UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO
BACHARELADO EM BIBLIOTECONOMIA

INGRID MOANA PEREIRA DA SILVA

SEGURANÇA DA INFORMAÇÃO E O BIBLIOTECÁRIO: um guia prático

NATAL
2021

INGRID MOANA PEREIRA DA SILVA

SEGURANÇA DA INFORMAÇÃO E O BIBLIOTECÁRIO: UM GUIA PRÁTICO

Monografia apresentada ao curso de graduação em Biblioteconomia da Universidade Federal do Rio Grande do Norte, como requisito parcial à obtenção do título de Bacharel em Biblioteconomia.

Orientadora: Profa. Dra. Monica Marques Carvalho Gallotti

NATAL

2021

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro Ciências Sociais Aplicadas - CCSA

Silva, Ingrid Moana Pereira da.
Segurança da informação e o Bibliotecário: um guia prático / Ingrid Moana Pereira da Silva. - 2021.
56f.: il.

Monografia (Graduação em Biblioteconomia) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas, Curso de Ciência da Informação. Natal, RN, 2021.
Orientadora: Profa. Dra. Monica Marques Carvalho Gallotti.

1. Segurança da Informação - Monografia. 2. Profissional bibliotecário - Monografia. 3. Unidades de Informação - Monografia. I. Gallotti, Monica Marques Carvalho. II. Universidade Federal do Rio Grande do Norte. III. Título.

RN/UF/Biblioteca CCSA CDU 023.4:004.056

Elaborado por Eliane Leal Duarte - CRB-15/355

INGRID MOANA PEREIRA DA SILVA

SEGURANÇA DA INFORMAÇÃO E O BIBLIOTECÁRIO: UM GUIA PRÁTICO

Monografia apresentada ao curso de graduação em Biblioteconomia da Universidade Federal do Rio Grande do Norte, como requisito parcial à obtenção do título de Bacharel em Biblioteconomia.

Aprovada em: 17/09/2021

BANCA EXAMINADORA

_____

Profa. Dra. Monica Marques Carvalho Gallotti
Orientador(a)

_____

Profa. Dra. Ilaydiany Cristina Oliveira da Silva
Membro interno

_____

Profa. Ma. Adelaide Helena Targino Casimiro

Membro interno

Dedico esse trabalho a DEUS primeiramente, pois sem ele eu nada seria. Ademais, dedico a minha mãe Ângela Vírginia o ser humano mais incrível e amável que conheço, sem dúvidas ela é meu porto seguro.

AGRADECIMENTOS

Essa deveria ser a sessão mais longa desse trabalho, pois são tantas pessoas que me ajudaram até aqui que as páginas desse trabalho não seriam suficientes para mencioná-las e por elas serei eternamente grata!

O primeiro muito obrigado, vai para a pessoa que dá sentido à minha vida, que me permitiu colocar cada palavra nesse trabalho. Obrigado, meu senhor DEUS, por toda força que depositou em mim nesse processo, obrigado também por estar comigo e sempre me mostrar a quão capaz e amada sou. Amém!

Agradeço as quatro mulheres da minha vida, que me educaram e me ajudaram a descobrir como sou forte. A minha mãe Ângela Virgínia Lopes Agradeço de todo coração pelo apoio, pelas palavras de incentivo e pelos puxões de orelha, sem sombras de dúvidas essa mulher foi a primeira referência de resiliência que conheci.

Ainda agradeço as minhas avós materna e paterna por serem a real representação do amor de Deus por mim, por me apoiarem e protegerem com cuidado e afeto, por isso tudo muito obrigado! Eliana Virginia Lopes e Maria de Lourdes Pereira da Silva, não poderei mencionar o amor que tenho por vocês apenas em palavras. A quarta mulher da minha vida é minha tia Marluce Pereira do Nascimento que com seu jeitinho único, mas muito parecido com o meu, não me permitiu desistir quando enfrentei grandes desafios ao decorrer dessa graduação, dessa forma sou muito grata por seu apoio, elas são minha âncora em terra.

Agradeço ainda a todas as pessoas que fizeram parte do meu crescimento na Universidade Federal do Rio Grande do Norte, colegas de sala, professores e coordenadores, muito obrigado.

Sou grata pela oportunidade e principalmente pela amizade desenvolvida com a Íris Álvares Dantas, Coordenadora do Laboratório de imagens da UFRN - Labim, na qual tive o prazer de colaborar com o trabalho de alta qualidade desenvolvido por ela e por uma equipe maravilhosa. Posso afirmar que essa experiencia me trouxe crescimento profissional e pessoal.

Uma gratidão especial tenho pela minha orientadora Monica Marques Carvalho Gallotti, profissional e ser humano incrível que me apoiou em todo o processo de construção desse trabalho de conclusão de curso, acreditou na capacidade e, no meio do turbilhão de acontecimentos, mostrou confiança e amor pela profissão que escolheu. Espero um dia ser espelho dessa profissional que eleva a Biblioteconomia com amor e garra!

Por fim, agradeço de fato a todos envolvidos diretos ou indiretos na profissional que se forma com esse trabalho, com essa graduação, com esse curso e com essa instituição, chamada UFRN.

Então, vê agora por que os livros são tão odiados e temidos? Eles mostram os poros no rosto da vida. As pessoas acomodadas só querem rostos de cera, sem poros, sem pêlos, sem expressão.

Ray Bradbury

RESUMO

A sociedade atual é caracterizada pelo excesso de informações colocadas ao alcance das pessoas como consequência das tecnologias digitais que avançam em ritmo célere e causam impactos variados. Um dos impactos trazidos por esta nova era é a necessidade de melhoria das estratégias de organização, tratamento, preservação e em especial, a da segurança da informação (SI) no contexto das organizações. A partir da seguridade informacional é que as organizações podem atingir seus objetivos e dar continuidade as suas atividades de negócios, produzindo inovação e obtendo vantagens competitivas. Diante disso, este trabalho tem como objetivo geral analisar a importância dos preceitos da segurança da informação nas organizações e o papel do bibliotecário neste contexto. Especificamente visa elencar os principais conceitos e características destes preceitos, apontar a sua importância bem como identificar normas, legislações e cartilhas voltadas para boas práticas neste campo. A metodologia foi caracterizada como exploratória, com uso da estratégia da pesquisa bibliográfica considerando fontes de informação, como periódicos científicos, livros e sites, dentre outros. Por fim, infere-se que na atualidade, a segurança da informação se reveste em uma estratégia de salvaguarda e controle eficiente dos ativos informacionais de organizações diversas, tais como as unidades de informação, porém, ainda se faz necessário a implementação de boas práticas neste campo de maneira que se reforce a sua importância. Aponta-se também a necessidade de Bibliotecário atuar neste campo em conjunto com uma equipe multidisciplinar, com vistas a perpetuar as boas práticas e promover a inovação desejável na atualidade.

Palavras-chave: Segurança da Informação; Profissional Bibliotecário; Unidades de Informação.

ABSTRACT

Today's society is characterized by information excess that is made available to people as a result of digital technologies that are advancing rapidly causing varied impacts. One of the impacts brought by this new era is the need to improve information organization, treatment, preservation and, in particular, information security strategies in the context of organizations. Based on informational security, organizations can achieve their goals and continue their business activities, producing innovation and obtaining competitive advantages. Therefore, this work aims to analyze the importance of information security precepts in organizations and the role of the librarian in this context. It specifically aims to point out the main concepts and characteristics of these precepts, reinforce their importance as well as identify standards, legislation and booklets aimed at good practices in this field. The methodology was characterized as exploratory, using the bibliographic research strategy considering information sources such as academic journals, books and websites, among others. As a result, it is inferred that currently, information security is safeguarding and efficient strategy in order to control informational assets in organizations such as information units. However, it is still necessary to implement good practices in this field. Th research also reinforces the need for Librarians to work in this field together in a multidisciplinary team, with a view to perpetuating good practices and promoting the desired innovation today.

Keywords: Information Security; Professional Librarian; Information Units.

LISTA DE FIGURAS E QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BS	British Standard
CCSC	Commercial Computer Security Centre – no português Centro de Segurança da Informação
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CID	Confidencialidade, Integridade e Disponibilidade
CRB	Conselho Regional de Biblioteconomia
DTI	Departamento de Comércio e Industria do Reino Unido
ENIAC	Electronic Numerical Integrator And Computer
IBM	International Business Machines Corporation
IEC	International Electrotechnical Commission – no português Comissão Eletrotécnica Internacional
ISSA	Information Systems Security Association – no português Associação de Segurança em Sistemas de Informação
ISO	International Organization of Standardization – no português Organização Internacional de Padronização de Tecnologias
MEC	Ministério da Educação e Cultura
NBR	Norma Brasileira
PPT	Pessoas, Processos e Tecnologias
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação
STJ	Superior Tribunal de Justiça
SWOT	Strenghts, Weaknesses, Opportunities e Threats – no português Forças, Fraquezas, Oportunidades e Ameaças
TCU	Tribunal de Contas da União

SUMÁRIO

1 INTRODUÇÃO

A sociedade atual caracteriza-se como a Sociedade da Informação, isso porque as tecnologias propiciaram uma maior propagação da informação pelas redes, alcançando lugares extremos e permitindo a disseminação da informação em escala exponencial. Essa "democratização" informacional está atrelada diretamente a ascensão das mídias e tecnologias digitais que se fazem presentes na palma da mão da população global. Essa caracterização foi absorvida a partir da leitura do livro Sociedade da Informação no Brasil ou "livro verde", como é popularmente conhecido por profissionais da área da informação, organizado por Tadao Takahashi.

