UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS
CURSO DE BIBLIOTECONOMIA

MAURO CÉLIO FRAZÃO COSTA

O BIBLIOTECÁRIO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

São Luís
2019

MAURO CÉLIO FRAZÃO COSTA

O BIBLIOTECÁRIO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada ao curso de graduação em Biblioteconomia, da Universidade Federal do Maranhão – UFMA, como requisito para obtenção do título de Bacharel.

Orientador: Profº. Roosewelt Lins Silva

São Luís

2019

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UFMA

Costa, Mauro Célio Frazão.
O bibliotecário no contexto da segurança da informação / Mauro Célio Frazão Costa. - 2019. 50 p.

Orientador(a): Roosewelt Lins Silva.
Monografia (Graduação) - Curso de Biblioteconomia, Universidade Federal do Maranhão, São Luís, 2018.

1. Bibliotecário. 2. Educação Continuada. 3. Informação. 4. Segurança da Informação. 5. Vulnerabilidades. I. Silva, Roosewelt Lins. II. Título.

MAURO CÉLIO FRAZÃO COSTA

O BIBLIOTECÁRIO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada ao curso de graduação em Biblioteconomia, da Universidade Federal do Maranhão – UFMA, como requisito para obtenção do título de Bacharel.

Aprovado em: __/__/ 2019

BANCA EXAMINADORA

_____
Profº. Drº Roosewelt Lins Silva (orientador)
Universidade Federal do Maranhão

_____
Profª. Drª Cenidalva Miranda de Sousa Teixeira
Universidade Federal do Maranhão

_____
Profª Ms. Raimunda Ramos Marinho
Universidade Federal do Maranhão

São Luís

2019

A todos os meus familiares, que sempre me apoiaram nos meus estudos.

À equipe do departamento do curso de Biblioteconomia por todo apoio e colaboração que me foi dado neste importante momento da minha vida.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus que me concedeu força, coragem e determinação para que eu pudesse superar todas as dificuldades encontradas no caminho e assim chegar a este momento. À equipe do Departamento do curso de Biblioteconomia por todo apoio e colaboração que me foi dado neste importante momento da minha vida.

Ao meu orientador Roosewelt Lins Silva, pelo suporte no pouco tempo que lhe coube, pelas suas correções e incentivos.

Agradeço aos membros da banca examinadora, pela disponibilidade de participar e pelas contribuições pessoais acerca da monografia.

A esta universidade, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.

A todos os meus familiares, que sempre me apoiaram nos meus estudos. Agradeço também aos meus poucos porem excelentíssimos amigos tanto deste como dos meus outros cursos, que de forma especial iluminaram os meus pensamentos me levando a buscar mais conhecimentos.

“Acho que vírus de computador deve contar como vida. Creio que dizem algo sobre a natureza humana que a única forma de vida que criamos até agora é puramente destrutiva. Nós criamos vida à nossa própria imagem.”

Stephen Hawking

RESUMO

O bem mais importante dentre os ativo das organizações, a informação. Objetiva fazer uma análise dos aspectos relacionados à questão da segurança da informação no sentido de verificar a forma como o bibliotecário atua frente aos desafios impostos na era da informação. Apresenta as principais noções dos conceitos relacionados à segurança da informação, a partir do entendimento do significado do conceito de dados e informação. Descreve o processo evolutivo da segurança da informação. Enfatiza que as vulnerabilidades são os principais alvos das ameaças. Apresenta as principais ameaças à segurança da informação na era tecnológica. Demonstra a relevância da educação continuada no sentido de preparar o profissional bibliotecário a vencer os desafios impostos na era da informação. Utiliza como procedimento metodológico a pesquisa bibliográfica, caracterizada como pesquisa básica, exploratória. Conclui que a segurança da informação é fator primordial na preservação dos dados, bem como na manutenção de qualidade nas relações de compartilhamento desses dados entre a organização e seus colaboradores e clientes. E, ainda que, com base na afirmação que o papel do bibliotecário é de gestão dos recursos informacionais disponíveis na biblioteca ao qual ele está vinculado, o bibliotecário deve estar afinado com as novidades tecnológicas que surgem diariamente no mercado, principalmente no que tange às tecnologias voltadas para a gestão da segurança da informação, assim vai estar habilitado para lidar com os riscos inerentes à mesma.

Palavras-chaves: Bibliotecário. Educação Continuada. Segurança da Informação.

ABSTRACT

The most important asset among organizations, information. It aims to make an analysis of the aspects related to the issue of information security in order to verify how the librarian acts in front of the challenges imposed in the information age. It presents the main notions of concepts related to information security, from the understanding of the meaning of the concept of data and information. Describes evolutionary process of information security. Emphasizes that vulnerabilities are the main targets of threats. It presents the main threats to information security in the technological era. It demonstrates the relevance of continuing education to prepare the professional librarian to meet the challenges imposed in the information age. It uses as a methodological procedure the bibliographic research, characterized as basic, exploratory research. It concludes that information security is a primary factor in the preservation of data, as well as the maintenance of quality in the relations of sharing of this data between the organization and its employees and clients. And, even if, based on the assertion that the librarian's role is to manage the information resources available in the library to which he is linked, the librarian must be attuned to the technological innovations that arise daily in the market, especially in relation to technologies aimed at the management of information security, so it will be able to deal with the risks inherent to it.

Keywords: Librarian. Continuing Education. Information security.

LISTA DE QUADROS E FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

SEED – Secretaria de Educação à Distancia

SETEC – secretaria de Educação Profissional e Tecnológica

TIC – Tecnologia da Informação e Comunicação

UEMA – Universidade Estadual do Maranhão

UFMA – Universidade Federal do Maranhão

SUMÁRIO

1 INTRODUÇÃO

Grandes volumes de informação são produzidos e compartilhados diariamente. A Internet favoreceu muito a formação desse cenário. Conforme afirma Sêmola (2014, p. 20) "era do *bigdata*, em que volumes maciços de informação são gerados, armazenados, manipulados e compartilhados o tempo todo, entre todas as entidades que possamos imaginar [...]". Porém, a mesma Internet abre portas para os incontáveis ataques virtuais que ocorrem diariamente, tendo como foco a apropriação indevida das informações tanto pelas pessoas, como, principalmente, pelas organizações. Dessa forma, não se proteger desses ataques pode gerar a perda da privacidade, bem como causar elevados prejuízos financeiros, por vezes irreversíveis.

A era atual, conhecida como sociedade contemporânea, caracterizada pelo uso massivo das tecnologias da informação e comunicação, evidencia que tanto os indivíduos como as organizações estão cada vez mais dependentes dessas tecnologias, e na mesma proporção dessa dependência está a preocupação em manter a informação em ambiente seguro, seja a informação de caráter pessoal, ou a de caráter organizacional.

Manter em segurança as informações armazenadas, como exemplo, as informações estratégicas e confidenciais, cadastros de clientes, senhas, dados pessoais e outros, representa um grande desafio para a Gestão da Segurança da Informação nas organizações, visto que tudo pode se tornar alvo de ataques. Então, essas informações devem estar seguras no sentido de garantir sua integridade.

Nesse sentido, as organizações deram à informação importância, visto que é a informação que irá auxiliá-las nos processos de tomadas de decisão, dando a ela um espaço no topo da pirâmide do planejamento organizacional. Fato esse que tornou imprescindível o desenvolvimento e adoção de políticas de segurança em qualquer que seja a organização.

O que motivou a realização deste trabalho, foi o fato de após ingressar no Curso de Biblioteconomia em 2011 da Universidade Federal do Maranhão-UFMA, paralelamente em 2012, iniciei o curso de Técnico em Informática. O curso teve a duração de dois anos e foi ofertado pela Universidade Estadual do Maranhão-UEMA, através do e-Tec.

O e-Tec diz respeito a uma rede nacional pública de ensino, que integra a Escola Técnica Aberta do Brasil Escola essa instituída pelo Decreto nº 6.301, de 12 de dezembro 2007, e tem como objetivo democratizar o acesso ao ensino técnico público, na modalidade a distância.

O programa é resultado de uma parceria entre o Ministério da Educação, por meio das Secretarias de Educação à Distância (SEED) e de Educação Profissional e Tecnológica (SETEC), as universidades e escolas técnicas estaduais e federais.

No decorrer do curso técnico na UEMANET foram ministradas vinte e cinco (25) disciplinas[1]. Dentre elas cita-se a disciplina Segurança da Informação que despertou minha atenção, pois no curso de Biblioteconomia o Bibliotecário é definido como um profissional da informação que tem basicamente a função de guardar, organizar e disseminar a informação.

Quanto à questão do problema questionou-se qual a postura do bibliotecário frente aos desafios de segurança impostos na era da informação ao desempenhar seu papel na guarda e disseminação da informação. A partir do pressuposto que o Bibliotecário ao adotar a postura de permanente atualização (educação continuada) se qualifica para vencer os desafios do dia a dia no desempenho de suas tarefas. Assim, o bibliotecário devidamente qualificado está apto para vencer os desafios da segurança da informação na medida em que eles surgem.

O objetivo geral da pesquisa é discutir os aspectos relacionados à segurança da informação no âmbito das unidades de informação e verificar de que forma o Bibliotecário atua frente a esse paradigma. E, de forma específica, os objetivos foram:

a) Identificar os conceitos relacionados à segurança da informação;
b) Descrever o processo evolutivo da segurança da informação;
c) Apresentar as ameaças à segurança da informação no contexto de Unidade de Informação;
d) Demonstrar a relevância da educação continuada no sentido de preparar o profissional bibliotecário a vencer os desafios relacionados a Segurança da Informação.

O trabalho encontra-se dividido em seis partes, e está estruturado da seguinte forma:

Na primeira fez-se esta introdução; na segunda aborda-se a metodologia; na terceira são apresentados os conceitos relacionados à segurança da Informação; na quarta parte destaca-se os ataques e ameaças à segurança da informação; na quinta fez-se um estudo do Bibliotecário no contexto da Segurança da Informação; e na sexta parte a conclusão.

---

[1] As disciplinas foram: Ambientação em Educação a Distância; Português Instrumental; Inglês Instrumental; Ética Profissional; Fundamentos de Informática; Programas Aplicativos; Arquitetura de Computadores; Lógica de Programação; Técnicas de Programação; Sistemas operacionais; Estrutura de Dados; Banco de Dados; Programador de Linguagem Comercial; Empreendedorismo; Redes de Computadores; Análise de Sistemas; Programação Orientada a Objetos; Técnicas Avançadas de Programação; Interação Humano-Computador; Programador Web; Fundamentos do Desenvolvimento WEB; Programação para WEB; Projeto e Desenvolvimento de Sistemas; Protocolos e Serviços de Rede; Saúde, Meio Ambiente e Segurança no Trabalho; Segurança da Informação; e Teste de Software.

2 METODOLOGIA

O levantamento bibliográfico realizado para fins do cumprimento dos objetivos deste estudo resultou no material que aborda os fundamentos da segurança da informação, deles foram extraídos os dados que irão subsidiar a pesquisa e suas respectivas fundamentações.

Neste estudo, vale destacar algumas considerações disponíveis na literatura quando o assunto é Metodologia do Trabalho Científico, no sentido de melhor compreender as abordagens aqui utilizadas bem como, enfatizar a importância da pesquisa bibliográfica.

Nessa expectativa, Demo (2000, p. 20), defende que a "Pesquisa é entendida tanto como procedimento de fabricação do conhecimento, quanto como procedimento de aprendizagem (princípio científico e educativo), sendo parte integrante de todo processo reconstrutivo de conhecimento".

Portanto, para desenvolver o trabalho de investigação é necessário obedecer a critérios, tendo em vista que

> A pesquisa científica é a realização de um estudo planejado, sendo o método de abordagem do problema o que caracteriza o aspecto científico da investigação. Sua finalidade é descobrir respostas para questões mediante a aplicação do método científico. A pesquisa sempre parte de um problema, de uma interrogação, uma situação para a qual o repertório de conhecimento disponível não gera resposta adequada. Para solucionar esse problema, são levantadas hipóteses que podem ser confirmadas ou refutadas pela pesquisa. Portanto, toda pesquisa se baseia em uma teoria que serve como ponto de partida para a investigação. No entanto, lembre-se de que essa é uma avenida de mão dupla: a pesquisa pode, algumas vezes, gerar insumos para o surgimento de novas teorias, que, para serem válidas, devem se apoiar em fatos observados e provados. Além disso, até mesmo a investigação surgida da necessidade de resolver problemas práticos pode levar à descoberta de princípios básicos. (PRODANOV; FREITAS, 2013, p. 43).

Ou seja, o pesquisador deve utilizar-se de métodos e técnicas indispensáveis para a coleta e tratamento de dados que resultam em uma verdade, mesmo que parcial, de um problema levantado, o que caracteriza de certa forma, a finalidade de uma pesquisa.

Em conformidade com Prodanov e Freitas, (2013, p. 43), a pesquisa se inicia "[...] a partir de interrogações formuladas em relação a pontos ou fatos que permanecem obscuros e necessitam de explicações plausíveis e respostas que venham a elucidá-las".

