças ambientais, ações de pessoas não autorizadas e/ou mal-intencionadas danifiquem ou se apropriem das informações para fins ilícitos.

4.19 Controle de entrada física

Estabelecimento de proteção das áreas seguras, por controles adequados de entrada permitida, a somente de pessoal autorizado.

Restringir acesso aos setores em que são processadas ou armazenadas informações sensíveis, a apenas pessoal autorizado.

Deve ser exigido que todos os funcionários, fornecedores, partes externas e todos os visitantes, tenham alguma forma visível de identificação (Crachá).

Estabelecer proteção com a criação de uma ou mais barreiras físicas, sobretudo para as áreas de processamento ou armazenamento de informações;

Estabelecer controle de registro de hora e data de entrada e saída de visitantes, com autenticação da identidade do visitante, com permissões de acessos concedidas para finalidades específicas e autorizadas.

4.20 Gestão dos elementos tecnológicos

Desenvolver um canal de comunicação entre a BC e Superintendência de Tecnologia da Informação para garantir a manutenção e cumprimento das normas de segurança referentes aos itens de tecnologia da informação.

4.21 Cumprimento da política de segurança da informação

Assegurar que sejam documentados e executados todos os procedimentos de segurança que compete a responsabilidade da Biblioteca.

Estabelecer revisão periódica de todas as áreas, para que seja garantido o cumprimento dos procedimentos e normas de segurança.

4.22 Penalidades

As ações que venham a comprometer a implementação ou controle dessa PSI, referente à segurança da informação, implicará em penalidade, conforme os critérios da Gestão geral, apresentadas em Resolução. Quando de reincidências, caberá ao infrator responder a processo disciplinar.

ANEXO A – Aprovação do Comitê de Ética

UFPB - CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS: Proposta de uma política de segurança da informação para a Biblioteca Central da Universidade Federal da Paraíba

Pesquisador: FERNANDO ANTONIO FERREIRA DE SOUZA

Área Temática:

Versão: 1

CAAE: 58076417.5.0000.5188

Instituição Proponente: Universidade Federal da Paraíba

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 2.084.493

Apresentação do Projeto:

A pesquisa será desenvolvida pelo discente Fernando Antonio Ferreira de Souza, do MESTRADO PROFISSIONAL GESTÃO EM ORGANIZAÇÕES APRENDENTES da UFPB, sob orientação do Prof. Dr. Wagner Junqueira de Araújo.

Objetivo da Pesquisa:

Objetivo Primário:

Analisar os elementos de Gestão da Segurança da Informação que permitam a elaboração de uma minuta de Política de Segurança da Informação para a Biblioteca Central da UFPB.

Objetivo Secundário: Diagnosticar os aspectos de gestão de segurança da informação no ambiente da BC/UFPB; Mapear riscos, vulnerabilidades e ameaças à Segurança da Informação na BC/UFPB; Elaborar uma minuta de política para gestão da segurança da informação adaptada às necessidades da BC; Promover o debate sobre a minuta proposta junto aos gestores da BC.

Avaliação dos Riscos e Benefícios:

Riscos: Sem riscos, previsíveis.

Benefícios: Contribuir no desenvolvimento de melhores práticas de segurança da informação na

Endereço: UNIVERSITARIO S/N
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** eticaccsufpb@hotmail.com

UFPB - CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA

Continuação do Parecer: 2.064.403

Biblioteca Central, bem como no desenvolvimento pessoal e profissional, tendo em vista que, com a análise e avaliação dos riscos e identificação das ameaças à segurança da informação, pode-se propor soluções para a diminuição dos fatores que possam impactar nas atividades da Biblioteca.

Comentários e Considerações sobre a Pesquisa:

Pesquisa relevante, em consonância com os objetivos e metodologia

Considerações sobre os Termos de apresentação obrigatória:

Apresenta todos os termos necessários

Recomendações:

Atualizar o cronograma, lembrando que o projeto que envolve seres humanos somente poderá ser iniciado após efetiva aprovação pelo CEP.

Conclusões ou Pendências e Lista de Inadequações:

aprovado

Considerações Finais a critério do CEP:

Certifico que o Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba – CEP/CCS aprovou a execução do referido projeto de pesquisa.

Outrossim, informo que a autorização para posterior publicação fica condicionada à submissão do Relatório Final na Plataforma Brasil, via Notificação, para fins de apreciação e aprovação por este egrégio Comitê.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_879695.pdf	09/05/2017 10:23:22		Aceito
Folha de Rosto	FOLHADEROSTO.pdf	09/05/2017 10:22:30	FERNANDO ANTONIO FERREIRA DE	Aceito
Outros	AutorizaPesquisa.pdf	16/04/2017 09:59:05	FERNANDO ANTONIO FERREIRA DE	Aceito
Outros	Declar_Qualif.pdf	16/04/2017 09:55:34	FERNANDO ANTONIO FERREIRA DE	Aceito
Projeto Detalhado / Brochura	ProjetoPesquisa.pdf	16/04/2017 09:50:58	FERNANDO ANTONIO	Aceito

Endereço: UNIVERSITARIO S/N
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** eticaccsufpb@hotmail.com

UFPB - CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA

Continuação do Parecer: 2.084.488

Investigador	ProjetoPesquisa.pdf	16/04/2017 09:50:58	DE SOUZA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	Termoconsentimentolivreesclarecimento.pdf	16/04/2017 09:09:18	FERNANDO ANTONIO FERREIRA DE SOUZA	Aceito
Cronograma	Cronograma.pdf	10/03/2017 11:33:28	FERNANDO ANTONIO FERREIRA DE	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

JOAO PESSOA, 26 de Maio de 2017

Assinado por:
Eliane Marques Duarte de Sousa
(Coordenador)

Endereço: UNIVERSITARIO S/N
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** eticaccsufpb@hotmail.com