> [...] passamos – em geral, sem uma percepção clara nem maiores questionamentos – a viver na Sociedade da Informação, uma nova era em que a informação flui a velocidades e em quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais. (TAKAHASHI, 2000, p. 03).

Esse paradigma nas telecomunicações e na informática impactam diretamente na proporção da difusão da informação e no processo de absorção, disseminação e produção do conhecimento humano. A Sociedade da Informação baseia-se fundamentalmente na informação e no poder transformador que ela tem na vida das pessoas, nas relações e nos negócios, sendo considerado um fenômeno global. Assim como apontado a seguir:

> É um fenômeno global, com elevado potencial transformador das atividades sociais e econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infra-estrutura de informações disponível. [...] Tem ainda marcante dimensão social, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação. (TAKAHASHI, 2000, p. 05).

Como já apresentado, ao falar das relações interpessoais na contemporaneidade não se pode deixar de elencar a importância que a Sociedade da Informação tem sobre as relações pessoais, pois, com as tecnologias de comunicação as maiores distâncias foram amenizadas com, por exemplo, a comunicação por chamada em vídeo, conectando famílias, amigos e ainda grupos de pesquisa. Porém, esse estreitamento de distâncias trouxe problemas para a comunicação face a face, causando quadros de dessocialização e exclusão social, as pessoas preferem se comunicar por mensagens instantâneas e com uso de *emojis* (ideogramas que

representam como as pessoas estão se sentido no momento), isso afeta diretamente a capacidade de se comunicar, de realizar diálogos ou debates e principalmente de discernir os sentimentos vivenciados na vida real.

Ademais, a disseminação de informações em alta escala e sem controle faz emergir algumas problemáticas, por exemplo: como gerir essa informação toda de maneira eficiente e eficaz; como distinguir informações confiáveis das não confiáveis e como democratizar de fato as tecnologias da informação para que alcancem o maior número de pessoas; e como diminuir o impacto negativo do "boom" da informação na qualidade das relações interpessoais.

Uma das principais preocupações, sem dúvidas, é com o fenômeno de informações duvidosas e enganosas inseridas no contexto virtual e nas redes sociais, esse excesso informacional de *Fake News*, trouxe à tona um novo conceito, a infodemia. Essa terminologia surgiu com a situação de pandemia do COVID-19, que abalou o mundo com uma contaminação viral, na qual contabiliza no Brasil mais de meio milhão de mortos. Porém, além da disseminação da doença, ainda foi necessário lidar com a alta propagação de *Fake News* no país, além da desinformação, que foi responsável por 800 mortos em três meses de pandemia segundo a BBC Brasil[1].

A infodemia caracteriza-se como um "fenômeno recente de disseminação de informações potencializada por conta da revolução tecnológica. Estamos vivendo a primeira grande infodemia da nova era digital, que pode comprometer, inclusive, nossa saúde mental", segundo o site do Governo do estado de São Paulo – Secretaria da educação.[2]

Tal situação é impactada pelo processo de filtragem informacional, assim tem-se muita informação disponível, porém a sociedade não sabe garimpar ou filtrar o que de fato é confiável, e assim se faz necessário a educação midiática, na qual, pode ser considerada como habilidades educativas que auxiliam no processo de acesso e garimpagem de informações, para garantir a pesquisa e disseminação de informações, com intuito de desenvolver cidadãos críticos. Em consonância, temos a caracterização de educação midiática, como:

> Conjunto de habilidades para acessar, analisar, criar e participar de maneira crítica do ambiente informacional e midiático em todos os seus formatos - dos impressos aos digitais -, como requisito fundamental para a formação do cidadão e para o fortalecimento da democracia. (GOVERNO DO ESTADO DE SÃO PAULO – SECRETARIA DA EDUCAÇÃO, [*s. d*])[3]

[1] Disponível em: https://www.bbc.com/portuguese/internacional-53762751
[2] Disponível em: http://www.escoladeformacao.sp.gov.br/portais/Default.aspx?tabid=4572&EntryId=4711
[3] Disponível em: http://www.escoladeformacao.sp.gov.br/portais/Default.aspx?tabid=4572&EntryId=4711

Ainda sobre o consumo informacional em alta quantidade, temos o estudo *How Much information*[4], publicado em 2009 e de autoria da Universidade de Barkeley, na qual revela que os estadunidenses passam 12 (doze) horas por dia consumindo informação, o que equivale a cerca 34 (trinta e quatro) gigabytes de informação, assim caracterizando de fato uma avalanche informacional.

Com a ascensão das tecnologias os desafios sob o processo de gestão da informação, são relacionados com a produção, representação, armazenamento, disseminação e descarte da informação. E é a partir desses desafios que surgem as estratégias de controle e gestão da informação, como também estratégias para garantir a seguridade dos ativos informacionais.

Nesse cenário, surge a preocupação com a Segurança da Informação (SI) de maneira mais latente, vista nos mais diversos ângulos e nos mais distintos ambientes. Desse modo, sendo fundamental a preocupação com o desenvolvimento de mecanismos que garantam o resguardo informacional nas organizações, prevalecendo assim os princípios de: confidencialidade, integridade e disponibilidade.

Assim como a informação permeia toda sociedade, não seria diferente nas organizações. Para que as empresas desenvolvam suas atividades diariamente, é necessário o uso de ativos informacionais e uma gestão consciente desses recursos, assim tais fatores são determinantes para o sucesso das organizações, pois, a partir disso, empresas conseguem manter suas principais informações longe da concorrência e garantem considerável vantagem competitiva no mercado.

Para ajudar e contribuir na gestão estratégica, temos a figura do profissional bibliotecário, agente capaz de lidar com a informação em todo o processo e ciclo de vida, colaborando com o processo de gestão da informação e principalmente com a adaptação de normas, legislações e políticas de SI nas organizações.

Nesse contexto, temos a ação desse profissional em ambientes além dos convencionais, como bibliotecas e centros de documentação, mas também em corporações que trabalhem com os mais diferentes tipos de informações e dados. Esses novos ambientes podem também ser galgados a partir dos requisitos apontados pela Lei Geral de Proteção à Dados, que aponta como as organizações devem resguardar as informações de seus clientes, e sobre a transparência na utilização desses dados. Em seguida os nossos objetivos.

[4] Disponível em: https://bit.ly/3AXbvi5

1.1 Objetivos

Geral: Analisar a importância dos preceitos da SI nas organizações e o papel do bibliotecário nesse contexto.

Específicos:

- Elencar os principais conceitos e características da Segurança da Informação;
- Identificar as principais normas e legislações neste campo;
- Apontar a importância da SI em organizações;
- Indicar as boas práticas no campo da SI.

1.2 Metodologia

Para a consecução dos objetivos propostos e com vistas a promover um embasamento teórico sobre o assunto, recorreu-se a pesquisa bibliográfica, na qual tem o objetivo de apresentar parte do conteúdo já desenvolvido sobre uma temática e apresentar as tendências futuras da literatura. Desse modo, inicialmente foi realizado um levantamento referencial sobre a temática central, em bases de dados e plataformas digitais de pesquisa, verificando a ocorrência de forma isolada e depois a correlação das seguintes expressões de busca: "Segurança da Informação", "Biblioteconomia" e "Bibliotecário". Adicionalmente, foi feito um levantamento em livros da área, consulta a *websites*, e vídeos. Para Gil (2002, p. 50) este tipo de pesquisa: "se constitui numa proposta de se tentar compreender e/ou explicar um fenômeno a partir de um referencial teórico, que pode ser composto por livros, artigos científicos, dentre outras fontes".

Corroborando com tal perspectiva, Lakatos e Marconi (2003) indicam que a pesquisa bibliográfica visa o levantamento da bibliografia já publicada em forma de artigos, em revistas e sites, teses, dissertações, livros, publicações avulsas e representadas por meio convencional ou digital. Ainda nesta linha de pensamento, Severino (2017) enfatiza que este tipo de pesquisa "para proporcionar o avanço em um campo do conhecimento é preciso primeiro conhecer o que já foi realizado por outros pesquisadores e quais são as fronteiras do conhecimento". Portanto,

foram coletadas as evidências na literatura e foi feito um cotejo entre as narrativas sobre o assunto supracitado.

A pesquisa é de caráter descritivo e de natureza qualitativa, pois conforme exposto, tem como objetivo identificar conceitos difundidos na área da SI. Com isso, trabalhar inicialmente com o que já foi produzido traz considerável bagagem para se pensar nos próximos avanços, e, principalmente, no possível impacto gerado pela ampliação de fronteiras do conhecimento na área.

1.3 Justificativa

Apesar da SI ser uma área com tempo de estrada e pesquisa, é notório a dificuldade ainda presente na sociedade de lidar com todas as implicações em torno dessa temática. Isso não é diferente no contexto das organizações que precisam gerenciar a informação com muito mais cautela, uma vez que lida com dados sensíveis de clientes, fornecedores e colaboradores. Por esse motivo, surge a importância do papel do profissional da informação, nesse caso o bibliotecário, capaz de gerir e desenvolver técnicas eficientes para o processo de gestão da informação.

Assim, destaca-se que é necessário trabalhar com tal temática, pois a preservação da informação é uma questão urgente a ser pensada e avaliada, uma vez que é de responsabilidade das organizações garantir a proteção de seus ativos informacionais, pensando em manter tais recursos disponíveis, quando necessário, para as pessoas certas e de maneira íntegra.

Ao analisar a SI e o profissional bibliotecário é possível verificar novas estratégias de como lidar com a seguridade das informações, e com novas oportunidades para o mercado de trabalho para o bibliotecário. Ademais, possibilitará diversas visões e ampliações do fazer profissional, que com advento das tecnologias da informação teve a ampliação do seu reportório de ações, propostas de trabalho. A partir da atual pesquisa, profissionais da informação serão encorajados a tomar para si as atividades voltadas para seguridade informacional, promovendo a aplicação de políticas de SI voltadas para as necessidades específicas presentes em cada ambiente ou organização.