Para caracterizar este estudo do ponto de vista metodológico, será utilizado os seguintes parâmetros:

a) **Quanto à natureza** – trata-se de uma Pesquisa Básica, pois "[...] objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais"; (PRODANOV e FREITAS, 2013, p. 51).

b) **Quanto aos objetivos** – diz respeito a uma Pesquisa Exploratória, pois objetiva "[...] facilitar a delimitação do tema da pesquisa; orientar a fixação dos objetivos e a formulação das hipóteses ou descobrir um novo tipo de enfoque para o assunto". (PRODANOV; FREITAS, 2013, p. 51).

c) **Quanto ao procedimento técnico** – se refere a uma Pesquisa Bibliográfica, ao considerar que foi

> [...] elaborada a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet, com o objetivo de colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa. Em relação aos dados coletados na internet, devemos atentar à confiabilidade e fidelidade das fontes consultadas eletronicamente. Na pesquisa bibliográfica, é importante que o pesquisador verifique a veracidade dos dados obtidos, observando as possíveis incoerências ou contradições que as obras possam apresentar. (PRODANOV; FREITAS, 2013, p. 54).

Nesse sentido, a pesquisa se caracteriza como Pesquisa Exploratória; e quanto ao procedimento técnico como Pesquisa Bibliográfica.

3 CONCEITOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

Nesta seção propõe-se a apresentar a noção dos principais conceitos relacionados à segurança da informação, a partir do entendimento do significado do conceito de dados e informação.

Para Dantas (2011, p. 9) "Os dados compreendem a classe mais baixa da informação".

De forma mais abrangente, Vieira (2010, p. 14), apresenta a definição de dados como sendo "[...] elementos que podem ser imagens, símbolos ou registros sem muitos significados, ou seja, pode ser considerada a matéria-prima da informação, aquilo que, depois de tratado, se transformará em informação e depois em conhecimento".

Dessa forma, dado representa a menor parte da informação, que podem ser representados de variadas formas, e após processamento culminam em conhecimento.

Ao que tange o termo informação segundo registros evidenciados pela investigação da história da humanidade, a informação sempre foi parte integrante do cotidiano dos indivíduos. Sob diferentes formas, e com a utilização de técnicas diversificadas, o homem deixou registros informativos de sua vida cotidiana, seus hábitos e costumes, para o uso futuro, ou ainda, para que outras pessoas pudessem utilizá-los. O uso de variados suportes favoreceu o deslocamento desses registros de um local a outro como forma de transmitir o conhecimento. A título de exemplo, as pinturas nas paredes das cavernas, os tabletes de argila e os pergaminhos.

Na atualidade o processo de organização de dados e informação se assemelha ao utilizado no passado, no entanto a tecnologia contribuiu para o surgimento e uso de novos suportes, tendo a Internet como principal veículo de disseminação da informação no formato digital.

No entanto, de modo contraditório, a Internet também serve de veículo para inúmeros ataques nocivos que colocam em risco a integridade dessas informações. Assim, zelar pela integridade das informações tem sido a principal preocupação das organizações, que investem altos recursos financeiros no sentido de se proteger desses ataques, que poderão acarretar prejuízos incalculáveis.

No que tange à definição do conceito informação, Machado (2003, p. 15) argumenta que "[...] é uma palavra que nunca foi fácil definir, mas seu uso regular está sempre presente em nossa vida como elemento imprescindível - podemos dizer que vivemos em uma sociedade da informação".

Nessa mesma linha de raciocínio, Silva e Gomes (2015, p. 145), afirma que "[...] a complexidade, variedade de conceitos e ocorrências da informação no contexto cotidiano e

técnico-científico têm promovido uma diversidade de significados que dificultam a construção de sentidos mais consistentes".

Percebe-se em decorrência disso que o conceito informação se apresenta correlacionados a outras terminologias, segundo afirmam Silva e Gomes (2015, p. 149), são elas:

Quadro1 – Correlações do conceito informação

TERMINOLOGIA	CORRELAÇÃO
Documento	Materialidade enunciativa e crítica.
Dado	Relações de significado quantitativo (metadados) e qualitativo (conteúdos histórica e cognitivamente potenciais dos sujeitos da informação).
Mensagem	Interações sociais entre sujeitos da informação
Informação	Interação social Estrutura social Hermenêutica Apreensão, compreensão e apropriação
Comunicação	Processos humanos de descobertas e construções de mensagens e significados
Conhecimento	A informação tem base em conhecimentos prévios e tem a finalidade de construir novos conhecimentos

Fonte: adaptado de Silva e Gomes (2015, p. 149)

Assim, o significado do conceito informação, segundo o entendimento de Silva e Gomes (2015, p. 145), é que

> A informação é uma produção fenomenicamente social que tem por finalidade dinamizar a intercomunicação humana e promover exposições e descobertas para construção do conhecimento através de interações entre sujeito/autor e sujeito/usuário por meio de dados (plano físico e histórico-social dos sujeitos da informação), mensagens (no plano abstrativo) e atividades documentais (plano material), que favorecem predicativos hermenêuticos aos sujeitos da informação e resultam na apreensão e apropriação pelo sujeito/usuário efetivando um caráter de compreensão.

Em outra linguagem, ao tratar do significado do conceito de informação, Machado (2003, p. 15) defende que:

> Na linguagem comum, o conceito de informação está sempre ligado ao significado e é usado como sinônimo de mensagem, notícia, fatos e idéias [ideia] que são adquiridos e passados adiante como conhecimento. O homem procura manter-se informado sobre a vida política do país e do mundo, sobre os progressos da ciência, pelo simples prazer de saber.

De uma forma mais objetiva Moreira (2001, p.67), afirma que "a informação é um ativo digital valioso para qualquer organização, independentemente da atividade. Tudo gira

em torno da informação, ou seja, depende do quanto ela é sensível e o quanto é valiosa perante sua representação diante do negócio".

Nessa perspectiva, conforme o exposto acima, estabelecer um significado para o conceito informação não é tão simples, dado à complexidade que envolve o tema, porém, segundo afirma Fontes (2006, p. 2), "Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal e profissional", numa abordagem mais objetiva.

Dessa forma, em conformidade com os argumentos de Fontes (2006, p. 2),

> [...] a informação é um bem, tem valor para a empresa e deve ser protegida. A informação deve ser cuidada por meio de políticas e regras, da mesma maneira que os recursos financeiro e material são tratados dentro da empresa. Com isso queremos dizer que a informação é um ativo de valor. É um recurso crítico para a realização do negócio e a execução da missão da organização. Portanto, sua utilização deve ter regras e procedimentos.

Para dar suporte às organizações quanto às regras e procedimentos a serem adotadas na questão segurança da informação, foi editada a norma ABNT NBR ISO/IEC 17799, em 2005, com o propósito de "[...] prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI)".

Segundo consta na norma, acima citada,

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades [...].
>
> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. (ABNT NBR ISO/IEC 17799, 2005, p. 9).

A norma, acima mencionada, destaca a importância da informação, bem como a necessidade de sua proteção, de forma adequada, visto que com o advento da Internet as organizações estão cada vez mais conectadas e compartilhando informações, e isso de certa forma, se dar em um ambiente vulnerável às constantes ameaças.

Ao se referir à importância da informação Laureano (2012, p. 7) enfatiza que "A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias".

Para se pensar no valor que a informação assume é preciso destacar sobre o ativo cujo entendimento dado pela Ciências Contábeis é que ativo representa o conjunto de bens e direitos de uma organização. No entanto, afirma Dantas (2011, p. 21),

> [...] atualmente, um conceito mais amplo tem sido adotado para se referir ao ativo como tudo aquilo que possui valor para a empresa. Como a informação tem ocupado um papel de destaque no ambiente de negócios, e também tem adquirido um potencial de valoração para as organizações e para as pessoas, ela passou a ser considerada o seu principal ativo.

Nessa expectativa, de acordo com Sêmola (2003, p. 45),

> Ativo é todo elemento que compõe os processos que manipulam e processa a informação, tais como equipamentos, aplicações, usuários, ambientes, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

Acrescenta ainda Sêmola (2001, p.20), que "ativo é tudo que manipula direta e indiretamente uma informação, inclusive a própria informação, dentro de uma organização ou fora dela".

Para corroborar essas afirmações, Moreira (2001, p. 20) assevera que

> Ativos são todos os bens que a empresa tem de propriedade, tais como: veículos, imóveis, móveis e um dos mais valiosos, as informações. As informações precisam ser transmitidas por canais seguros, a fim de que possam conter confiabilidade e integridade em seu conteúdo (MOREIRA, 2001, p.20).

Dessa forma, sendo as informações o bem mais valioso da organização, assim como os demais ativos, necessitam serem identificadas, inventariadas e outros requisitos, conforme consta na ABNT NBR ISO/IEC 27002 (2005, p.21),

> [...] convém que a organização identifique todos os ativos e documente a importância desses ativos, convém que o inventário do ativo inclua todas as informações necessárias que permitam recuperar de um desastre, incluindo o tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças e a importância do ativo para o negócio.

Segundo essa mesma norma, existem diferentes tipos de ativos, são eles:

> **Ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócio, procedimentos de recuperação, trilas de auditoria e informações armazenadas;
> **Ativos de software**: aplicativos, sistemas, ferramentas de desenvolvimentos e utilitários;
> **Ativos físicos**: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
> **Serviços**: serviços de computação e comunicações, utilidades gerais, por exemplo, aquecimento, iluminação, eletricidade e refrigeração;
> **Pessoas e suas qualificações, habilidades e experiências**;
> **Intangíveis**, tais como a reputação e a imagem da organização; (ABNT NBR ISO/IEC 27002, 2005, p.21).

A informação pode ser classificada seguindo um nível de relevância e a quem se destina a informação, obedecendo a critérios de segurança quanto ao acesso. Sob esses aspectos Laureano (2012, p. 8), classificou a informação da seguinte forma:

> **Pública** – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
> **Interna** – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;
> **Confidencial** – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
> **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

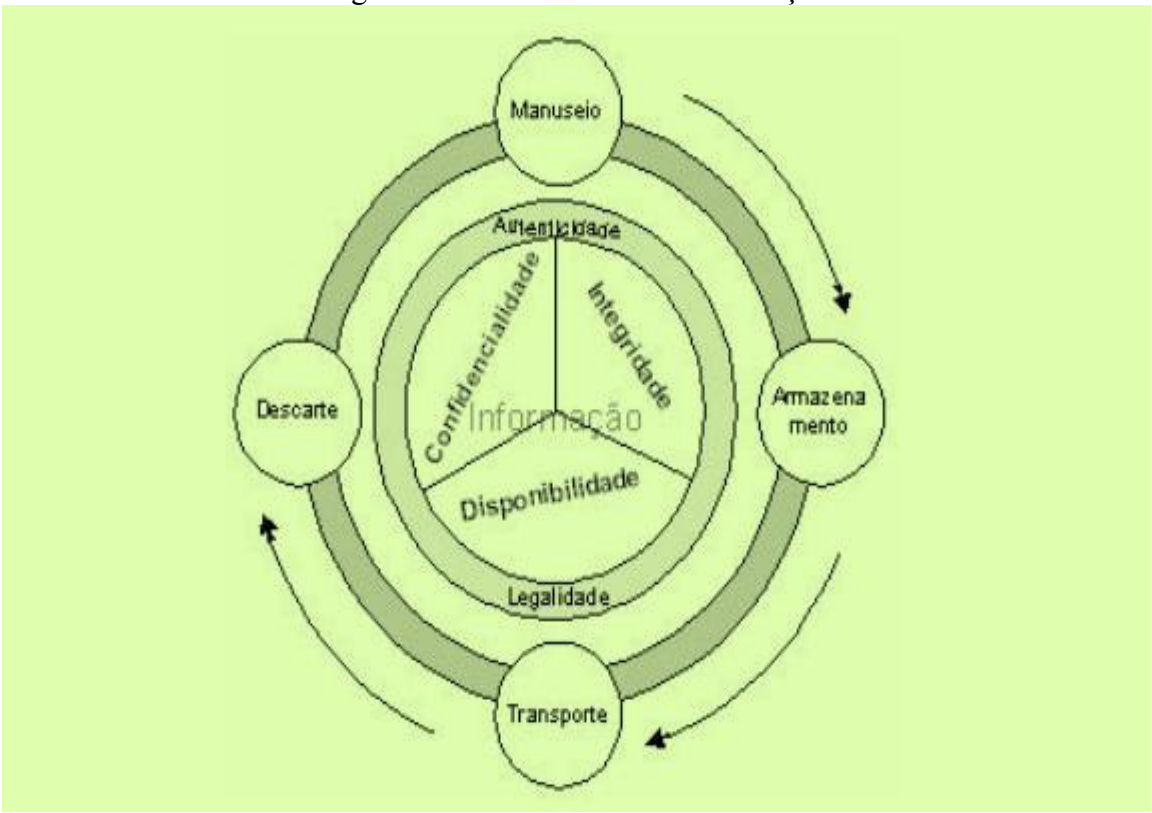
A classificação apresentada põe em evidencia que o quesito segurança é um fator preponderante, e aumenta à medida que o acesso se torna mais restrito.

A informação desde a sua criação e/ou obtenção, que pode ser tanto no meio interno como no externo à organização, passa por diversos momentos. Esses momentos representam todo o processo pelo qual passa a informação dentro da organização no que tange à sua manipulação no sentido de torná-la disponível para uso e reuso, enquanto for de utilidade para a organização no processo de tomada de decisão. Assim, com base nos apontamentos de Laureano (2012, p. 10), o ciclo de vida da informação ocorre da seguinte forma:

> **Manuseio** – Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.
> **Armazenamento** – Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo.
> **Transporte** – Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
> **Descarte** – Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CDROM usado que apresentou falha na leitura.

A figura 1 ilustra de forma clara os conceitos acima apresentados e onde cada um se manifesta no ciclo da informação:

Figura 1 – Ciclo de vida da Informação



Fonte: Laureano (2012, p. 10)

Os diversos momentos apresentados fazem parte da rotina de qualquer organização, sejam elas públicas ou privadas, no entanto não ocorrem de forma aleatória, esse ciclo é imperativo, e necessita de um planejamento para que não ocorra a perda ou descarte indevido, causando sérios prejuízos à organização. Além disso, segundo Freitas (2009, p. 11),

> A falta de planejamento do ciclo de vida da informação irá se refletir em erros na estimativa dos recursos necessários para a segurança e no armazenamento da informação, o que poderá redundar em desgaste da equipe e prejuízos tanto na aquisição dos equipamentos quanto na manutenção da informação. Esta estratégia reforça ainda mais o ciclo de melhoria continua, também conhecido como ciclo de Deming ou ciclo PDCA (Plan, Do, Check, Action).

Assim, as organizações que não incluem em suas estratégias as questões relacionadas ao ciclo de vida da informação, dentro de um processo de melhoria contínua bem planejada, no sentido de reduzir ao mínimo as falhas, expõem a riscos o seu bem mais precioso, a informação, em consequência, o fracasso é iminente. Em contrapartida, as organizações que incluem nas suas estratégias essa questão, com ênfase na segurança da informação, o efeito é contrário. Em outras palavras, Freitas (2009, p. 17), argumenta que

> Em termos estratégicos, a segurança da informação pode agregar valor ao dar maior confiabilidade ao próprio processo de transformação. A integração entre o negócio e a tecnologia empregada pode imprimir maior maturidade e solidez às transações com o cliente. A confiabilidade nas transações vai se traduzir na idéia de maior confiabilidade nos negócios.

Portanto, o planejamento do ciclo da informação, no qual deve está inserido o quesito segurança, é primordial, pois transparece “maturidade e solidez” que reflete “confiabilidade”, e se traduz em sobrevivência, ou seja, garante à organização manter-se em plena atividade em um mercado altamente competitivo.

3.1 Segurança da informação

Ao longo da história da humanidade, conforme atestado pelos diversos registros deixados pelos ancestrais do homem, como os desenhos nas paredes das cavernas, a informação sempre se fez presente sob todos os aspectos no cotidiano das pessoas. Mas foi a invenção da escrita que possibilitou que grande volume de informações geradas no passado fossem recuperadas em tempos atuais.

Segundo Planez (2015, p. 1), “A evolução da escrita se apresenta como a primeira estruturação da informação, permitindo sua reprodução de geração em geração. Antes da escrita, boa parte do conhecimento se perdia, pois esta era passada de forma verbal”.

No entanto, a forma rudimentar de reproduzir o conhecimento não era garantia de integridade, visto que, “[...] a utilização dos escribas como meio de reprodução da informação era ineficiente, além do risco ao conteúdo, inerente ao processo”. (PLANEZ, 2015, p. 1).

Ao se reportar sobre essa questão evolutiva, Sêmola (2014, p. 1), argumenta que

> Se resgatarmos a história, veremos diversas fases. Desde as revoluções industrial e elétrica, a abertura de mercado e o aumento da competitividade proporcionado pela globalização, passando pelos momentos relacionados à reengenharia de processos, à terceirização, à virtualização e, mais recentemente, aos efeitos da tecnologia da informação aplicada ao negócio de forma cada vez mais abrangente e profunda. Em todas essas etapas, a informação sempre esteve presente e cumpria importante papel para a gestão dos negócios.

Assim, da mesma forma que a evolução da humanidade é um processo contínuo, as informações geradas nesse processo exigem o desenvolvimento e emprego de novas tecnologias, no sentido de garantir a sua preservação, e principalmente, sua integridade, confidencialidade e disponibilidade, o três pilares da Segurança da Informação.

E para garantir a segurança da informação, a história registra que desde tempos remotos já eram utilizados mecanismos para dificultar o acesso a pessoas não autorizadas, como a criptografia, por exemplo. Segundo Kahn (1967, p.64- 67 apud SILVA, 2014, p. 31),

> [...] cerca de 4.000 anos atrás os egípcios deixaram marcas de elementos essenciais da criptografia, a partir de transformação da escrita comum. As inscrições do túmulo de Khnumhotep II (um arquiteto do faraó Amenemhet II) demonstram evidências da utilização de símbolos hieróglifos incomuns no lugar outros comuns. Mais tarde, cerca de 1.500 A.C., os mesopotâmicos registraram o uso da criptografia numa fórmula para fazer esmaltes para cerâmica. A partir do uso de símbolos especiais com significados diversos. Nesta época, os assírios usaram intáglios, peças planas de pedra com símbolos entalhados para a sua identificação.

Diversos métodos rudimentares para criar códigos foram desenvolvidos ao longo dos anos. No entanto, "[...] Esses métodos foram eficientes até o final do século XIX e início do século XX. Tornaram-se obsoletos devido ao surgimento de máquinas com princípios mecânicos e elétricos". (SILVA, 2014, p. 32).

Um marco do século XX que revolucionou no setor da segurança da informação foi "A chegada dos minicomputadores e posteriormente dos microcomputadores marcado no final dos anos 1970". (SILVA, 2014, p. 33).

Fato esse que favoreceu o crescimento de outro setor, o de desenvolvimento de *softwares.* Porém, argumenta Saltzer e Schroeder (1975 apud SILVA, 2014, p. 33),

> O desenvolvimento de novos softwares foi acompanhado pela chegada dos primeiros vírus de computadores, que no início representava apenas um 'troféu' para os programadores, uma demonstração de capacidade de invadir outro ambiente, mas logo passou a chamar a atenção, devido aos primeiros casos de vazamento de informação e prejuízo financeiro.
> Diante disso, a criptografia em formato digital passou a ganhar mais importância. Assim, em 1975, com a apresentação da cifra DES (Data Encryption Standard) definiu-se nos EUA o início de uma nova fase para a criptografia.

Segundo Silva (2014, p. 35) "Até os anos 1980 as agências militares eram os principais patrocinadores das pesquisas que movimentavam essa indústria. Entretanto com a proliferação do uso dos computadores no setor comercial, as diferenças de escopo tornaram-se evidentes em relação aos objetivos militares".

Com a popularização da Internet nos anos 1990,

> [...] a segurança da informação iniciou um importante processo de transformação. A internet levou a criação do comercio eletrônico, aumentou de forma significativa a velocidade com que a informação é transmitida e consequentemente a complexidade dos objetivos de TI em relação à década anterior. (SILVA, 2014, p. 36).

No entanto, foi com os últimos acontecimentos do nosso século, que a segurança da informação passou a ser uma preocupação de primeira instancia. Dentre esses acontecimentos podemos citar:

a) O ataque de 11 de setembro de 2001 às torres gêmeas do World Trade Center, nos Estados Unidos;
b) A *tsunami* em 2004 na Indonésia; dentre outros acontecimentos.

A consequência desses fatos forma, entre outras, é que ocorreu uma grande perda de informações, conforme assevera Dantas (2011, p. 5), ao dizer que

> Esses exemplos levantam uma questão peculiar: a proteção das informações. Em ambos os acontecimentos (ataques terroristas e tsunami), muitas informações foram destruídas e com elas muitos negócios. As empresas que foram atingidas por esses fatos puderam continuar com suas atividades de negócios? As empresas que retornaram às suas atividades possuíam um plano de recuperação de desastres? Quantas pessoas morreram em consequência de equipamentos e sistemas que deixaram de funcionar?

A forma como era tratada a segurança da informação mudou sensivelmente depois desses acontecimentos, segundo os argumentos de Dantas (2011, p. 6), quando afirma que

> É um fato que a evolução da tecnologia mudou a forma dos negócios. Hoje, a nova estrutura dos negócios corporativos é a tecnologia da informação, o seu sistema nervoso é a informação, e o seu ambiente, alcança, também, o ciberespaço. O mundo virtual e a sua capacidade de processamento tornaram a vida melhor ao facilitarem muitas coisas, e trouxeram consigo não só benefícios mas também ameaças à segurança da informação.

Assim, na atualidade, com o grande volume de informações que transitam diariamente através da Internet, desperta o interesse de pessoas não autorizadas a se apossar dessas informações de forma ilícitas. Milhares de ataques são registrados diariamente, muitas vezes bem sucedidos, causando sérios prejuízos financeiros às organizações, muitas vezes irreversíveis.

As notícias veiculadas pela mídia apontam a dificuldade enfrentada pelas organizações em manter as informações seguras, livres dos sucessivos ataques que ocorrem diariamente no mundo cibernético. Além disso, questões de estrutura físicas, intempéries e sinistros faz com que as organizações tenham um cuidado especial quando o assunto é segurança da informação, tendo em vista que o menor descuido pode acarretar em altos prejuízos, muitas vezes irreversíveis. Em outras palavras,

> As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. (ABNT NBR ISO/IEC 17799, 2005, p. 9).

Com ênfase a norma considera que

> A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado. (ABNT NBR ISO/IEC 17799, 2005, p. 9).

Nesse sentido, segundo Fontes (2006, p. 3) "Proteger a informação é responsabilidade de cada pessoa na organização, independentemente de seu nível hierárquico! Do mais alto executivo ao mais novo estagiário". Ou seja, a segurança da informação trata-se de um recurso que envolve a organização como um todo, onde atuam todos os elementos que fazem parte da comunicação: os processos, as tecnologias e as pessoas, conforme já dito anteriormente.

Nesse aspecto, é indiscutível o tratamento dado pelas organizações quando o assunto é segurança da informação. As organizações estão cada vez empenhadas em planejar e implementar ações que garantem a segurança dos seus ativos. Ou seja,

> [...] é crescente a conscientização das organizações frente ao valor e às vulnerabilidades de seus ativos no que diz respeito à segurança. Hoje em dia, a segurança da informação é determinante para assegurar competividades, lucratividade, atendimento aos requisitos legais e a imagem da organização junto ao mercado, às organizações, tanto no setor público quanto no setor privado. (COELHO; ARAÚJO; BEZERRA, 2014, p. 26).

Dito isto, Segurança da Informação se refere à "[...] proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". (ABNT NBR ISO/IEC 17799, 2005, p. 9).

Ao planejar as diretrizes que irão orientar a implementação de uma política de segurança da informação, em qualquer organização, é indispensável a observância de no mínimo 3 princípios básicos. Esses princípios também chamados de serviços, segundo afirma Coelho; Araújo; Bezerra (2014, p. 26), deverão estar em conformidade com o "[...] padrão ISO 7498-2, que compreende os aspectos relacionados à segurança no modelo Open Systems Interconection (OSI), os serviços de segurança são medidas preventivas escolhidas para combater ameaças identificadas".

Também, acrescentam Coelho; Araújo; Bezerra (2014, p. 26),

> Os serviços e mecanismos de segurança devem ser aplicados de modo a atender aos requisitos de segurança da organização, levando em consideração o equilíbrio entre as necessidades de segurança e custos respectivos. Em especial, ao identificar e priorizar serviços de segurança, é essencial fazer uma análise dos riscos e impacto prováveis que compreendem toda a organização em questão.