Outra justificativa fundamental é que, a pesquisa desenvolvida não impactará apenas no fazer profissional dos bibliotecários, mas também influenciará positivamente no processo de incentivo à boas práticas, trazendo credibilidade e confiabilidade as instituições que adotarem políticas e práticas de SI de forma consciente e metodológica.

O despertar da autora surgiu inicialmente a partir de filmes e séries voltadas para a temática e se consolidou há quatro anos quando iniciou sua graduação em Biblioteconomia. No decorrer do curso esse interesse foi ampliado quando teve a oportunidade de aprofundar seus conhecimentos na disciplina sobre SI, ofertada pelo curso de biblioteconomia e ministrada pela professora Eliane Ferreira da Silva. Adicionalmente, foi possível em certa medida colocar a aprendizagem sobre o assunto em prática por meio de estágios realizados em instituições públicas e privadas, ou seja, foi a partir dos estágios que a autora verificou na prática a atuação do profissional bibliotecário como agente da seguridade informacional.

Além dos aspectos mencionados a pesquisadora corrobora que, todo cidadão precisa estar atento sobre SI, pois para exercer sua cidadania plena e fortalecer a democracia, se torna fundamental ter acesso a informação de qualidade e segura.

Para um melhor encadeamento lógico este trabalho encontra-se dividido em seções. Inicialmente são registrados os elementos referentes a contextualização do assunto, a justificativa e os objetivos. A segunda seção abordará as perspectivas e os principais conceitos voltados para SI, seus pilares e fundamentos, mecanismos físicos e lógicos mais utilizados, os principais códigos maliciosos e seus comparativos. e como a segurança informacional se desenvolveu até o momento que vivemos.

A terceira seção aborda diretamente as organizações e a importância desse tipo de segurança nessas instituições, além disso menciona a engenharia social e as normas e legislações vigentes que versam sobre o assunto. Serão apresentadas cartilhas de Boas práticas neste campo, na qual, o critério de seleção foi o de serem cartilhas emanadas por instituições que se dedicam a pesquisar o assunto.

A quarta seção, está voltada para o profissional bibliotecário e a SI, com vista a apontar as relações existentes nos dois âmbitos. Por fim, as considerações finais são o apanhado geral de tudo que foi apresentado neste trabalho e ainda serão apontadas outras possibilidades de pesquisa e ampliação de conhecimentos na área.

2 A SEGURANÇA DA INFORMAÇÃO E SUAS PERSPECTIVAS

Como exposto anteriormente, a sociedade atual é complexa devido as características informacionais que circundam essa cultura. A sociedade atual denominada de Sociedade da Informação tem como característica básica a informação, que neste contexto, adquire um *status* de recurso ou ativo chave. Outra característica desta sociedade são as formas como se lida com a informação, bem como o excesso de informações colocadas ao alcance das pessoas. Dessa maneira, torna-se necessário, na atualidade, o uso de estratégias para melhor lidar e gerir esse recurso, especialmente no seu acesso, organização e difusão. Sobretudo, se torna necessário o uso de estratégias para se resguardar a informação, e é neste contexto que se apresentam as boas práticas no campo da SI.

Esse campo pode ser definido como uma área do conhecimento que agrega técnicas e práticas científicas, capazes de manter ativos informacionais longe de usuários indevidos/indesejados, e torná-los acessíveis e disponíveis para usuários com permissão e que possibilitam a manutenção da integridade do seu conteúdo.

Em consonância com esta afirmação temos a definição de Sêmola (2003, p. 43) para SI como sendo: “uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade."

Para que haja o desenvolvimento desta área, trabalha-se com a ideia dos três pilares da SI, conforme é também apresentado por Fontes (2006), são eles:

- **Confidencialidade**: propriedade de dar acesso às informações apenas para pessoas autorizadas;
- **Integridade**: relaciona-se com a exatidão da informação, sua continuidade e dos métodos de processamento;
- **Disponibilidade:** é o atributo que garante que os usuários autorizados tenham acesso à informação quando for necessária.

Essa tríade apresenta considerável importância para o campo, pois é a partir dela, por exemplo, que profissionais e organizações podem criar alternativas seguras para lidar com a informação e seus níveis de acesso.

Com a ampliação dos estudos referentes à segurança, notou-se a necessidade de observar e elencar mais características fundamentais para análise de tal temática, dessa forma

desenvolveu-se os princípios da **legalidade**, **auditabilidade** e **não repúdio**. Dessa forma as significações a seguir foram adaptadas a partir do ponto de vista de Fontes (2006), assim temos que:

- **Legalidade:** está voltada para uso da informação dentro da legislação vigente, de acordo com regras, normas e preceitos estipulados por entidades internacionais e nacionais, mas também por normas estabelecidas pela própria organização a partir de seus ideais e princípios;
- **Auditabilidade:** deriva do verbo auditar, é a possibilidade de verificação de quem teve acesso à informação e, principalmente, como foi utilizada;
- **Não-repúdio:** também conhecido como o princípio de **irretratabilidade**, diz respeito à autoria da informação, nesse caso uma pessoa ou entidade não pode negar a autoria da informação.

Ainda, deve-se levar em consideração a promoção da SI, fazendo-se necessário se ater aos três componentes fundamentais para sua efetivação, são eles: **pessoas**, **processos** e **tecnologias.** A partir da percepção de Lino (2016), termos que:

- **Pessoas**: são componentes essenciais para a efetivação da SI, assim capacitar as pessoas para lidarem com a informação é um ponto necessário e que merece atenção, visto que a partir da capacitação os colaboradores desenvolvem a conscientização e passam a exercer boas práticas de maneira natural.
- **Processos**: desenvolver processos padronizados e mapeados para manuseio e utilização da informação são fundamentais para dar continuidade às atividades.
- **Tecnologias**: deve estar alinhado às pessoas, processos e principalmente ao tipo de ativo informacional que precisa ser protegido.

Apesar de ter apresentado esses pilares separadamente, é de suma importância explicitar que tais conceitos precisam trabalhar juntos para uma SI efetiva, assim como no corpo humano, no qual os sistemas com funções independentes, é fundamental o equilíbrio entre todas as suas partes. Um exemplo que pode ser dado é quando se envia um *e-mail* para um colega de trabalho, constando informações sobre o balanço de vendas da empresa, claramente o mecanismo de envio *de e-mail* permite garantir os seis últimos pilares representados até então.

Outros autores também conceituam a SI pautando-se em seus pilares, como Beal (2005, p. 01) que a entende como: “o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade”. Além disso, tem também o olhar de Cristiano Silva Ribeiro que segue basicamente o mesmo fluxo, mas que apresenta a narrativa voltada à seguridade informacional para organizações, conforme fica evidente a seguir:

> A Segurança da Informação é semanticamente a preservação da confidencialidade, integridade, disponibilidade e autenticidade de todas informações e dados indispensáveis para uma organização e/ou indivíduo. Essa preservação passa pelo ambiente físico, tecnológico e gestão de pessoas, tornando assim uma área que estimula o interesse dentro de uma organização que se importa com a qualidade e continuidade dos seus negócios (RIBEIRO, 2016, p. 03).

Outra narrativa verificada com frequência em conceitos voltados para a SI, diz respeito ao suporte que essa informação está inserida, assim temos que: “Segurança da Informação envolve uma série de metodologias que visam assegurar a confidencialidade, a integridade e a disponibilidade dos dados, sejam eles físicos ou virtuais” (SCHULTZ, 2020). Com isso observamos que esta área não se restringe apenas à seguridade das informações presentes em meios digitais, mas que tem a função de resguardar a informação independente do seu suporte.

Além da perspectiva voltada para a tríade da SI, nota-se uma crescente ênfase dessa temática em instituições organizacionais, isso porque a informação se caracteriza como um ativo empresarial, um bem valioso, que necessita ser protegido e gerenciado com qualidade. Para Ferreira (2003, p. 01): “ Segurança da Informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades”. No mesmo raciocínio temos o conceito a seguir:

> A Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada (FONTES, 2006, p. 11).

Ao verificar as falas apresentadas anteriormente, fica explícito algumas coincidências e divergências no que tange a conceituação da temática abordada. Sêmola (2003), Beal (2005) e Ribeiro (2016), projetam a SI com foco voltado para Confidencialidade, Integridade e Disponibilidade, entretanto Sêmola (2003) a conceitua caracterizando os 03 (três) principais pilares da SI (CID) sem citar suas terminologias diretamente, enquanto Beal (2005) cita diretamente a Confidencialidade, Integridade e Disponibilidade, que são os principais pilares

da SI. Já Ribeiro (2016) agrega o fundamento da autenticidade com a continuidade dos negócios e a importância da Gestão de pessoas, nesse caso, apresentando uma pauta voltada as organizações.

Ferreira (2003), por sua vez, perpassa pelas ameaças e benefícios da implementação da SI, considerando a continuidade de negócios e as organizações. Apesar de Fontes (2006) convergir com autor citado anteriormente, observa-se que ele está mais concentrado nas normas, políticas e procedimento em torno da seguridade informacional. Por fim, tem-se a ideia apresentada por Schultz (2020) que elenca a CID, mas também traz que a seguridade informacional é importante para os diversos tipos de suporte, seja físico ou digital.

Apesar de elencar as perspectivas desses autores, não é adequado afirmar que autor X ou Y só se preocupa com determinada narrativa, uma vez que a análise está sendo feita a partir de recortes de conceitos definidos, e não por todo seu conteúdo de trabalhos acadêmicos desenvolvidos na área. Essas perspectivas são detalhadas no Quadro 1.