Dessa forma, esses princípios ou serviços de segurança básicos são:

a) **Confidencialidade:** diz respeito à autorização dada pelo proprietário da informação a entidades legitimas. Ou seja, somente tem acesso à informação a entidade devidamente autorizada. Qualquer tentativa de acesso por entidade não autorizada será considerada violação. Ou ainda, segundo o entendimento de Coelho; Araújo; Bezerra (2014, p. 26),

   > A confidencialidade compreende a proteção de dados transmitidos contra ataques passivos, isto é, contra acessos não autorizados, envolvendo medidas como: controle de acesso e criptografia. A perda de confidencialidade ocorre quando há uma quebra de sigilo de uma determinada informação (exemplo: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

b) **Integridade**: é a garantia que a informação deve se manter inalterada em suas características na forma em que foi criada, ou seja, sem adulteração das suas

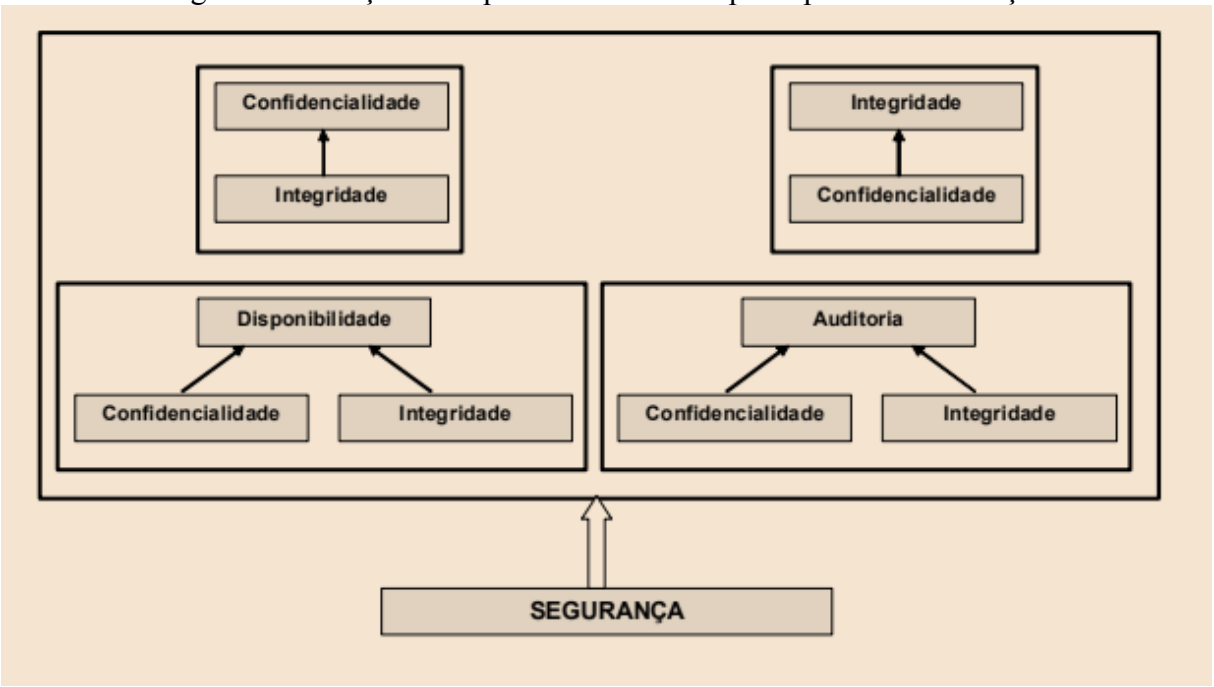
características originais, ao ser manipulada. Ou quando ocorrer mudanças, que seja controlada de modo a garantir o processo natural do ciclo de vida da informação. Ou seja, "A perda da integridade surge no momento em que uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário da informação". (COELHO; ARAÚJO; BEZERRA, 2014, p. 26).

c) **Disponibilidade**: é o princípio que garante o uso legítimo da informação por usuários autorizados por seu proprietário. Ou ainda,

> Determina que recursos estejam disponíveis para acesso por entidades autorizadas, sempre que solicitados, representando a proteção contra perdas ou degradações. A perda de disponibilidade acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de um servidor ou uma aplicação crítica de negócio que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada por pessoas com ou sem má intenção. (COELHO; ARAÚJO; BEZERRA, 2014, p. 27).

Esses princípios tem uma relação de dependência entre si, ilustrada conforme a figura 2. A ponta da seta indica a dependência de uma propriedade em relação a outra, por exemplo, a **disponibilidade** é dependente da **confidencialidade** e **integridade**, e assim sucessivamente.

Figura 2 – Relação de dependência entre os princípios da informação



Fonte: Laureano (2012, p.13)

Essas três propriedades consideradas básicas, são os atributos de segurança que figuram em qualquer que seja o sistema de informação. No entanto, as recorrentes mudanças que ocorrem nas transações comerciais de forma globalizada, principalmente por meio eletrônico, tendo a Internet como facilitadora dessas transações, necessariamente foram

acrescentadas novas propriedades àquelas, Segundo Laureano (2012, p. 12), essas novas propriedades são:

> **Autenticidade** – Garante que a informação ou o usuário da mesma é autêntico; Atesta com exatidão, a origem do dado ou informação;
> **Não repúdio** – Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;
> **Legalidade** – Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
> **Privacidade** – Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade da informação); É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.
> **Auditoria** – Rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em software significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

Assim, essas propriedades incrementam o quesito segurança em se tratando de manipulação da informação por pessoas no âmbito das organizações, de forma a garantir sua legitimidade.

A definição do conceito de ameaça, segundo Beal (2008, p.14), pode ser entendido como sendo "a expectativa de acontecimentos acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação".

Essa ameaça pode se concretizar por meio do ataque que segundo Beal (2008, p.14), trata-se de um "evento decorrente da exploração de uma vulnerabilidade por uma ameaça".

Enquanto que a vulnerabilidade, conforme Laureano (2012, p. 17) diz respeito ao "[...] ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc". Esses três aspectos da Segurança da Informação serão abordados no capítulo 4 com maior ênfase.

3.2 Sistemas de informação

Na atualidade é quase impossível conceber uma organização que não utiliza equipamentos tecnológicos no gerenciamento das informações imprescindíveis para a gestão e continuidade do negócio. Esse gerenciamento é facilitado através dos sistemas de informação que segundo Laureano (2012, p. 5),

> Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o

> controle de uma organização. Além de dar suporte à tomada de decisões, à coordenação e ao controle, esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos.

Nessa mesma linha de raciocínio, Stair e Reynolds (2016, p.9) afirmam que

> [...] sistema de informação (SI) é um conjunto de elementos ou componentes inter-relacionados que coleta (entrada), manipula (processo), armazena e dissemina dados (saída) e informações, e fornece reação corretiva (mecanismo de realimentação) para alcançar um objetivo. O mecanismo de realimentação é o componente que auxilia as organizações a alcançar seus objetivos, como aumentar os lucros ou melhorar os serviços ao cliente.

E ainda, por serem uma parte sensível da organização, os sistemas de informação necessitam de proteção contra os constantes aos quais eles estão sujeitos, necessitando, dessa forma, de uma política de segurança da informação, que diz respeito 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. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. (BRASIL, 2012, p.10).

A política de segurança da informação é elaborada, geralmente, por profissionais da área de TI capacitados. No entanto, ela deve ser de fácil acesso, de modo a ser compreendida por todos os colaboradores da organização, ou ainda,

> 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 softwares. (BRASIL, 2012, p.12).

Assim, os sistemas de informação presentes em toda e qualquer organização, em conformidade com os conceitos apresentados, são indispensáveis para que um ou mais objetivos sejam alçados de modo a garantir a sobrevivência da organização.

3.3 Ataques e ameaças

O uso das Tecnologias da Informação e Comunicação por parte das organizações, na atualidade, é imprescindível para automatizar os serviços e agilizar os processos, como forma de atingir um grau maior de eficiência e eficácia. Nesse processo, independente do tamanho e das atividades que desempenham, as organizações, "[...] (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversações e apresentações)". (NBR ISO/IEC 27002:2013, p. 4).

No entanto, essa mesma tecnologia torna vulneráveis os sistemas de informação e comunicação das organizações a ataques e ameaças, principalmente quando as informações são compartilhadas via Internet. Compartilha esse entendimento, Dantas (2011, p. 6) ao afirmar que

> É um fato que a evolução da tecnologia mudou a forma dos negócios. Hoje, a nova estrutura dos negócios corporativos é a tecnologia da informação, o seu sistema nervoso é a informação, e o seu ambiente, alcança, também, o ciberespaço. O mundo virtual e a sua capacidade de processamento tornaram a vida melhor ao facilitarem muitas coisas, e trouxeram consigo não só benefícios, mas também ameaças à segurança da informação.

Nesse sentido, a preocupação das organizações em manter em segurança seus ativos é uma constante, em especial quando esse ativo é a informação, tendo em vista a sua vulnerabilidade às ameaças tanto de forma proposital como por um descuido ou falta de atenção. E ainda, pelo fato que

> A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2003, p. 18).

Em se tratando de vulnerabilidade, para Laureano (2012, p. 17), vulnerabilidade pode ser definida como sendo "[...] o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc.".

Segunda Dantas (2011, p. 24) "[...] vulnerabilidades são fragilidades que podem provocar danos decorrentes da utilização de dados em qualquer fase do ciclo de vida das informações".

Reforça esse argumento Dantas (2011, p. 24) quando afirma que

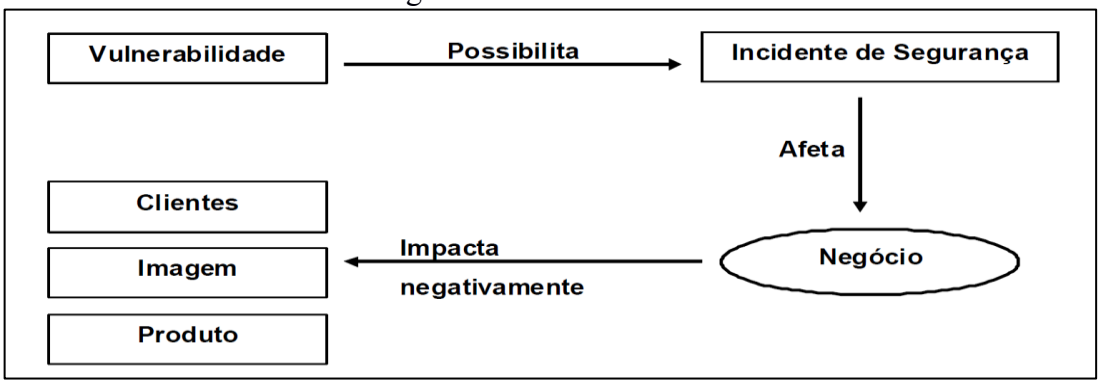
> [...] as vulnerabilidades estão relacionadas diretamente com as fragilidades. Essas fragilidades podem estar nos processos, políticas, equipamentos e nos recursos humanos. Por si só, elas não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou de condição favorável, já que se trata de ameaças.

As vulnerabilidades podem ter várias origens. Segundo Dantas (2011, p. 25) as vulnerabilidades podem ser classificadas quanto à sua origem como:

> **Naturais -** As vulnerabilidades naturais estão relacionadas com as condições da natureza ou do meio ambiente que podem colocar em risco as informações.
> **Organizacional** - As vulnerabilidades de origem organizacional dizem respeito a políticas, planos e procedimentos, e a tudo mais que possa constituir a infraestrutura de controles da organização e que não seja enquadrado em outras classificações.
> **Física -** As vulnerabilidades físicas dizem respeito aos ambientes em que estão sendo processadas ou gerenciadas as informações.
> *Hardware* **-** Caracterizam-se como vulnerabilidade de *hardware* os possíveis defeitos de fabricação ou configuração dos equipamentos que podem permitir o ataque ou a alteração dos mesmos.
> *Software* **-** As vulnerabilidades de *software* são constituídas por todos os aplicativos que possuem pontos fracos que permitem acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede.
> **Meios de armazenamento -** Os meios de armazenamento são todos os suportes físicos ou magnéticos utilizados para armazenar as informações.
> **Humanas -** As vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior vulnerabilidade.
> Sua origem pode ser: falta de capacitação específica para a execução das atividades inerentes às funções de cada um; falta de consciência de segurança diante das atividades de rotina; erros; omissões; descontentamento; desleixo na elaboração e segredo de senhas no ambiente de trabalho; não utilização de criptografia na comunicação de informações de elevada criticidade, quando possuídas na empresa.
> **Comunicação -** Nas comunicações, as vulnerabilidades incluem todos os pontos fracos que abrangem o tráfego das informações, por qualquer meio (cabo, satélite, fibra óptica, ondas de rádio, telefone, internet, *wap*, fax, etc.).

Pelo exposto, infere-se que a vulnerabilidade representa os pontos fracos de um sistema de informação e comunicação, tanto na dimensão material, como na dimensão lógica e humana. E ainda, que são esses pontos fracos que fortalecem as ameaças. Conforme esquematizado na Figura 3.

Figura 3 - Vulnerabilidade



Fonte: Laureano (2012, p. 18)

As ameaças que são causadas por agentes, de forma acidental ou proposital, sendo que esses agentes podem ser um fenômeno natural, um indivíduo ou programa de computador. Uma enchente, um incêndio não criminoso, uma falha no equipamento, um erro na

programação de um sistema, podem ser caracterizados como ameaças causadas de forma acidental.

Enquanto que as ameaças propositais podem ser exemplificadas pelas invasões de sistema por pessoas não autorizadas, fraudes nas informações e roubos. E ainda, as ameaças propositais são classificadas, segundo Dias (2000, p.57) como: "a) **ativas** - envolvem alteração de dados; b) **passivas - e**nvolvem invasão e/ou monitoramento, mas sem alteração de informações".

Sob outro aspecto, do ponto de vista intencional, Sêmola (2003, p. 47), classifica as ameaças da seguinte forma:

> **Naturais** – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.
> **Involuntárias** – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causados 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.

Dessa forma o espaço cibernético é o mais utilizado para a exploração das vulnerabilidades através da Ameaça Inteligente, fato esse que obriga as organizações a investir em constantes melhorias em seus sistemas de informações, no sentido de detectar os possíveis pontos fracos no sistema, porta de entrada dos códigos maliciosos.