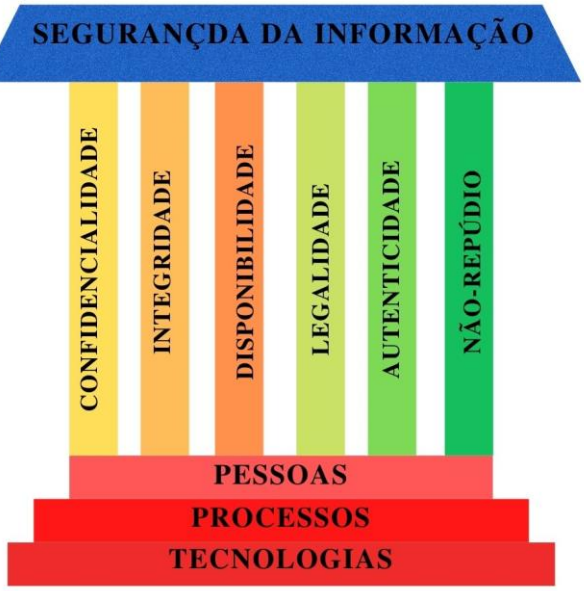
Quadro 1 – Conceitos de SI apresentados com seus respectivos focos

AUTORES	ANO	FOCO DA SI EM:
SÊMOLA, Marcos.	2003	Não cita diretamente os pilares da SI, mas ao ler as entrelinhas fica evidente que está caracterizando a CID.
FERREIRA, Fernando Nicolau Freitas.	2003	Combate às ameaças + organizações + implementação da SI para continuidade dos negócios .
BEAL, Adriana.	2005	Cita claramente a CID.
FONTES, Edison.	2006	Normas, políticas e procedimentos, além do enfoque para alcance da missão de organizações.
RIBEIRO, Cristiano da Silva.	2016	CID + autenticidade + organizações + continuidade de negócios + implementação de Gestão de Pessoas.
SCHUTLTZ, Felix.	2020	CID + diversidade de suportes da informação.

Fonte: Elaborado pela autora (2021).

A imagem a seguir representa a SI e seus pilares principais e sua base de Pessoas, Processos e Tecnologias, apresentados anteriormente:

Figura 1 – Os pilares da Segurança da Informação



Fonte: Elaborado pela autora (2021).

A SI tem como objetivos principais a implantação de procedimentos e normas capazes de resguardar as informações pessoais e organizacionais de pessoas indevidas, mitigar os riscos e as vulnerabilidades com plena divulgação e adoção desses procedimentos, e minimizar o impacto de possíveis incidentes. As **ameaças** são derivadas de ações humanas (acidental ou proposital) ou ambientais, capazes de explorar **vulnerabilidades** em um sistema para obter, corromper ou destruir um ativo informacional. Já as vulnerabilidades podem ser caracterizadas como gargalos ou fraquezas em um sistema de informação. (MARINHO, 2015)[5].

Um exemplo simples para diferenciação desses termos é: quando se tem uma biblioteca física, com materiais informacionais impressos em uma cidade com clima predominantemente chuvoso, mas o prédio não apresenta condições físicas favoráveis, capaz de conter a ameaça chuvosa. Nesse caso, a principal vulnerabilidade seria as goteiras que poderiam ser resolvidas/mitigadas, já a ameaça ambiental está fora do controle humano ou prevencionista. Assim a vulnerabilidade é o problema que não foi cuidado ou previsto com antecedência, para isso temos a Gestão de riscos, que se caracteriza como um estudo profundo das possíveis vulnerabilidades de uma organização, como será visto na segunda sessão deste trabalho.

[5] Disponível em: https://cryptoid.com.br/banco-de-noticias/ameacas-x-riscos-x-vulnerabilidade-o-que-eu-tenho-ver-com-isso/

Para garantir e prover a seguridade das informações utilizam-se técnicas e ferramentas que objetivam implementar os serviços de segurança. Nesse caso, consideram-se seus **mecanismos,** que por sua vez podem ser divididos em **físicos** e **lógicos.**

A primeira categoria está relacionada com barreiras físicas, como cofres, paredes e trancas, estando associado diretamente ao ambiente físico e a privação de pessoas não autorizadas a um determinado ambiente. A segunda refere-se a mecanismos lógicos que impedem o acesso não autorizado à aplicativos e a dados de sistemas, alguns exemplos são:

- Senhas;
- Criptografia;
- Identificação digital;
- *Token*;[6]
- Cópias de segurança – *backups*;
- Registro de tramitações.

Uma vez mencionados, os fundamentos da SI e seus tipos de mecanismos de proteção, é necessário atenção aos fenômenos das ameaças, e como as vulnerabilidades são exploradas a partir de brechas presentes no trio de componentes essenciais Pessoas, Processos e Tecnologias, apresentado anteriormente.

As principais ameaças às informações podem ser classificadas em três tipos, são elas: internas, externas e físicas. No nível de ameaças internas pode-se citar as pessoas e suas relações, que por muitas vezes, de forma intencional ou acidental, colocam em risco as informações. Já as ameaças externas podem ser consideradas como *hackers*[7] e *crackers*[8], que acabam instalando na rede de computadores códigos maliciosos para prejudicar organizações e/ou pessoas. No âmbito das ameaças físicas é possível citar questões causadas por mudanças climáticas ou ambientais, falhas em sistemas devido sua baixa qualidade ou ausência de manutenção, e até mesmo má preservação dos recursos utilizados na gestão da informação.

[6] É uma chave eletrônica capaz de assinar documentos digitais e garantir a autenticidade, não-repudio e permissão de acesso a documentos e informações.

[7] Pessoa com grande conhecimento na internet, profissional da área de Segurança da Informação que é contratado por empresas para verificar as possíveis vulnerabilidades presentes em um sistema de informação. (Privacy Tech, 2020). Disponível em: https://bit.ly/3p00Q36.

[8] Já figura do *cracker*, pauta-se na ideia de quebra (vem do inglês *crack*) dos ideais legais trazidos com a figura do *hacker*, dessa forma entende-se que os *crackers* possuem grande arsenal de conhecimentos na internet, mas os utilizam de má fé, prejudicando usuários das redes de computadores e empresas. (Privacy Tech, 2020). Disponível em: https://bit.ly/3lAq71p.

De acordo com a Fundação Joaquim Nabuco (2020), os códigos maliciosos ou *malwares* são programas desenvolvidos para executar danos as redes e aos sistemas, utilizando brechas ou vulnerabilidades como arma principal. Outras brechas podem ser exploradas para a disseminação dos códigos maliciosos, como o uso de disco removível (*pendrives*), utilização de navegadores vulneráveis para acesso a sites infectados, ou até mesmo pela execução de arquivos contaminados. Ainda sobre os *malwares*, pode-se observar:

> Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques [...]. (FUNDAÇÃO JOAQUIM NABUCO, 2020)[9].

Diante do exposto, fica evidente que os principais objetivos de quem se utiliza de códigos maliciosos é praticar uma atividade ilícita com objetivos escusos e ganhos pessoais. A seguir serão listados os principais *malwares*, seu modus operandi e características principais a partir da perspectiva do site da Fundação Joaquim Nabuco (2020) e da autora.

- **Vírus**: é um trecho de código utilizado para reprogramar um *software* já existente, sua ação é desencadeada e embutida em um *software* comum, ou seja, aparentemente o usuário está utilizando um programa longe de suspeitas, mas que em contrapartida tem traços maliciosos. Além disso, vale salientar, que há várias maneiras desses vírus se propagarem, seja por meio de *e-mail*, *script* ou telefone celular. Nesse caso trata-se da execução de um arquivo que foi infectado;
- ***Worm***: é um programa completo que contém todas as tarefas e funcionalidades para que se possa desempenhar seu papel infeccioso, para agir precisa ser executado pelo usuário. Esse tipo de código geralmente envia cópias de si, replicando-se muito rápido e em rede, deixando o processamento dos computadores bem mais lento. Nesse quesito é a execução explicita do próprio código malicioso;
- ***Bot****:* é um programa malicioso que se comporta como um robô, na qual passa a controlar de maneira remota o computador infectado. O computador controlado remotamente é conhecido como "zumbi", pois perde o controle de suas ações, ou seja, é controlado sem a permissão do usuário. A partir do agrupamento e controle de diversos "computadores

[9] Disponível em: https://www.fundaj.gov.br/index.php/area-de-imprensa/13552-codigos-maliciosos-malware.

zumbis", tem-se o chamado *botnet*, que se caracteriza como uma rede extensa de computadores controlados a partir de um *bot* que se espalhou em rede. Um exemplo bem claro é quando o computador de controle se utiliza dos seus "zumbis" para fazer muitas requisições de acesso à um servidor, assim o servidor que é atacado pelas requisições para de funcionar pela alta demanda e disponibiliza seu serviço, isso se caracteriza por um ataque DDoS (Ataque de negação de serviço);

- ***Trojan horses***: é o *software* que carrega o vírus para o computador, a partir da proposta de um arquivo aparentemente inofensivo, também conhecido como cavalo de Tróia, permite a entrada dos vírus a partir, por exemplo, de vídeos e *softwares* pirateados. Para que o cavalo de Tróia tenha acesso aos computadores é preciso que o usuário permita sua entrada de forma voluntária, dessa forma contar com a conscientização desse usuário é fundamental, pois é seu comportamento nas redes pode colocá-lo em risco. Ademais, ao ser instalado e executado permite a abertura para ataques, como por exemplo o compartilhamento remoto de informações de acesso ao dispositivo infectado;
- ***Spyware***: é um programa espião que monitora as informação e atividades de um sistema e depois as envia para alguém que se interessa pelos dados ou para própria pessoa que instalou o espião no computador vulnerável. Esse tipo de programa também pode ser usado para questões legítimas e legais, como investigações da Polícia, o que vai determinar a possibilidade do uso é se a da vulnerabilidade de computadores tem aparato legal para ser explorada. Existem subdivisões nessa categoria de código malicioso, como o *Keylogger* que permite que o invasor registre tudo que foi digitado no teclado físico e o Screenlogger que armazena a posição do cursor ao fazer cliques, fazendo *prints* ou imagens de congelamento de tela;
- ***Backdoo*r**: é um programa que deixa vulnerabilidades abertas em um sistema permitindo a entrada ou retorno de outros códigos maliciosos para o computador comprometido. Procura se manter discreto para que continue facilitando a entrada de outros *malwares* a partir de brechas ou "portas dos fundos";
- ***Rootkit***: conjunto de programas e técnicas que permitem esconder a presença de um invasor ou outro código malicioso. Os sistemas de defesa acreditam que seja o próprio usuário do computador que está realizando certas atividades, mas na realidade é a presença do *rootkit* que está mascarando as atividades danosas. Se mantém escondido, rouba informações sensíveis, uma vez que suas ações se confundem com as do administrador. As permissões dadas a esse código malicioso são bem consideráveis.

Algumas atitudes e práticas são fundamentais para garantir a segurança de dispositivos contra códigos maliciosos, como por exemplo o letramento digital e a conscientização do usuário, pois são atitudes mais que necessárias no contexto de utilização das redes. Além disso, não fazer uso de programas piratas (cópias de programas não autorizados), fazer uso de um bom antivírus, não utilizar *pen-drives* ou mecanismos de armazenagem externa desconhecidos nos computadores, realizar as atualizações dos programas utilizados (é a partir dessas atualizações que brechas e vulnerabilidades de *softwares* são fechadas), e, por fim, não abrir arquivos duvidosos ou *e-mails* que não se sabe a origem, ou que não sejam esperados.

O quadro a seguir foi desenvolvido pela Fundação Joaquim Nabuco (2020), que indica os 07 (sete) tipos de códigos maliciosos apresentados anteriormente, apontando especificadamente como esses malwares são obtidos, como se instalam e se propagam, e quais danos podem causar ao usuário.

Quadro 2 – Resumo comparativo entre os códigos maliciosos

Códigos Maliciosos							
	Vírus	***Worm***	***Bot***	***Trojan***	***Spyware***	***Backdoor***	***Rootkit***
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por *e-mail*	✓	✓	✓	✓	✓		
Baixado de *sites* na Internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓

Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga:							
Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por *e-mail*		✓	✓				
Não se propaga				✓	✓	✓	✓

Fonte: Fundação Joaquim Nabuco (2020).

2.1 Como a Segurança da Informação se desenvolveu

O processo de assegurar o conteúdo informacional deve ser representado e caracterizado junto com o processo evolutivo do *Homo Sapiens* (-35000 a.C.), visto que é necessário considerar a evolução dos mecanismos de comunicação, a gestão do conhecimento humano, a escrita e o suporte da informação, pois a partir do momento que se tem o registro de informações importantes, nasce a preocupação com a manutenção dessa informação. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020)[10].

[10] Disponível em: https://bit.ly/39UQcBH

Assim, o esboço histórico da SI é indicado a partir dos primeiros registros feitos de entalhes em pedras, por volta de -35000 a.C., e posteriormente com as pinturas rupestres em cavernas e em sítios arqueológicos, por volta -32000 a.C, mostrando as atividades diárias realizadas, representando a fauna e a flora. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020).

Em torno de -3500 a.C., tem-se a escrita cuneiforme dos Sumérios, e nesse ponto é possível observar a necessidade de preservação da informação e do suporte dessa informação, essa passou a ser uma preocupação para a sociedade da época. Tradições orais e aspectos sociais eram registrados como uma maneira de passar esse conhecimento para posteridade. Acredita-se que essa organização e cuidado é derivada da necessidade de preservar a memória dessa civilização, e assim se pode afirmar que quanto mais organizada e bem estabelecida é a sociedade/povo maior será a preocupação com a SI. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020)

Em – 2700 AC, vê-se o desenvolvimento da escrita egípcia, que não se limitou apenas a um sistema gráfico, relacionava o tipo de escrita com a função desempenhada na civilização egípcia, situação econômica e política. Como fica evidente a seguir:

> O desenvolvimento da escrita no Antigo Egito serviu para o conhecimento e a própria sustentação de variadas facetas dessa antiga civilização. Não se restringindo à invenção de um único sistema gráfico, os egípcios foram responsáveis pela existência de três modos diferentes de escrita: a demótica, compreendida por grande parte da população e utilizada para a realização de negócios; a hieroglífica, empregada nas escritas sagradas e na parede dos túmulos; e o hierática, uma versão simplificada do sistema anterior. (SOUSA, [*s. d.*]).[11]

Mais contemporaneamente, tem-se o marco histórico da Guerra de Tróia (-1200 AC), evento que deu origem ao nome de um tipo de vírus já apresentado, o *Trojan*. O nome deve vírus foi dado em referência ao presente dado pelos gregos aos troianos, um grande cavalo para representar a rendição grega. Os troianos receberam o presente e colocaram dentro de suas muralhas, decretaram sua vitória e passaram aquela noite comemorando, entretanto mal sabiam eles que quando dormissem seriam atacados pelos gregos que se organizaram dentro do cavalo de madeira.

Essa história contada ao longo dos tempos foi capaz de mencionar o estrago e os impactos negativos trazidos pela não prevenção e análise de riscos para segurança. O desfecho

[11] Disponível em: https://bit.ly/3zW2kx8

foi o mais trágico possível para os troianos que comemoram antes do tempo e perderam a guerra. Tempos depois tivemos invenções capazes de influenciar todo contexto da informação, comunicação e a preservação. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020)

Por volta de 1450 a.C. com a invenção da prensa de tipos móveis de Gutenberg, foi capaz de aumentar a produção de livros e jornais em escala considerável, uma vez que anteriormente os materiais informacionais eram feitos à mão, assim tornando-os caros, inacessíveis e nem um pouco democráticos. A prensa ainda foi responsável pelo aumento da alfabetização e acesso à leitura de adultos pela Europa, permitiu a ampliação e disseminação do conhecimento científico. Com essa explosão da produção literária surgiu uma nova preocupação para a sociedade, que seria a forma de localizar a informação no meio de tantas outras, e como resguardar e cuidar dos suportes para fazer a informação perdurar. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020).

Outras invenções como o telefone em 1876 por Alexander Graham Bell, a máquina de criptografia Hebern em 1917 e do primeiro computador eletrônico, ENIAC, desenvolvido pelo exército estadunidense em 1946, marcaram a trajetória histórica dos elementos da comunicação e do desenvolvimento tecnológico para a informação. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020).

A partir da década de 1960 o mundo passou a disseminar informações através das redes de informação e comunicação, sendo contextualizado com o surgimento da internet e a globalização mundial das redes de computadores. Em 1964 a IBM lança o primeiro computador multitarefa comercial, o S/360, um *mainframe* (computador de grande porte) na qual foi sucesso de vendas. (HISTÓRIA SEGURANÇA DA INFORMAÇÃO, 2020).

Na década de 1980 ocorreu a ampliação do grupo de usuários de computadores, que anteriormente estavam ligados apenas às instituições universitárias e as forças armadas. A partir desse momento as pessoas poderiam ter acesso ao mundo da internet ao uso de computadores em casa, mas para isso era necessário condições financeiras. Não precisavam se preocupar, por exemplo com a adequação da ventilação dos ambientes que estavam esses computadores, diferentemente das precauções que se tinha ao utilizar os *mainframes*.

Com o esse novo grupo de usuários a necessidade da SI ficou mais eminente e evidente, e nesse ponto começaram a se preocupar com a segurança das informações digitais, visto que o fluxo de trocas informacionais aumentou consideravelmente e anonimidade dessas relações nesse meio de comunicação também.

Nesse contexto, temos a figura do John McAfee, programador britânico que foi um dos pioneiros no desenvolvimento de antivírus para computadores por volta de 1980, anos depois, mais precisamente, em 1987 abriu a McAfee Associates, uma empresa que trabalha diretamente com programas de antivírus. Tal organização é conhecida até os dias atuais por disponibilizar *softwares* de antivírus de maneira gratuita por um determinado tempo ou como avaliativo, dando a possibilidade de o usuário fazer sua assinatura. Atualmente seu fundador não é mais o proprietário, pois se desligou da empresa 1994, segundo Santino (2021).

Os antivírus são desenvolvidos para combater tipos específicos de vírus, assim precisa ser desenvolvido com capacidade combater situações especificas, mas algo claro é que nem sempre os antivírus são desenvolvidos ou atualizados no mesmo passo que os códigos maliciosos e suas ameaças. Dessa forma, não adianta ter um antivírus que não se atualize com frequência e que não tenha credibilidade com os usuários. Por isso a combinação de dois ou mais tipos desse mecanismo de segurança é uma boa opção.

Essa dinamicidade na atualização da tecnologia e avanço de códigos maliciosos e ameaças exigem cada vez mais dos mecanismos e recursos de Segurança da Informação das instituições. Ademais, se faz necessário o desenvolvimento de políticas de Segurança da Informação, capazes de garantir a continuidade de métodos concretos e processos claros, mesmo na ausência de alguém da equipe nas organizações, mas também orientações que possam o direcionar os usuários de rede que não estão ligados a uma instituição, mas que fazem uso das redes de informação.