Os códigos maliciosos que merecem uma atenção especial são os denominados *malware.* Segundo Dantas (2011, p. 37) os principais códigos maliciosos são:

> O **Vírus** é um programa ou parte de um programa de computador, o qual se propaga por meio de cópias de si mesmo, infectando outros programas e arquivos de computador. O vírus depende da execução do programa ou do hospedeiro para ser ativado.
> O **Cavalo de Tróia** (*trojan horse*) é um programa que executa funções maliciosas sem o conhecimento do usuário. Normalmente esse código é recebido como um presente (cartão virtual, prêmios, fotos, protetor de tela, etc.). O seu nome tem origem na mitologia grega.
> O **Adware** (*Advertising software*) é um tipo de *software* projetado para apresentar propagandas, seja por meio de um navegador (*browser*), seja com algum outro programa instalado em um computador.
> O **Spyware** é um *software* espião que tem como objetivo monitorar atividades de um sistema e enviar as informações coletadas para terceiros.
> Os **Backdoors** são programas que procuram dar a garantia de retorno a um computador comprometido, sem utilizar novas técnicas de invasão, ou retornarem ao computador comprometido sem serem notados.
> Os **Keyloggers** são programas capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.
> O **Worm** é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Difere do vírus por não embutir cópias de si mesmo em outros programas ou arquivos.
> O **Bot** é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. Normalmente, o *bot* se conecta a um servidor de IRC (Internet Relay Chat) e entra em um canal (sala) determinado, aguardando as instruções do invasor, monitorando as mensagens que estão sendo enviadas para esse canal. O invasor, ao

> se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por sequências especiais de caracteres, que são interpretadas pelo *bot*. Tais sequências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.
> Os **Botnets** são as redes formadas por computadores infectados com *bots*. Essas redes podem ser compostas por centenas ou milhares de computadores. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo: para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*; para desferir ataques de negação de serviço, etc.
> O **Rootkits** é um conjunto de programas que utiliza mecanismos para esconder e assegurar a presença do invasor no computador comprometido.

Os códigos citados acima são na realidade uma amostra da grande quantidade das ameaças. Diariamente os sistemas de informações das empresas, e até os computadores pessoais, são bombardeados por esses códigos maliciosos, tendo como consequência um grande investimento de recursos financeiros para a atualização dos equipamentos e treinamento de pessoal. Tendo em vista que na mesma proporção que as organizações investem no combate a esses códigos maliciosos os programadores desses códigos investem na sua criação.

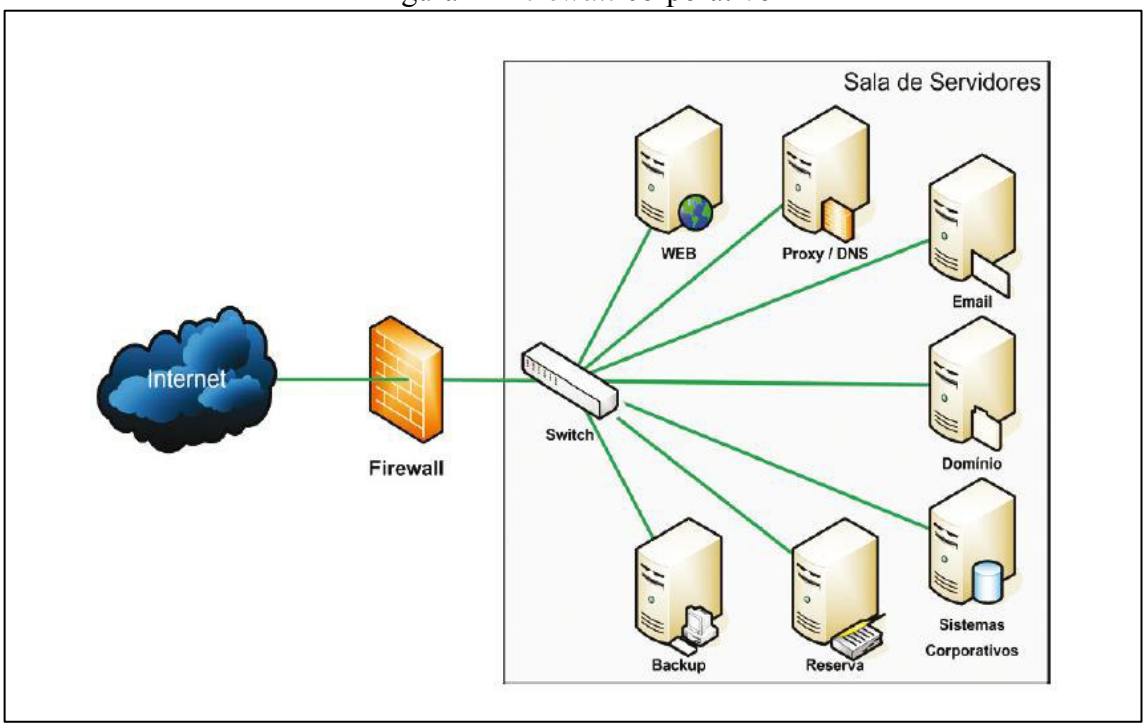
As principais ferramentas utilizadas para o combate dessas ameaças são: os *firewalls* que detectam uma possível intrusão no sistema por pessoas não autorizadas; os antivírus; e, principalmente, uma bem elaborada política de segurança da informação, onde deve abarcar todas as diretrizes necessárias para garantir que a informação permaneça em ambiente seguro.

Os *firewalls* podem ser classificados, conforme o entendimento de Novo (2010, p. 95), em:

> **a) *firewall* pessoal**: é aquele desenvolvido com o intuito de proteger o tráfego de dados entre um computador pessoal e a internet. Em geral, oferece poucas opções de configuração, podendo ser gratuito ou pago;
> **b) *firewall* corporativo**: é aquele desenvolvido com o intuito de proteger o tráfego de dados entre uma rede de dados empresarial e a internet. Oferece muitas opções de configuração, necessitando de profissionais qualificados para operá-lo. Pode ser *software* livre ou *software* comercial proprietário.
> **c) *firewall* em *software***: são programas de computador que executam atividades comuns a *firewalls*. Podem ser instalados na máquina do usuário ou na borda externa de uma rede de dados. Têm a desvantagem de consumir recursos de processamento e memória do computador onde está instalado;
> **d) *firewall* em *hardware***: são equipamentos dedicados a executar atividades comuns a *firewalls*. Podem ser instalados na máquina do usuário ou na borda externa de uma rede de dados. Têm desempenho superior, porém são mais caros que as soluções em *software*, além de necessitar de alimentação elétrica.

Destaca-se aqui os *firewalls* corporativos, que exige para o sua plena eficácia de profissionais altamente qualificados, tendo em vista que a informação é disponibilizada em rede, sendo uma área bastante suscetível de ataques, por apresentar alto grau de vulnerabilidades. A Figura 4 ilustra a estrutura de um *firewall* corporativo:

Figura 4 - F*irewall* corporativo



Fonte: Novo (2010, p. 95)

Assim, diante dessa acirrada batalha pela apropriação da informação a qualquer custo, nenhuma organização na atualidade está isenta de sofrer ataques aos seus sistemas de informação diariamente, sendo em alguns casos causando danos irreparáveis.

Os danos causados quando é rompida a barreira de proteção de um sistema de informação se referem a, segundo Novo (2010, p. 41), "[...] quaisquer prejuízos sofridos pela informação ou por seus detentores, podendo ser de três tipos":

> **Danos lógicos**. Os danos lógicos são aqueles que comprometem apenas as informações armazenadas em um meio físico. As informações podem ser comprometidas de três maneiras.
> 1 Exclusão total A informação armazenada é completamente excluída do meio físico.
> 2 Exclusão parcial Apenas uma parte da informação armazenada é excluída do meio físico, por causa de falhas na gravação.
> 3 Substituição A informação antiga é substituída por outra mais nova, em geral incorreta ou imprecisa.
> **Danos físicos**. Os danos físicos são aqueles que comprometem o meio físico onde a informação está armazenada. Em boa parte dos casos de danos físicos, a informação também fica comprometida.
> São exemplos de danos físicos a queima de componentes de discos rígidos por causa da sobre tensão elétrica, CDs e DVDs riscados como consequência da má conservação, documentos em papel descartados por engano, entre outros.
> **Danos pessoais**. Os danos pessoais são aqueles que comprometem o dono da informação ou o seu patrimônio. Em geral, ocorrem após o furto, roubo, perda, corrupção ou uso indevido dessas informações.

Desses três danos o que apresenta maior incidência é o dano lógico, tendo em vista que quase a totalidade das organizações utilizam recursos eletrônicos para armazenar suas

informações, dessa forma esses recursos apresentam um grau de vulnerabilidade acima do normal, sendo alvo de sucessivos ataques.

A evolução da tecnologia traz em seu bojo um lado meio obscuro. A tecnologia favorece a criatividade humana, porém, muitas vezes esse criatividade é usada para realização de tarefas pouco ortodoxas. A cada dia são lançados na rede mundial de computadores programas cada vez mais sofisticados que objetivam burlar sistemas de informações das corporações e/ou pessoais.

Compartilha esse entendimento, Oliveira (2001, p. 7) ao afirmar que:

> O nível de sofisticação destes ataques varia amplamente; enquanto geralmente se acredita que a maioria das invasões tem sucesso devido a códigos secretos fracos, há ainda um número grande de intrusões que usam técnicas mais avançadas para invadir. Pouco se sabe sobre a maioria das técnicas de invasão, porque elas podem ser de diversa natureza e então tornam-se muito mais difíceis de descobrir.

Grande parte dos ataques que ocorrem contra os sistemas de informação tem como principal objetivo tornar uma informação indisponível, dentre outros. O entendimento de Lyra (2015, p. 15) sobre esse quesito é que:

> Ataques podem ter como foco diferentes princípios da segurança. Um exemplo seria a invasão de uma rede corporativa por um hacker a deixando inoperante. Tal resultado está diretamente ligado ao princípio da disponibilidade, visto que, a informação requerida pelo usuário provavelmente não poderá ser acessada (não estará disponível). Em complementação a essa situação hipotética, suponhamos que o mesmo invasor, além de tornar a rede inoperante, tenha adulterado um arquivo, logo, além da quebra da disponibilidade, este acaba de praticar a quebra de integridade.

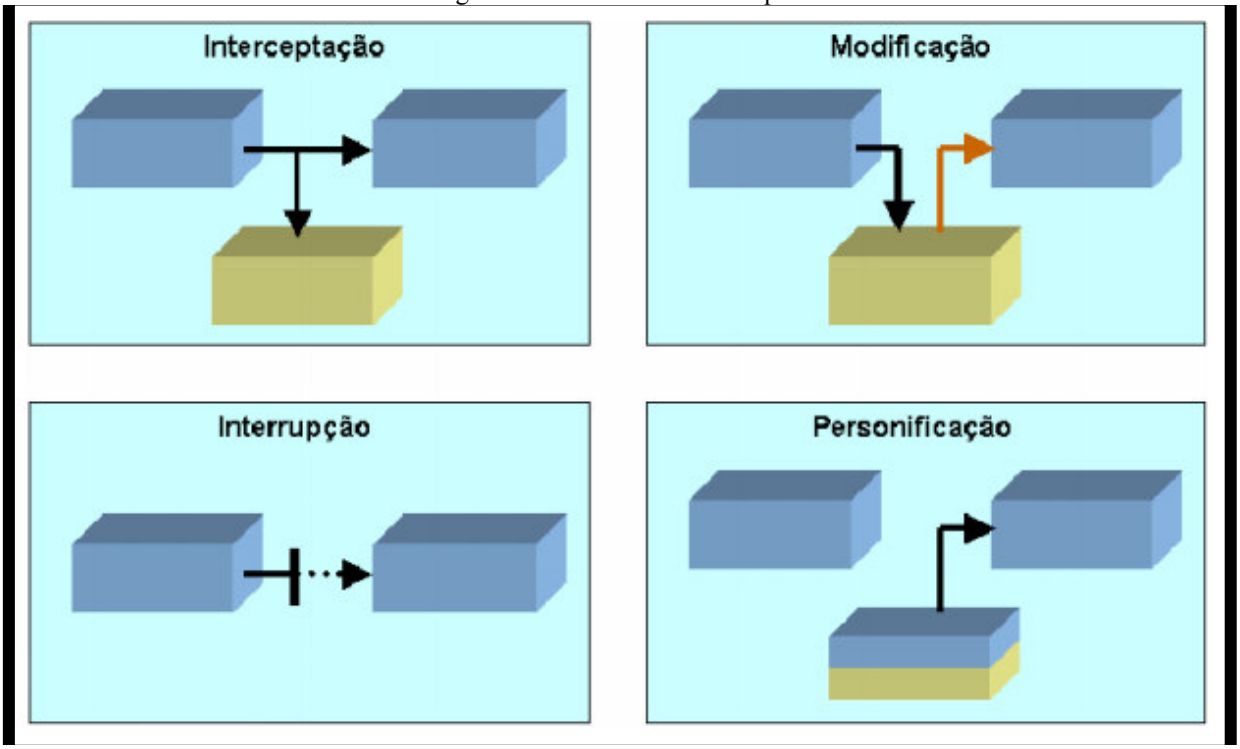
Assim, a grande preocupação da segurança da informação está em não permitir que acessos não autorizados violem seus princípios, através da utilização de mecanismos e/ou ferramentas que inibem esses ataques.

Os acessos não autorizados podem ser de quatro formas ou modalidades, conforme elenca Laureano (2012, p. 15)

> **Interceptação**: considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).
> **Interrupção**: pode ser definida como a interrupção do fluxo normal das mensagens ao destino.
> **Modificação**: consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.
> **Personificação**: considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.