Ao buscar o precursor ou de fato onde ou quem deu início à temática da seguridade informacional, o que mais se encontra na pesquisa bibliográfica é a apresentação de personagens que ficaram amplamente conhecidos pela quebra da SI, como por exemplo Kevin Mitnick. É ainda corriqueiro encontrar a definição de SI a partir do significado dos termos “segurança” e “informação” separadamente. A situação apresenta-se como um paradoxo, uma vez que a temática se volta para a gestão e resguardo da informação contra ameaças, mas também como registro para as gerações futuras.

A partir do que foi visto é fundamental o investimento em novas tecnologias que auxiliem a promoção de segurança da informação nos quesitos confidencialidade, integridade e disponibilidade. A implementação dessas novas tecnologias ao combate de riscos deve partir de um estudo capaz de identificar as vulnerabilidades, sendo esse um trabalho que deve ser realizado por uma equipe multidisciplinar.

3 A SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

O ativo informacional é um recurso fundamental para as organizações, primeiramente porque é a partir dele que ocorrerá o processo de tomada de decisões e segundamente porque o recurso informação corrobora para a continuidade dos negócios. Assim, manter seguro esse ativo é uma questão de vantagem competitiva, e que deve ser trabalhado nas organizações junto com sua cultura organizacional.

Segundo Silva (2020) o termo cultura organizacional foi introduzido nos anos 1970 na literatura acadêmica dos Estados Unidos por Pettigrew, e vem sendo desenvolvida por grandes empresas pelo mundo. É caracterizada como um conjunto de ideais, crenças, valores e fazeres práticos dos colaboradores em uma instituição, tem intuito norteador de como a empresa trabalha e quais são seus focos. Não tem papel limitador para a instituição, mas sim oferece possibilidade de expansão dentro de suas características principais. Em consonância com esse pensamento:

> Simboliza o conhecimento consensual de normas de condutas em uma organização, expressando os seus valores, ideias e crenças de grande parte dos seus membros. Este consenso manifesta-se dentro da organização através de elementos simbólicos, mitos, rituais, lendas e uma linguagem própria do ambiente, incluindo premiações e punições. São os funcionários responsáveis por transmitir as regras e normas de conduta dentro das organizações. Eles definem e controlam a maneira de se comportarem dentro do ambiente corporativo, composto de culturas e subculturas departamentais. (GUERRA, 2019)[12].

Sobre a vantagem competitiva que o ativo informacional traz, nas organizações podem ser observados que a permanência no mercado depende também diretamente de manter as informações seguras e distantes da concorrência.

> [...] as empresas, de modo geral, buscarem apropriar-se de informações valiosas dos concorrentes para, talvez, obter vantagem competitiva. Para esse fim recorrem à inteligência empresarial e, por vezes, até mesmo, ao uso de meios ilícitos. No cenário atual para permanecer no mercado, é vital que as organizações façam uma gestão abrangente da Segurança da Informação, protegendo estes ativos vitais: os informacionais. (SILVA, 2008 p. 15)

Para uma SI eficaz e eficiente é preciso que as empresas se pautem nos pilares principais apresentados no capítulo anterior, mas que busquem o equilíbrio entre a gestão de

[12] Disponível em: https://bit.ly/39TkW68

pessoas, gestão de processos e de tecnologias, já que não é possível garantir a seguridade informacional sem que esses três elementos convirjam entre si.

Conforme exposto anteriormente, os pilares da SI trazem a tríade das Pessoas, Processos e Tecnologias como elementos fundamentais para análise das práticas e necessidades da aplicação destes preceitos em organizações. Uma vez que se tem bem definido os **processos** de manuseio e utilização da informação, os erros nesse percurso podem ser minimizados consideravelmente. Além disso, considerar a importância dos recursos **tecnológicos** para o combate as vulnerabilidades são de grande relevância, visto o avanço tecnológico dos mais diversos códigos e ataques virtuais. Assim, a Gestão de pessoas nas organizações deve ser considerado para manutenção das atividades, pois além de se caracterizarem como um recurso, as pessoas ainda são valiosas pelas informações que detêm sobre o funcionamento da instituição.

Desse modo, as pessoas e o fator humano merecem alta atenção quando falamos desse tipo de segurança, pois são justamente as pessoas que utilizam os recursos tecnológicos junto com o mapeamento dos processos para dar continuidade as atividades de uma empresa, assim o processo de conscientização voltado para as pessoas precisa ser bem desenvolvido, pois esse grupo é considerado o elo mais fraco da SI.

O cuidado deve se estender aos colaboradores diretos e aos indiretos (fornecedores, prestadores de serviço e consultores). Assim, corroborando para o processo de conscientização de todas as pessoas que fazem parte de fato de uma instituição, minimizará falhas advindas do elo mais fraco da SI. Esse processo de desenvolver a atenção e a concepção de colaboradores para essa temática pode ser fomentada com o uso de palestras, utilização de filmes e de documentários que versam sobre a SI e principalmente o uso de exemplos práticos e diários com o qual o colaborador pode se deparar, e como isso pode impactar a vida do profissional e principalmente da empresa.

Atualmente, quando o colaborador entra na empresa, recebe treinamento voltado para SI e assina um contrato que dimensionará as responsabilidades dele perante as informações que está tendo acesso. Esse é um contrato de responsabilidade informacional/ou termo de compromisso, garantindo o direito da empresa à informação manuseada e o profissional que recebeu treinamento adequado para lidar com os dados sensíveis. Esse deve ser o ciclo básico de contratação em empresas que levam a sério o seu ativo informacional.

Ainda sobre o termo de compromisso Fontes (2005) explica o objetivo dessa formalização e o que deve conter nesse documento:

> […] explicar […]as responsabilidades perante a organização. Você realizara seus serviços profissionais sabendo como a organização deseja que você trate informação armazenada nada nos recursos de tecnologia e no ambiente convencional. Eventualmente, também serão descritas as penalidades, caso as normas e os regulamentos não sejam cumpridos. Todas essas questões estão de acordo com a lei com as leis vigentes do país e com um organismo maior na qual a organização está inserida (grupo empresarial ou segmento de negócio). (FONTES, 2015 p. 20)

A seguir destaca-se uma citação que trabalha com a falsa ideia que geralmente os colaboradores tem de que, a informação que ele tem acesso enquanto trabalha em algum lugar pertence a ele, entretanto engana-se, pois a informação que ele utiliza para desempenhar suas atividades caracteriza-se como recurso da instituição.

> É muito comum o ex-funcionário ter acesso a banco de dados, cadastro de clientes e fornecedores, dados pessoais sensíveis, planos estratégicos de negócios, segredos comerciais e profissionais, bem como demais confiança que exercia previamente. Na rotina de trabalho, ao participar do desenvolvimento dos negócios ou ao ter acesso a este fluxo privilegiado de informações, muitas pessoas têm a falsa crença de que estas informações também lhe pertencem, o que é um engano, e acabam armazenando consigo todo esse histórico, levando para si próprio uma cópia desses dados, sem qualquer autorização. E assim, repassam isso para uma empresa concorrente ou utilizam na construção de seu próprio negócio autônomo. (TRUZZI, 2019)[13].

Não existe uma "receita de bolo" para a SI ser implementada nas organizações, porém temos algumas boas práticas que podem ser adaptadas de acordo com o tipo de instituição, com sua cultura organizacional e principalmente com o tipo de informação que precisa ser resguardada. Silva (2008) enfatiza a importância do uso de chaves pessoais, uso de senha em todos os dispositivos possíveis, manter a mesa de trabalho organizada, não expor informações da empresa e utilizar com sabedoria os *e-mails*, são boas práticas de SI em organizações. Convergindo com as ideias de Silva (2008), Beal (2005), vai além e aponta mais algumas diretrizes para minimizar os riscos que podem ser gerados pelo fator humano nas organizações:

- Análise minuciosa do histórico profissional do colaborador que será contratado, independente de qual cargo ou nível hierárquico será alocado;
- Os colaboradores precisam estar cientes das normas e da política de SI da instituição, de preferência na contratação. Além disso, ler e concordar com o termo de

[13] Disponível em: https://bit.ly/3FawMY8

conhecimento e responsabilidade, assim garantindo a aplicação desses conhecimentos nas atividades que desempenhará na instituição;

- Manter os funcionários em observação, com acompanhamento de um gerente qualificado que possa observar as atitudes e detectar situações de risco;
- Dividir as responsabilidades de um determinado setor entre diferentes colaboradores, dessa forma não se tem um único conhecedor do processo em determinado setor;
- Treinar todos os funcionários da empresa para que tenham consciência da importância de assegurar as informações da instituição;
- Punir colaboradores que violem as regras, desde que eles estejam cientes das normas e padrões da empresa. Essa parte é voltada para os mecanismos de controle;
- O processo de demissão deve ser seguro e vetar de imediato o acesso do funcionário demitido aos ativos informacionais empresariais.

Algo fundamental para as instituições é a realização da análise de riscos de SI, da mesma forma que se realiza a análise SWOT - Strengths (Forças), Weaknesses (Fraquezas), Opportunities (Oportunidades) e Threats (Ameaças). Tradicionalmente utilizada para identificar as forças, fraquezas, oportunidades e ameaças de uma organização. A análise de riscos é de grande valia para instituição, pois verifica os possíveis riscos para a segurança informacional, no qual a empresa pode estar exposta.

Assim como na análise SWOT, a avaliação dos riscos é vista sob o cenário interno e externo do empreendimento, e a partir do resultado será traçado estratégias capazes de mudar o contexto de risco e preocupação e assim a análise de riscos é utilizada no processo de tomada de decisões. Os principais objetivos da Gestão da análise de riscos, conforme Silva (2021)[14], são:

- Identificar e mitigar em ameaças em potencial à segurança de Tecnologia da Informação e a probabilidade de que se concretizem;
- Identificar o valor dos recursos e estruturas, inclusive seu valor indireto, caso sejam danificados violados;
- Usar essa análise de valores para identificar as ações mais adequadas para correção das fragilidades;

[14] Disponível em: https://bit.ly/2Ww04yX

- Definir e gerenciar uma política de gestão de riscos de segurança;
- Definir processos para aprimorar o gerenciamento de risco na empresa;
- Garantir a melhoria contínua de toda a infraestrutura de segurança da empresa.

Para alcançar os objetivos descritos anteriormente é necessário o uso de recursos financeiro, de pessoal e de tempo. Muitas vezes, o recurso financeiro desprendido para ajudar na concretização da SI é visto pela organização e pelo gestor como um gasto, entretanto desprender recursos voltados para segurança se caracteriza como um investimento, pois a partir do momento que empresa sofre algum ataque às suas informações, automaticamente terá danos financeiros e principalmente danos em relação a sua credibilidade no mercado. Nesse contexto, temos que é mais benéfico e mais barato investir nesse tipo de seguridade do que lidar com as consequências de uma má gestão da informação, uma vez que os prejuízos para empresa vão bem além de prejuízos financeiros, conforme descreve Santino (2016):

> Enfim, investir em Segurança da Informação é, com certeza, uma estratégia que impacta diretamente nos resultados dos negócios, ao evitar perdas financeiras e problemas associados à reputação da marca e de seus serviços os quais, muitas vezes, são irreversíveis. No entanto, investir só em tecnologia não basta. É preciso envolver pessoas, parceiros e clientes e ter processos para enfrentar de forma inteligente a estratégia dos cibercriminosos. (SANTINO, 2016)[15]

Como se pode perceber são variadas as vantagens da aplicação dos preceitos da SI. Percebe-se que não se trata meramente de instalar um processo mecânico nas organizações, ao contrário, se reveste em uma estratégia holística para a empresa que envolve desde a informação, ativos-chave, tecnologias e o fator humano, essenciais para o funcionamento das organizações. Mas, para além destes elementos discutidos, faz-se necessário abordar outros impactos advindos da complexidade da SI. Em seguida, serão abordados assuntos relativos a Engenharia Social.

3.1 A arte da persuasão: Engenharia social

A engenharia social caracteriza-se como um grupo de procedimentos e práticas de alta persuasão, capazes de fazer as vítimas passarem informações confidenciais de uma empresa ou organização sem darem conta de tal situação. Essas práticas são utilizadas para explorar o elo

[15]Disponível em: https://bit.ly/3im850Q

mais fraco da SI, mais precisamente o fator humano. Com isso o indivíduo golpista se aproveita das informações que podem ser obtidas através de um colaborador da empresa e as utiliza de maneira ilícita e criminosa. Os engenheiros sociais usam a enganação e/ou exploração da confiança das pessoas. Em convergência ao que foi apresentado conceitua-se o que seria engenharia social para Fontes (2015):

> Chamamos de engenharia social o 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. É a velha conversa do malandro! (FONTES, 2015, p. 120)

Esse tipo de ataque pode ocorrer de maneira presencial, a partir de contato físico e socialização direta entre o engenheiro e a vítima, mas também pode ocorrer pelas mídias digitais. A técnica de exploração digital chamada de *phishing*, consiste basicamente em enganar usuários para obter informações confidenciais, como dígitos de um cartão, *login* e senha. A expressão *phishing* vem do inglês e significa pescaria ou lançar o anzol, na realidade o engenheiro social lança por meio de *e-mails* ou mensagens nas redes uma isca, assim a vítima ao não observar o que está escrito acaba fornecendo informações para o engenheiro, e não para empresa ou remetente que ela achava que estava respondendo. Desse modo, observar o conteúdo dos *e-mails*, verificar se há erros ortográficos e, muitas vezes, até entrar em contato com a possível empresa que envio o *e-mail* são mecanismos para manter a SI contra a engenharia social.

O responsável por esses ataques pode retirar informações físicas, virtuais, psicológicas e comportamentais apoiando-se em práticas simples de manipulação. O engenheiro social fala com conhecimento sobre determinados assuntos, cita setores de uma organização e ainda se apropria da linguagem e da cultura organizacional daquele ambiente, além disso o fraudador passa confiança inicialmente para a vítima, pode até ajudá-la a resolver um problema que ele mesmo criou só para ampliar o vínculo de confiança e ter acesso, por exemplo, ao seu computador ou anotações em sua mesa.

O engenheiro social não é considerado um profissional, mas sim um indivíduo que se apropria de técnicas para persuadir grupos de pessoas, nem sempre indefesos ou ignorantes no assunto. A ideia de um engenheiro leva as pessoas a acreditarem que os ataques serão sempre bem planejados e com alta qualidade, mas não é bem isso, alguns ataques não são tão bem elaborados, apresenta erros ortográficos e as vezes as informações que o criminoso tem sobre a vítima não são suficientes para aplicação do golpe com maestria.

Mesmo com uma qualidade duvidosa, dificilmente a vítima sabe que está sendo enganada, as vezes por falta de atenção, por pressa e falta de análise crítica sobre a situação de interação entre ela e o engenheiro social. Assim como apresentado pelo site *We live Security* (2016), pode-se inferir sobre a atuação do engenheiro social:

> O aspecto mais preocupante sobre ataques desse tipo é que não há aviso imediato, não há sinal claro de que você está sendo atacado ou que seu computador foi infectado[...]. Na maioria das vezes, os criminosos realizam seus ataques, roubam os dados que procuram e depois desaparecem. E se for roubo de dados, você provavelmente nunca descobrirá a infecção, muito menos se seus dados estiverem sendo vendidos ilegalmente[...]. (WE LIVE SECURITY, 2016)[16].

A partir do que foi apresentado, fica evidente a necessidade de gerir adequadamente as pessoas e os recursos de uma empresa, principalmente o ativo informacional, com isso é necessário que empresas se adaptem e cumpram as normas, legislações e políticas de SI. Para garantir o equilíbrio entre as atividades da organização e o aporte teórico sobre essa temática é importante que a instituição esteja em *compliance*, que é mais especificadamente uma maneira de garantir que as políticas e normas internas e externas estejam sendo aplicadas nas atividades diárias, assim como apontado a seguir:

> Sendo assim, o *compliance* é uma maneira de garantir que a política de segurança está sendo cumprida. Isso permite mais tranquilidade para o trabalho e para as atividades da empresa como um todo. Afinal, um bom trabalho de *compliance* deve ter como aliada uma solução de segurança digital que assegure a proteção dos dados corporativos. (FSENSE, [202-])[17]

A seguir serão apresentados algumas normas, legislação e cartilhas de SI que devem ser utilizadas para embasamento das práticas e para aplicação do *compliance*.

3.2 Normas técnicas voltadas à Segurança da Informação

Para concretizar as necessidades de segurança informacional, o Departamento de Comércio e Industria do Reino Unido (DTI), de forma pioneira, criou o Centro de Segurança da Informação (CCSC) para tratar de questões relacionadas a informação, e dentre elas desenvolveram uma norma específica sobre SI para as organizações daquele país. A partir do

[16] Disponível em: https://bit.ly/3D2URy9
[17] Disponível em: https://fsense.com/pt/qual-e-a-importancia-do-compliance-para-a-seguranca-da-informacao/

ano de 1989 alguns documentos que tratavam sobre o assunto foram criados de maneira preliminar, em 1995 foi concretizada pela CCSC a primeira parte da British Standard 7799 (BS7799), seguida da segunda parte no ano de 1998, ambas para consulta pública.

O BS7799 foi a primeira norma a trazer diversos tópicos sobre a área desse tipo de segurança, motivo pelo qual, após dois anos de sugestões e alterações, teve *status* internacional reconhecido, tornando-se a norma ISO/IEC 17799:2000. No Brasil, a referida norma foi devidamente traduzida e homologada pela ABNT em 2001, sendo denominada NBR ISO/IEC 17.799. Ela traz em seu corpo um aparato mais completo e extenso, tratando na sua introdução de conceitos primários (o que é informação) para nortear os seus usuários, relação de significados de termos na língua inglesa, além de parâmetros para estabelecer requisitos de SI, avaliação de riscos e seleção de controles.

Nesse sentido a norma também traz alguns princípios básicos para a gestão da segurança informacional, assim como tipos de controles baseados em requisitos legais e em boas práticas de segurança. Tais parâmetros podem ser aplicados em grande parte das organizações, sejam elas públicas ou privadas, devido ao seu conteúdo generalista.

A norma, atualmente, encontra-se na sua segunda edição (NBR ISO/IEC 17.99:2005) e não terá mais atualizações, pois em 2007 foi incorporada à NBR ISO/IEC 27002, fazendo parte da família NBR 27.000. O princípio dessa família foi dado pela ISO/IEC 27000, homologada no Brasil, e após poucos anos tal norma constituiu uma grande família que trata sobre a Gestão de SI, sendo composta atualmente de 45 (quarenta e cinco) normas sobre o tema. As mais conhecidas para uso como referência para a criação de Políticas e Normas para a segurança de empresas são as normas NBR 27000, NBR 27001 e NBR 27002, que tratam respectivamente de: informações básicas sobre as normas da série; normas que definem requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) em uma organização e Certificados para Empresas; código de práticas e controles que auxiliam a implantação de um SGSI e a Certificação Profissional.

A família ISO/IEC 27000, portanto, é ampla em seu escopo, e abrange múltiplas questões, desde privacidade, confidencialidade e Tecnologias da Informação, até assuntos que envolvem *cibersegurança*. Ela pode ser aplicada aos mais diversos tipos de organizações, independentemente do tamanho e de sua cultura organizacional.