Dessa forma, essa classificação corrobora a afirmação de que os ataques tem como foco os princípios de segurança. A Figura 5 esquematiza as diferentes modalidades de ataques e suas interferências nos princípios de segurança da informação.

Figura 5 – Modalidades de ataques



Fonte: Laureano (2012, p. 17)

Os incidentes de segurança que ocorrem podem ser prevenidos através de medidas de segurança implementadas no sentido de proteger a informação de possíveis riscos de ataques e/ou a exploração das vulnerabilidades pelas ameaças.

Conforme Moreira (2001, p.31), "[...] medidas de segurança são esforços como procedimentos, software, configurações, *hardware* e técnicas empregadas para atenuar as vulnerabilidades com o intuito de reduzir a probabilidade de ocorrência da ação de ameaças".

A implementação dessas medidas é de grande importância, visto que o risco de ataque é controlado, além disso, limitam seus impactos, segundo o entendimento de Sêmola (2003, p. 49). Para ele as medidas de segurança podem ser caracterizadas como:

> Preventivas: medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança na instituição. Como exemplos podemos citar as políticas de segurança, instruções e procedimentos de trabalho, especificação de segurança, campanhas e palestras da política de segurança (*firewall*, antivírus, configurações adequadas de roteadores e dos sistemas operacionais etc.);
> Detectáveis: medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. Alguns exemplos são: 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 as mesmas se adaptem 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 (SÊMOLA, 2003, p. 49).

Ao se reportar sobre essa questão Moreira (2001, p.22), alerta sobre a importância da implementação de medidas de segurança eficientes, com as seguintes palavras:

> [...] todos os ambientes são vulneráveis, partindo do pressuposto de que não existem ambientes totalmente seguros. Muitas vezes, as medidas de segurança implementadas pelas empresas possuem vulnerabilidades. Nesse caso, a ineficiência de medidas de proteção, em função de configurações inadequadas é uma das causas.

Dessa forma, para manter as informações em ambiente seguro, a adoção de medidas preventivas, ou de proteção deve ser prioridade em qualquer instituição.

Para manter a informação segura no âmbito organizacional, o "ponto de partida" é a elaboração de documento com diretrizes que contemplam os princípios da informação no que tange a manipulação na sua totalidade, envolvendo não apenas o uso dos equipamentos, mas também todo pessoal envolvido no processo.

Dantas (2011, p. 131) ao se reportar sobre a política da informação argumenta que:

> [...] a política é a materialização da intenção do que desejamos fazer, e essa intenção é transformada em princípios, valores, compromissos, requisitos, objetivos e orientações sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.
> Nesse sentido, pode-se definir a política de segurança da informação como: um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades para com a segurança da informação.
> A sua forma, escopo e detalhes estão diretamente relacionados com as atividades de negócios e decisão da organização do nível e padrão de segurança que se pretende alcançar.

Para Ferreira e Araújo (2008, p.36), "[...] a política de segurança é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade".

Assim, a política de segurança da informação envolve a organização como um todo e onde é exposta a filosofia da organização para esse quesito, sendo necessário ressaltar que a divulgação dessa filosofia entre todos que direta ou indiretamente estão envolvidos com a manipulação da informação é indispensável, no sentido de prevenir possíveis danos causados a seus clientes e/ou colaboradores.

Um documento bem elaborado de política de segurança deve ser claro e objetivo, no sentido de permitir o acesso a todos da organização independentemente do grau de instrução ou cargo que ocupa.

Em outras palavras, ao se reportar a respeito da divulgação no âmbito da organização da filosofia adotada para segurança da informação, Mitnick (2003, p.209), argumenta que

> O objetivo do programa de conscientização de segurança é a comunicação da importância das políticas de segurança e o dano que a falha em seguir essas regras pode causar, Dada a natureza humana, os empregados às vezes ignoram ou sabotam as políticas que parecerem ser injustificadas ou que demandam muito tempo. A gerência tem a responsabilidade de garantir que os empregados entendam a importância das políticas e sejam motivados para atendê-las, e não tratá-las como obstáculos a serem contornados.

Dessa forma, os principais aspectos orientadores de uma política de segurança da informação, segundo Caruso (2006, p. 57) são:

> **Objetivos da segurança**: deve explicar de forma rápida e sucinta a finalidade da política de segurança;
> **A quem se destina**: deve definir claramente quais as estruturas organizacionais e os ocupantes de funções aos quais a política se aplica;
> **Propriedade dos recursos**: deve definir de forma clara as regras que regerão os diversos aspectos relacionados com a propriedade de ativos de informações;
> **Responsabilidades**: deve definir de forma clara quais os tipos de responsabilidades envolvidas com o manuseio de ativos de informações, a quem ele deve ser atribuído e quais os mecanismos de transferência;
> **Requisitos de acesso**: deve indicar de forma clara quais os requisitos a serem atendidos para o acesso a ativos de informações;
> **Responsabilização**: deve indicar as medidas a serem tomadas nos casos de infringência às normas;
> **Generalidades**: nesta seção da política podem ser incluídos os aspectos que não cabem nas demais. Pode-se incluir aqui uma definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias (CARUSO, 2006, p. 57).

E ainda, segundo Guimarães; Lins e Oliveira (2006, p.12),

> É importante que a política de segurança defina os perímetros de segurança da rede. Isso impõe limita e organiza a rede da organização. Como por exemplo, define uso, responsabilidades, normas e detalhes de planos e ações destinados a responder sobre violação de sua política. Lista o que é permitido ou não na rede e nos sistemas de sua organização.

Dessa forma, identificar os principais riscos que tornam suas informações vulneráveis é um dos principais requisitos a serem observados na elaboração da política de segurança. Além disso, o documento deve estabelecer as metas a serem alcançadas e a sua atualização em função de novas ameaças e técnicas de ataques que surgem diariamente.

4 O BIBLIOTECÁRIO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

O uso da tecnologia nos processos de gestão com vistas à realização dos seus objetivos e funções nas bibliotecas é uma realidade. Assim o bibliotecário, não se diferencia dos demais, em se tratando de qualificação para desenvolvimento de suas atividades no processo de segurança da informação.

As bibliotecas como uma organização utilizam-se de ferramentas tecnológicas para a realização de suas tarefas diárias. No entanto, todo esse aparato tecnológico não dispensa a utilização de pessoas, visto que ainda é pouco considerável os sistemas autônomos. E, segundo Novo (2010, p. 106),

> As pessoas são os principais atores da Segurança da Informação. Sua responsabilidade está em preservar a informação e os meios que a contém. Para isso, devem estar preocupadas em instalar softwares de segurança, cuidar para que os sistemas estejam sempre atualizados, fazer uma varredura semanal contra *malwares*, escolher boas senhas e trocá-las de tempos em tempos, cuidar de suas mídias removíveis, para que não se extraviem nem sejam descartadas com dados desprotegidos, cuidar de seu e-mail, pensar antes de clicar em um link, fazer backup, manter-se atualizado e sempre estudando, e ser ético.

O bibliotecário é responsável pela gestão de bibliotecas, conforme a Classificação Brasileira de Ocupações (CBO), elaborada pelo Ministério do Trabalho, onde é descrita sumariamente as atividades desse profissional da seguinte forma:

> Disponibilizam informação em qualquer suporte; gerenciam unidades como bibliotecas, centros de documentação, centros de informação e correlatos, além de **redes e sistemas de informação** [grifo nosso]. Tratam tecnicamente e desenvolvem recursos informacionais, disseminam informação com o objetivo de facilitar o acesso e geração do conhecimento; desenvolvem estudos e pesquisas; realizam difusão cultural; desenvolvem ações educativas. Podem prestar serviços de assessoria e consultoria. (BRASIL, 2017).

A área de atividade "gerencia de redes e sistemas de informação", acima destacada, se desdobra, entre outras atividades, em "controlar segurança patrimonial da unidade, rede e sistema de informação", segundo a CBO. Isso implica que o profissional da informação deve possuir competência e habilidade na aplicação das tecnologias, que segundo Mata e Cesarin (2010, p. 308), se refere ao

> [...] uso das tecnologias nas unidades de informação, devendo os profissionais ali atuantes possuir familiaridade com elas, visando atender e satisfazer às necessidades informacionais de seus usuários. O uso das tecnologias envolve os *softwares* de auxílio na organização da informação, no armazenamento e na difusão de informação em ambiente eletrônico, entre outros.

Então, o profissional da informação necessita acompanhar as mudanças que ocorrem no seio da sociedade sob todos os aspectos, com destaque para as inovações tecnológicas inerentes aos ambientes informacionais.

Ao se reportar sobre essa questão, Cunha (1984, p. 149), argumenta que

> Atualmente a sociedade está mudando a uma velocidade cada vez maior, e o bibliotecário precisa se manter atualizado com essas mudanças e incorporar novos conhecimentos, a fim de que possa exercer bem o seu papel social nesse cenário tão dinâmico. Com a automação da biblioteca e a introdução de novas tecnologias de informação, muitas funções exercidas pelo *staff* da biblioteca têm sido afetadas. em alguns casos, muitas funções têm sido alteradas, modificadas, e outras totalmente eliminadas. Por essas razões, o **bibliotecário precisa reconhecer a necessidade e as vantagens da educação continuada para si próprio** [grifo nosso], para a instituição provedora de informação (seja ela uma biblioteca, centro de informação, etc.) e, principalmente, para a comunidade a que atende.

Assim ficou evidenciada a importância da educação continuada para os profissionais da informação, pois além de enriquecimento intelectual próprio, contribui para o desenvolvimento da instituição, com reflexos na eficiência do atendimento ao usuário. Em outras palavras, Figueiredo e Lima (1986, p. 50), enfatizam que

> O desenvolvimento profissional, além de preparar os indivíduos para a realização de tarefas específicas, deve transcender a isso, atingindo uma dimensão mais profunda, e criando atitudes desejáveis, para que sejam atingidas as metas institucionais e a elevação do nível de bem-estar da sociedade.

Dessa forma, a inserção de novas tecnologias nos ambientes organizacionais com vistas em agilizar os processos de tomadas de decisões, exige dos profissionais novas competências e habilidades para manusear esses aparatos tecnológicos com eficiência.

Os novos modelos de gestão, com o uso de tecnologias, obrigam os profissionais envolvidos, a um processo de qualificação permanente, dentro de um programa de educação continuada para manterem-se atualizados frente às constantes mudanças que caracterizam a era da informação. E nesse cenário se insere o Bibliotecário, enquanto profissional da informação.

Segundo Figueiredo e Lima (1986, p. 50)

> O treinamento deve ser um instrumento de intervenção no sistema de valores dos indivíduos e da organização para que o profissional acredite nos objetivos propostos como desejáveis e legítimos, e na importância do papel social que ele desempenha. Assim, o treinamento representa uma necessidade contínua, tal como a educação, que na realidade nunca termina e que deve estimular o indivíduo e a instituição, para que lance mão de seus recursos e esforços para melhorar rendimento e aumento de produtividade.

Assim, o investimento pelas organizações em qualificação dos profissionais que nelas atuam, representa uma valoração tanto do profissional quanto da organização, tendo em vista que as tarefas são executadas com mais eficiência e isso irá refletir na boa qualidade do produto.

Da mesma forma as bibliotecas devem reservar recursos financeiros para a formação continuada dos seus colaboradores, no sentido de acompanhar a evolução e usos das tecnologias, além de manter-se atualizado em relação às ferramentas que oportunizam a

intrusão dos seus sistemas de informação, que a cada dia estão mais sofisticados. Assim, assevera Cunha (1984, p. 153), ao tratar dessa questão que

> A biblioteca ou centro de informação deve também se preocupar em alocar recursos financeiros em seu orçamento para pagar despesas, ou parte delas, relativas a treinamento do bibliotecário em atividades de educação continuada. Independente do seu tamanho, a biblioteca não pode diminuir a necessidade de desenvolvimento profissional de seus funcionários, esteja ou não consubstanciada formalmente em programas de desenvolvimento de recursos humanos.

Por outro lado, o profissional também deve procurar o seu crescimento com investimento de recursos próprio. Em outras palavras, segundo Cunha (1984, p. 154), "[...] o bibliotecário deve investir em si próprio, assim como mostrar, divulgar e estimular tais organizações a oferecerem programas e facilidades que objetivam o desenvolvimento profissional".

No entanto, nem sempre as organizações tem essa visão, "Muitas empresas investem bastante nas melhorias tecnológicas de segurança e esquecem de focalizar o elo mais fraco na Segurança da Informação: o fator humano (SILVA et al., p. 31). Ou seja, vão na contramão daquilo que é de fato importante nessa questão de segurança da informação, o investimento na qualificação do pessoal.

Corrobora essa afirmação Sêmola (2003, p. 40), "A visão corporativa da segurança da informação deve ser comparada a uma corrente, em que o elo mais fraco determina seu grau de resistência e proteção".

Nesse sentido, um profissional que não está atualizado em relação aos movimentos tecnológicos, pode cair em um estado de ignorância, acarretando sérios prejuízos para a entidade. Conforme aponta Beal (2005, p. 78),

> Um aspecto de grande importância e muitas vezes negligenciado na segurança da informação é a proteção contra ataques de engenharia social. Hackers e outros tipos de pessoa mal intencionada podem valer-se da ingenuidade ou ignorância de usuários para obter informações confidenciais, como senhas, tipos de equipamento de segurança utilizados ou dados que podem comprometer a segurança da organização.

Portanto, a recomendação para as organizações em relação a essa questão, segundo Barros e Estrela (2015, p. 27) é que "As pessoas devem ser treinadas e educadas sobre quais são as informações que devem ser protegidas e como devem protegê-la para que estejam aptas a identificar situações de riscos, como um ataque de Engenharia Social".

A denominada Engenharia Social diz respeito, segundo Fontes (2006, p. 120) ao "[...] conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade".

Outro entendimento dado à questão da Engenharia Social é o de Mitnick (2003, p. 6) ao dizer que a Engenharia Social "[...] usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação".

Dessa forma o profissional bibliotecário que mantém uma agenda de educação continuada, nesse sentido, com certeza vai diminuir os riscos de ser persuadido.

Ainda, Santos (2000, p. 107), ao se reportarem sobre a questão da necessidade do profissional bibliotecário manter-se atualizado, enfatizam que

> O desenvolvimento das tecnologias da informação, "eliminando" as paredes das bibliotecas e disponibilizando informações abrigadas em sistemas distantes, de modo quase instantâneo, foi o grande argumento utilizado para exigir do profissional, além de um corpo de conhecimentos especializados na área do tratamento da documentação, outros conhecimentos e habilidades para a gerência de informações em suportes e locais diversificados.

Arruda et al (2004, p.23), ao tratar da questão do aprendizado contínuo, enfatiza que

> O delineamento de um novo perfil profissional não é exclusivo da área da informação, mas endógeno ao novo modelo econômico, que introduz novas formas de gestão do trabalho e de socialização dos indivíduos, valorizando a atuação em equipe, interdisciplinaridade, o aprendizado contínuo e atitudes comportamentais.

Dessa forma, o profissional bibliotecário deve possuir habilidades e competências não apenas no que tange ao tratamento e disseminação da informação, "[...] mas também conhecimentos e habilidades no uso das tecnologias para organizar, processar, recuperar e disseminar informações".

Porém isso não implica em dizer que o bibliotecário apenas deve adquirir habilidades para o manuseio das ferramentas tecnológicas, mas também formas de como gerenciar todo o processo que envolve essa questão, ou conforme Arruda et al., 2004, p.22),

> [...] a realidade contemporânea e da (re)definição do processo de trabalho, as análises sobre os novos requerimentos do conteúdo do trabalho dos profissionais da informação sinalizam não para a operacionalização tecnológica, mas para uma intensificação do trabalho abstrato (ensino de ferramentas informacionais, gerenciamento, planejamento e pesquisa), onde o conhecimento de tecnologia informacional é importante, mas não determinante para a realização do mesmo.

Pelo exposto, fica evidente que o profissional bibliotecário, na atualidade, deve possuir as habilidades e competências necessárias para suprir as novas demandas nas tarefas às quais estão sob sua responsabilidade, de forma eficiente.

Fato é que as bibliotecas armazenam em seus bancos de dados, além de seus registros de seus produtos, grande volume de dados cadastrais de seus usuários, com informações confidenciais que deverão ser mantidas em um ambiente seguro, de modo a dificultar a ação de intrusos, e violando assim o princípio da privacidade de seus usuários.

Dessa forma a biblioteca ou a entidade ao qual ela está vinculada, deve implementar uma política de segurança da informação, com objetivo de coibir o acesso por pessoas não autorizadas às informações da instituição e/ou dos seus usuários. A entidade deve estar ciente que a implementação dessa política visa não apenas proteger a informação, mas também precaver-se dos prejuízos que podem ser causados por uma falha de segurança ou a falta de uma política voltada para essa finalidade.

Manter o acervo em ambiente seguro, de modo a minimizar as vulnerabilidades, seja ela de origem natural, organizacional, física, de *hardware,* meios de armazenamento, humanas ou de comunicação, tem sido uma preocupação constante na rotina de toda e qualquer unidade de informação.

Segundo Souza (2014, p. 17), ao destacar a importância de se manter seguro o acervo no contexto da Segurança da Informação, argumenta que

> A Segurança da Informação de acervos torna-se importante em bibliotecas no momento em que cumpre a função de proteger as informações que a ela pertence ou que está sob sua responsabilidade, na busca de atender os princípios de confidencialidade, integridade e disponibilidade.

Nesse sentido, conclui Souza (2014, p. 19), "[...] a conservação e preservação de um acervo bibliográfico devem ter como base uma Política de Segurança que contemple as técnicas adequadas para garantirem a integração física do acervo".

A Política de Segurança deve contemplar, entre outras questões, as vulnerabilidades pelo o qual está sujeito o acervo de informação. A título de exemplo, cita-se aqui as de origem natural, ou seja, as variações que ocorrem tanto no ambiente externo como no interno, com base nos estudos de Souza (2014, p 18) que apontam alguns mecanismos de segurança da informação:

a) A temperatura e umidade relativa do ar deverão ser controladas de modo a fornecer um ambiente agradável aos usuários, assim como, um ambiente propício à conservação do acervo;
b) A iluminação pode ser tanto natural como artificial, no entanto não deve incidir diretamente no acervo, tendo em vista que a luz pode acelerar o processo de envelhecimento do papel;
c) A higienização do acervo, com o objetivo de controlar a ação de "[...] agentes biológicos constituídos principalmente por insetos, fungos e roedores são ameaças que causam danos irreparáveis". (SOUZA, 2014, p 18).
d) A proteção contra sinistros causados por incêndios e inundações, através de mecanismos de controle dos mesmos, como os dispositivos detectores de fumaça;

e) A proteção contra o roubo e o vandalismo, que segundo Souza (2014, p. 22)

> Na maioria das vezes isso vem acontecendo devido à falta de segurança e uma política de controle que evite esse tipo de ocorrência. Esse tipo de ataque ao acervo e documento é constante, sendo necessária a implantação de medidas que podem ajudar no combate a esses problemas.

Assim, explica Lima et al (2017, p. 397),

> Sobre os mecanismos de segurança da informação, destacam-se os controles físicos, os quais são considerados como barreiras que limitam o acesso direto à informação ou à infraestrutura, garantindo a existência da informação que a suporta. Para apoiar esses mecanismos de segurança (controles físicos: portas, blindagem, guarda etc.)

Esses mecanismos de controle físico, ainda sobre essa questão do roubo e vandalismo, o mercado dispõe de diversos equipamentos, conforme exemplificado através das ilustrações nas Figuras 6, 7, 8, 9.

Figura 6 – Dispositivo de Radiofrequência

Fonte: https://www.bibliotecas.ufu.br/servicos/seguranca-do-acervo

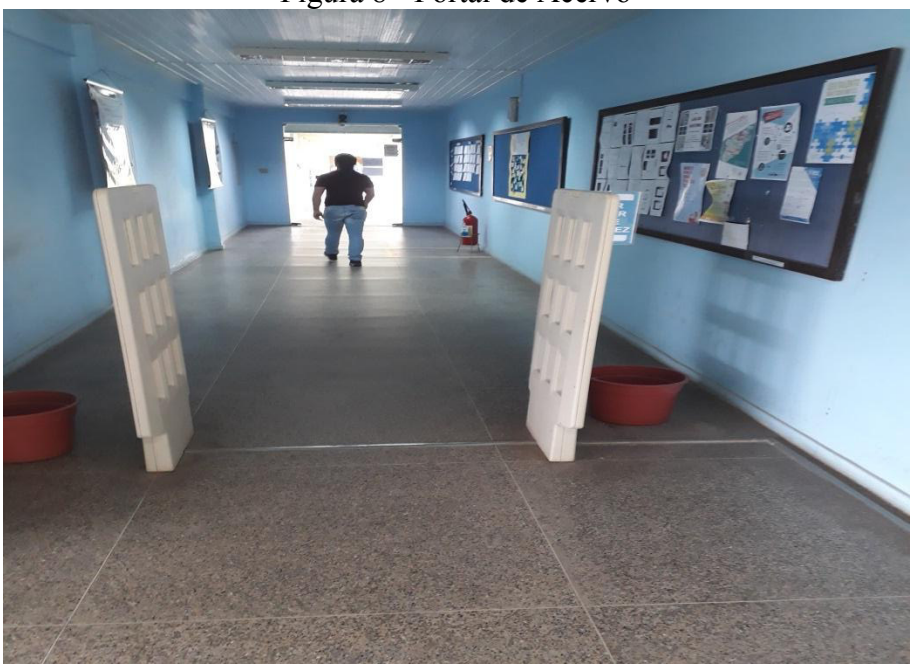
Este dispositivo é capaz de identificar o "[...] material informacional utilizado nas bibliotecas com possibilidades de receber informações digitais a serem transmitidas aos equipamentos de empréstimo [...]". (UFU, 2018).

Figura 7 – Equipamento para magnetizar material bibliográfico

Fonte: Biblioteca Central UFMA

Dispositivo utilizado para a proteção do livro, sendo que no ato do empréstimo a fita eletromagnética que se encontra dentro do material é desativada e reativada no ato da devolução.

Figura 8 - Portal de Acervo



Fonte: Biblioteca Central UFMA

Esse dispositivo é equipado com um sistema de detecção de itens ocultos. O sistema aciona um alarme caso algum protocolo de segurança ao acervo seja violado pelo usuário.

Figura 9 - Portal de Chaves

Fonte: https://www.bibliotecas.ufu.br/servicos/seguranca-do-acervo

Esse sistema controla e evita a utilização dos guarda-volumes por usuários que não pretendem permanecer no interior da biblioteca, ou seja, o usuário utiliza o guarda-volumes para armazenar seu material enquanto permanece em ambiente distinto ao da biblioteca.

Trata-se de um

> Sistema de detecção para as chaves dos escaninhos, de forma a garantir que os mesmos sejam utilizados somente no período de permanência do usuário no interior das bibliotecas. Dispara um alarme sempre que o usuário ultrapassa o portal para fora das bibliotecas com a chave acoplada ao sensor.

Esses sistemas apresentados representam o mínimo indispensável para manter a segurança física do acervo, no entanto, para o gerenciamento das informações do acervo o mercado dispõe de diversos sistemas de gerenciamento de bibliotecas ou sistema de informação.

Os sistemas de informações, via de regra, já possuem mecanismos de segurança que permitem a manutenção da informação dentro dos princípios de disponibilidade, confidencialidade e integridade.

Pode-se citar como exemplo o *software* Pergamum, que é um sistema informatizado de gerenciamento de dados, direcionado aos diversos tipos de Centros de Informação. Esse sistema objetiva facilitar a gestão dos centros de informação, melhorando a rotina diária com os seus usuários. É implementado na arquitetura cliente/servidor, com interface gráfica - programação em Delphi, PHP e JAVA, utilizando banco de dados relacional SQL (ORACLE, SQLSERVER ou SYBASE). (PERGAMUM, 2018).

Ainda, esse sistema permite a busca em catálogos em todas as bibliotecas que utilizam o sistema como gerenciador de suas tarefas e serviços, independentemente se a biblioteca pertence a essa ou aquela organização, dessa forma, o Pergamum possui a maior rede de bibliotecas do país.

O sistema oferece todas as funcionalidades necessárias para o desempenho das atividades gerenciais da biblioteca; as tarefas de processamento técnico; as tarefas de circulação de materiais; serviços de consultas e recuperação; e, serviços e tarefas online. (PERGAMUM, 2018).

Quanto às características técnicas o sistema oferece segurança e integridade dos dados; alta capacidade de armazenamento; atualizações do software; treinamento; acesso simultâneo. Dentre outros, no contexto de segurança da informação, destaca-se:

a) Segurança e integridade dos dados;
b) Alta capacidade de armazenamento;
c) Upgrade de versão sem custo para o contratante;
d) Treinamento para diferentes tipos de usuários;
e) Arquitetura cliente/servidor para acesso e atualização de dados em rede local e remotamente;
f) Acesso simultâneo de usuários às bases de dados;
g) Gerenciamento integrado de dados e funções da Biblioteca;
h) Migração da base de dados já existente na Biblioteca;
i) Utilização de senhas criptografadas;
j) Protocolo Z39.50 - Cliente/Servidor. (PERGAMUM, 2018).

Nessa expectativa, infere-se que os sistemas de informação para bibliotecas, de um modo geral, oferecem os mecanismos mínimos para manter segura e integra a informação, como por exemplo o uso de senhas criptografadas, conforme demonstrado acima.

Outro ponto importante é a atualização (*upgrade*) do sistema. Com o argumento que a evolução tecnológica, bem como, as novas configurações e demandas sociais, obrigam que os sistemas disponíveis no mercado sejam atualizados constantemente.

As bibliotecas, de modo geral, acompanham essas atualizações, com base nas constantes mudanças de versão do sistema que elas utilizam, no sentido de se adequarem à nova realidade a elas impostas e exigidas pelos usuários.

Fato esse de extrema importância, tendo em vista que segundo Lima et al (2017, p. 391), "Satisfazer as necessidades informacionais de cada usuário, individualmente, é importante tanto na forma tradicional de atendimento (presencialmente) quanto na forma que vem sendo exigida (virtualmente) [...]".

Quanto à questão do controle lógico, que para Lima et al (2017, p. 397) diz respeito às

> [...] barreiras que impedem ou limitam o acesso a informações que geralmente estão em ambiente controlado e eletrônico. Um dos mecanismos que apoia o controle lógico é a criptografia. Esta, por sua vez, permite codificar e transformar a informação de forma a torná-la ininteligível a terceiros, e, para tal, determinados algoritmos e chaves secretas são utilizadas para produzir uma sequência de dados criptografados a partir de dados não criptografados. Como mecanismos lógicos, pode-se citar também: a assinatura digital; as funções de "*Hashing*" ou de checagem; os mecanismos de controle de acesso (senhas, palavras-chave, biometria, *firewalls*, entre outros); e os mecanismos de certificação e de integridade e o *Honeypot*, programa cuja função é detectar e impedir a ação de um cracker, hacker e spammer, ou de qualquer outro agente externo. Existem, ainda, diversas ferramentas e sistemas voltados para a segurança, como os antivírus, firewalls, filtros AntiSpam, dentre outros.

O uso dessas ferramentas, acima citadas, são imprescindíveis, tendo em vista as inúmeras tentativas de infiltração por pessoas não autorizadas aos sistemas de informação que ocorrem constantemente. Portanto, afirmam Lima et al (2017, p. 397),

> "[...] 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, para 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 ou da gestão institucional".

Para tanto, a biblioteca deve manter em sua agenda um programa de capacitação e atualização dos seus colaboradores, em razão do aumento constante dos softwares programados para atacar seu sistema de informação. Assim, as unidades de informações constantemente devem reavaliar suas políticas de Segurança da Informação, no sentido de revisar seus objetivos, a forma de atuação, e os procedimentos, visto que na mesma medida que esses softwares são criados, também muda o modo de operação.

5 CONCLUSÃO

Abordar o tema Segurança da Informação não é tarefa fácil, por se tratar de algo sensível, complexo e com uma variedade enorme de conceitos. Porém, é um assunto que está em evidencia nos últimos tempos, principalmente no âmbito das organizações, como demonstrado ao longo do trabalho.

A informação configurada como o bem de maior valor para as organizações, vem merecendo um lugar de destaque, adquirindo grande importância. Dessa forma, a preocupação em manter a informação em um ambiente seguro tem ocasionado grandes investimentos financeiros na elaboração de estratégias que garantam essa segurança. Grandes investimentos são feitos no treinamento e capacitação de pessoas, bem como na atualização dos equipamentos e s*oftwares,* com vistas a coibir o acesso de pessoas não autorizadas ao sistema de informação das entidades. Segundo o esclarecimento de Stair e Reynolds (2016, p. 7),

> Vivemos hoje em uma economia informatizada. A informação por si possui valor, e o comércio muitas vezes envolve a troca de informações em vez de bens tangíveis. Os sistemas computacionais são cada vez mais utilizados para criar, armazenar e transferir informações. Utilizando sistemas de informação, os investidores tomam decisões multimilionárias, as instituições financeiras transferem bilhões de dólares eletronicamente ao redor do mundo e os produtores encomendam suprimentos e os distribuem bens mais rápido do que nunca. Computadores e sistemas de informação continuarão a mudar os negócios e o modo como vivemos. Para se preparar para essas inovações, você precisa estar familiarizado com os conceitos fundamentais de informação.

O uso das TIC's favoreceu a agilidade nos processos de tratamento da informação, porém, favoreceu certo grau de vulnerabilidade, sendo necessário um monitoramento constante. Tendo em vista que diariamente são lançados na rede mundial de computadores centenas de códigos maliciosos que podem causar grandes prejuízos financeiros à organização.

Dessa forma faz-se necessária a implementação de uma Política de Segurança da Informação que seja acessível a todos os colaboradores da organização, para não restar dúvidas, ou entendimento ambíguo, quanto à sua execução.

Em síntese Abreu (2002 apud LAUREANO, 2005, p. 56), "A Política de Segurança é apenas a formalização dos anseios da empresa quanto à proteção das informações".

O processo evolutivo pelo qual passou a Segurança da Informação confunde-se com a própria história evolutiva do homem. Ou seja, "Os primórdios da Segurança da Informação estão vinculados à própria evolução do homem e de sua vida em comunidade. Em determinado momento, a humanidade sentiu necessidade de representar seu dia a dia, sua religiosidade e a si própria". (NOVO, 2010, p. 15).

Da mesma forma, as bibliotecas estão inseridas nesse contexto enquanto organizações. O profissional bibliotecário responsável pela gestão da biblioteca deve primar por manter-se atualizado através de educação continuada, utilizando recursos da instituição ou próprios. Esse fator é primordial para garantir a segurança dos ativos de informação que estão sob sua responsabilidade.

Não resta dúvidas que o papel do bibliotecário é de gestão dos recursos informacionais disponíveis na biblioteca ao qual ele está vinculado. Dessa forma o bibliotecário deve estar afinado com as novidades tecnológicas que surgem diariamente no mercado, principalmente no que tange às tecnologias voltadas para a gestão da segurança da informação, assim vai estar habilitado para lidar com os riscos inerentes à segurança da informação.

Com base no material estudado e exposto aqui pode se inferir que a segurança da informação é fator primordial na preservação dos dados, bem como na manutenção de qualidade nas relações de compartilhamento desses dados entre a organização e seus colaboradores e clientes.

Ou ainda, segundo Freitas (2009, p. 17),

> Em termos estratégicos, a segurança da informação pode agregar valor ao dar maior confiabilidade ao próprio processo de transformação. A integração entre o negócio e a tecnologia empregada pode imprimir maior maturidade e solidez às transações com o cliente. A confiabilidade nas transações vai se traduzir na idéia de maior confiabilidade nos negócios.

Observou-se também que as ameaças às vulnerabilidades são uma constante. Assim, as organizações se movimentam para encontrar soluções que coíbam esses ataques ou minimizem os impactos nos ativos. Segundo Novo (2010, p. 29),

> Podemos incluir nos ativos de informação os meios físicos que os suportam (e que permitem seu transporte) e as pessoas que os utilizam. Como exemplos de meios físicos, temos os discos rígidos, pen drives, CDs, DVDs, cabeamento de redes, switches e roteadores. Além desses, também podemos citar documentos impressos, correspondências, linhas de código de programação, relatórios financeiros, projetos de engenharia, etc.

Assim, justifica-se o grande investimento feito pelas organizações em segurança da informação, visto que esses ativos representam grande parte do patrimônio das mesmas, sem essa proteção os danos ou prejuízos seriam em muitos casos irreparáveis. Fenômeno esse que também deve ocorrer nas bibliotecas, tendo em vista que "[...] independente da natureza e do público a que uma determinada biblioteca se destine, se a sua gestão não se sensibilizar com a questão da segurança da informação, a biblioteca estará sujeita a graves problemas [...]". (LIMA et al (2017, p. 397).

REFERÊNCIAS

ARRUDA, M. da C. C.; MARTELETO, R.M.; SOUZA, D.B. de. **Educação, trabalho e o delineamento de novos perfis profissionais**: o bibliotecário em questão. Ciência da Informação, Brasília, v.29, n.3, p.14-24, set./dez. 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2005. Disponível em: http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf. Acesso em: 05 maio de 2018.

BARROS, Edilberg Nunes; ESTRELA, Luana de Souza. Organização da segurança da informação. In: LYRA, Maurício Rocha (Org.). Governança da Segurança da Informação. Brasília: 2015, 160p.

BEAL. A. **Segurança da informação**: princípios e as melhores práticas para a proteção dos ativos de informações nas organizações. São Paulo: Atlas, 2008.

BRASIL. Ministério do Trabalho. Classificação Brasileira de Ocupações. Brasília, DF. 2017. Disponível em: http://www.mtecbo.gov.br/cbosite/pages/pesquisas/FiltroTabelaAtividade.jsf. Acesso em: 22 out. 2017.

BRASIL. Tribunal de Contas da União. Boas práticas em segurança da informação. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

CARUSO, C. A. A.; STEFFEN, F. D. Segurança em informática e de informações. 3. ed. rev. e ampl. São Paulo: Senac São Paulo, 2006.

CUNHA, M. B. O desenvolvimento profissional e a educação continuada. **Revista de Biblioteconomia de Brasília**, v. 12, n. 2, p. 149-156, 1984. Disponível em: http://www.brapci.inf.br/v/a/3018. Acesso em: 26 out. 2017.

DANTAS, Marcus Leal. **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 155 p.

DIAS Cláudia. **Segurança e auditoria da tecnologia da informação**. Editora Axcel Books, 2000.

DEMO, Pedro. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2000.

DEMO, Pedro. **Introdução à metodologia da ciência**. 2. ed. São Paulo: Atlas, 1985.

FERREIRA, Aurélio Buarque de Olanda. **Novo Dicionário Aurélio da Língua Portuguesa**. 3. ed. Curitiba: Editora Positivo, 2004.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação**: guia prático para elaboração e Implementação. Rio de Janeiro: Ciência Moderna., 2008.

FIGUEIREDO, N. M.; LIMA, R. C. M. Desenvolvimento profissional e inovações tecnológicas. **Revista da Escola de Biblioteconomia da UFMG**, v. 15, n. 1, p. 47-67, 1986. Disponível em: http://www.brapci.inf.br/v/a/2015. Acesso em: 26 out. 2017.

FREITAS, **Eduardo Antônio Mello. Gestão de riscos aplicada a sistemas de informação**: segurança estratégica da informação. Brasília: UCM, 2009.

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

GUIMARAES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo. **Segurança com Redes Privadas Virtuais**. São Paulo: Brasport Livros e Multimídia. v. 1, 2006.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**, 5. ed. São Paulo: Atlas 2003.

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 p.389-419 maio/ago. 2017. Disponível em: http://eprints.rclis.org/31861/1/8646416-25836-6-PB.pdf. Acesso em: 01 jul. 2018.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. Curitiba: Editora do Livro Técnico, 2012, 152 p.

LYRA, Maurício Rocha (Org.). **Governança da segurança da informação**. Brasília: 2015, 160p

MACHADO, Ana Maria Nogueira**. Informação e controle bibliográfico**: um olhar sobre a cibernética. -São Paulo: Editora UNESP, 2003. 159 p.

MITNICK, Kevin D. **Arte de Enganar**. São Paulo: Pearson Education do Brasil., 2003.

MATA, Marta Leandro; CASARIN, Helen de Castro Silva. A formação do bibliotecário e a competência informacional: um olhar através das competências. In: VALENTIM, Marta. **Gestão, mediação e uso da informação**. São Paulo: Cultura Acadêmica, 2010, 392 p. 301-319.

MOREIRA, Nilton Stringasci. **Segurança mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books. 2001.

NOVO, Jorge Procópio da Costa. **Softwares de segurança da informação**. Manaus: Centro de Educação Tecnológica do Amazonas, 2010. 116 p.

OLIVEIRA, Wilson. Segurança da Informação: técnicas e soluções. Lisboa: Inova, 2001. 2016 p.

PERGAMU. Características técnicas: tecnologias e características gerais. Disponível em: <http://www.pergamum.pucpr.br/redepergamum/pergamum_caracteristicas_tecnicas.php?flag=CollapsiblePanel1&ind=2>. Acesso em: 01 jul. 2018.

PLANES, Paulo. Um pouco de história para entender os sistemas de informação. **TI Especialista**. Disponível em: https://www.tiespecialistas.com.br/2015/10/um-pouco-de-historia-para-entender-os-sistemas-de-informacao/. Acesso em: 18 out. 2017.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

REYNOLDS, Georg W.; STAIR, Ralph M. **Princípios de sistema de informação**. 11 ed. Tradução: Noveritis do Brasil. São Paulo: 2016. 752 p.

SÊMOLA, Marcos. **Gestão da segurança da informação**: visão executiva da segurança da informação. Rio de Janeiro: Campus, 2003. ok

_____. Sociedade do conhecimento. In: _____. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014. cap. 1, p. 1-12.

SILVA, Abílio F. da; et al. Segurança da informação: o elo mais fraco. p. 13-32. In: SILVA, Eliane F. da. **Segurança da informação**: temas para uma prática. Natal: EDUFRN, 2008, 117 p.

SILVA, Fabio Alves da. **A evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro**. 2014, 72 f. Dissertação (Mestrado em Desenvolvimento Econômico) - Universidade Federal do Paraná, Curitiba, 2014.

SILVA, Jonathas Luiz Carvalho; GOMES, Henriette Ferreira. Conceitos de informação na ciência da informação: percepções analíticas, proposições e categorizações. João Pessoa: **Inf. & Soc**., João Pessoa, v.25, n.1, p. 145-157, jan./abr. 2015. Disponível em: http://www.ies.ufpb.br/ojs/index.php/ies/article/view/145/13200. Acesso em: 11 set. 2017.

SOUZA, Márcio Marinho de. A segurança da informação em acervos de bibliotecas: estudo de caso na biblioteca central da universidade federal da Paraíba – campus I. João Pessoa: UFPB, 2014, 41p.

UNIVERSIDADE FEDERAL DE UBERLANDIA. Segurança do acervo: Conheça as tecnologias utilizadas para segurança do acervo nas bibliotecas UFU. Disponível em: <https://www.bibliotecas.ufu.br/servicos/seguranca-do-acervo>. Acesso em: 01 jul. 2018.