Nesse contexto, todas as organizações, com o auxílio das normas técnicas, políticas e sistemas de SI, são encorajadas a avaliar constantemente os riscos de suas informações e, caso necessário, reestruturar os seus controles de segurança, de acordo com as novas exigências para

a manutenção da segurança almejada. O Brasil se junta à países que já tinham legislações especificas sobre a temática, mas agora com uma legislação específica e muito mais precisa sobre como empresas precisam se portar perante as informações de clientes e seus colaboradores. Com isso, temos a Lei Geral de proteção de dados, que será abordada mais claramente a seguir.

3.2.1 Lei Geral de Proteção de Dados

A Lei nº 13.709, de 14 de agosto de 2018, ou Lei Geral de Proteção de Dados tem objetivo de trazer mais privacidade para as informações de titulares em relação ao seu manuseio, armazenamento, compartilhamento e tratamento das informações vinculadas ao titular. As instituições ou empresas que atuam no Brasil, sejam de pequeno, médio ou grande porte que trabalhem e lidem com as informações de clientes e colaboradores precisam deixar claro para os titulares ou portadores, com quem é compartilhado as informações referentes à essas pessoas, como são compartilhadas, como resguardam essa informação e ainda dá a possibilidade de controle dessa informação ao titular como é de direito.

Nesse contexto vale salientar que empresas e organizações públicas e privadas devem trabalhar de acordo com os alinhamentos da LGPD, assim há duas maneiras distintas de pensar na privacidade de informações. A primeira está vinculada a situação de transparência dos dados que as instituições públicas precisam exercer e ainda sim resguardar certos dados, e a segunda vincula-se com a ideia direta de privacidade quando se trabalha com a necessidade de consentimento do titular, e para que as empresas possam tratar os dados e os utilizá-los. Tal situação é pontuada a seguir:

> Conforme já exposto, a LGPD irá valer tanto para o setor privado quanto para o setor público, e aqui podemos verificar a colisão de dois princípios: a necessidade de consentimento do titular quanto ao tratamento e coleta de seus dados pessoais (privacidade) e a transparência do poder público, que deve garantir a divulgação das informações relevantes aos cidadãos (publicidade).O estado de direito social, que preza pela transparência e democracia das informações, também deve respeito a privacidade do sujeito, e ambas características devem coexistir a fim de afastarmos qualquer totalitarismo estatal. A LGPD, em seu artigo 4º, excetua a aplicação da lei em casos com fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e infração penal. (PANEK, 2019, p.21)

A LGPD foi desenvolvida em torno de 04 (quatro) elementos ou figuras principais, assim temos o **dado** que é a informação que diz respeito a alguém, o **titular do dado** é aquele a quem a informação se refere, o **controlador dos dados** é quem diz se os dados vão ser coletados e como serão processados, e **operador de dados** que vai executar o que for decidido pelo controlador de dados.

Essa legislação foca sobre como as empresas fazem o tratamento dos dados do titular, desde o momento da sua coleta até o seu descarte ou reutilização em sistemas informatizados ou não. Nesse caso existe a gestão de SI em todas as fases e ciclos da informação, trabalhados de maneira específica com suas particularidades. Ademais, versa que o titular deve saber como seus dados serão tratados pelas instituições, e, principalmente, consentir que seja realizado determinado tratamento e ainda tem que ser explicado ao titular qual a finalidade da utilização dos seus dados.

A lei de proteção de dados conta com penalidades para as empresas que não estiverem de acordo com o que é apresentado, que vão desde advertências com prazo para regularização dos erros identificados até multas no valor de até R$ 50 milhões de reais por infração, ou seja, as empresas que não estiverem alinhadas com a LGPD terão sua credibilidade, a segurança das informações e o financeiro atingidos. Assim como apresentado a seguir:

> A aplicação das sanções e penalidades pela ANPD deverão levar em consideração os parâmetros fixados em lei (art. 52º, §1º)21 e vão de advertência até multas com limite de R$ 50.000.000,00 (cinquenta milhões de reais). Verifique-se que as Empresas deverão tratar com seriedade a conformidade com a LGPD, sempre atentando aos seus princípios norteadores, sob o risco de sofrerem graves punições. (PANEK, 2019, p.25)

A Autoridade Nacional de Proteção de Dados (ANPD), será a entidade responsável por essa fiscalização e poderá solicitar relatórios institucionais sobre risco de privacidade e os documentos para verificação de como está a gestão da SI em determinada organização. (CUNHA, 2021). Em seguida serão apontadas algumas cartilhas de boas práticas no campo, que tem como finalidade auxiliar empresas e colaboradores em uma gestão eficiente dos ativos informacionais, presando por sua segurança.

3.2.2 Cartilhas de boas práticas em Segurança da Informação

Além das disposições legais e normas, algumas instituições de caráter público disponibilizam cartilhas sobre boas práticas de SI, a serem aplicadas seja no meio físico ou digital, a fim de proteger as informações disponibilizadas na organização e conscientizar os seus colaboradores da necessidade de se aplicar procedimentos conscientes ao lidar com a informação em diferentes momentos do seu ciclo de vida.

Esse material é produzido com linguagem simples, clara e de fácil entendimento, algumas desenvolvidas para o público infantil trazem as informações como estórias ou histórias em quadrinhos. Para o contexto da conscientização dos colaboradores de uma empresa, o ideal é que a cartilha seja desenvolvida pela própria empresa ou que tinha sido elaborada por corporações afins no mercado de atuação. Por exemplo, em uma empresa voltada para área do direito é mais sensato adotar cartilhas desenvolvidas por órgãos dessa área, como a do Superior Tribunal de Justiça, pela familiaridade de termos e principalmente pelo alinhamento de temáticas.

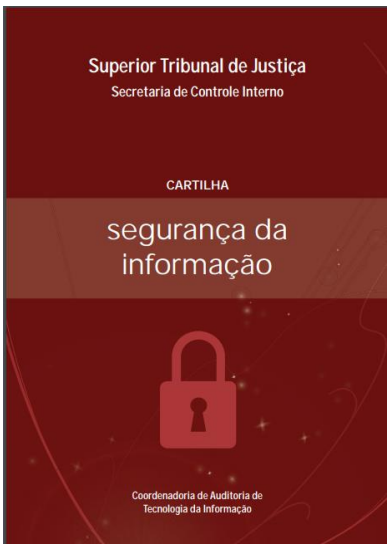
A seguir serão apresentadas três cartilhas que possuem destaque nacional e que podem contribuir para a desenvolvimento e conscientização de colaboradores em empresa com atividades afins, são elas:

1. **Cartilha do Superior Tribunal de Justiça (STJ)**[18]

Tal cartilha traz os pontos principais da SI, seus pilares, a importância da preservação da informação, classificação e políticas da informação. Um ponto que merece destaque é quando a cartilha trabalha com a importância de que todas as pessoas que fazem parte da instituição estarem inclusas e presentes no processo de seguridade informacional, dessa forma a cartilha apresenta os papeis de ministros, servidores, estagiários e dos terceirizados. Ademais, foi apresentado de maneira breve a engenharia social e seu impacto nas instituições, e para finalizar elencaram 10 (dez) dicas de boas práticas em SI.

[18] Disponível em: https://bit.ly/3BPTz9i

Figura 2 – Cartilha sobre Segurança da Informação do STJ



Fonte: Superior Tribunal de Justiça – site [2014]

2. Cartilha do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[19]

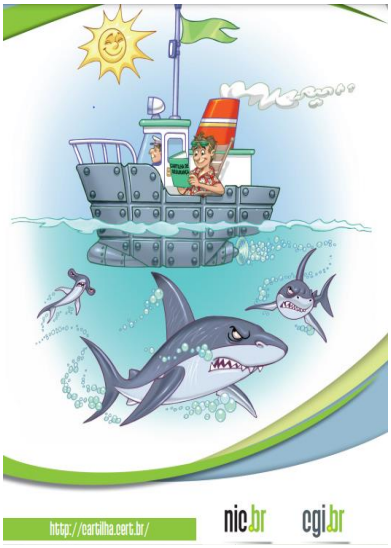
Caracteriza-se como uma das cartilhas mais completas, pela quantidade de conteúdo apresentado, provavelmente seja pela qualificação da empresa que a desenvolveu. Começou a ser desenvolvida em 2000 e sua versão mais recente foi lançada em 2012. Trata-se de uma cartilha dinâmica, pois considera novos riscos e novas perspectivas que passam a ser incluídos em uma nova versão. Ela é dividida em fascículos e no site o acesso pode ser feito de maneira individualizada, fascículo por fascículo, ou se for de preferência tem se o conteúdo total em livro digital, que também está no site principal.

Como essa cartilha está voltada para a SI em ambiente digital, em sua grande parte, o seu diferencial é a abordagem dessa temática voltada para dispositivos móveis, privacidade nas

[19] Disponível em: https://bit.ly/3FbJkOL

redes sociais e segurança de redes. Entretanto, também aborda questões fundamentais como os pilares da SI, golpes mais utilizados no meio digital e traz dicas de como fazer a prevenção. Essa cartilha pode ser utilizada para orientar todo e qualquer usuário da informação no meio digital, sejam colaboradores de empresas ou até mesmo o usuário comum/indivíduo. Além disso, o site conta com *links* para a plataforma *YouTube*, com vídeos explicativos sobre temas específicos abordados pelo fascículo temático. Dessa forma, além de ter o conteúdo escrito, também possui outras narrativas sobre a temática abordada, a partir de falas também de especialistas na área.

Figura 3 – Cartilha sobre Segurança da Informação do CERT.br



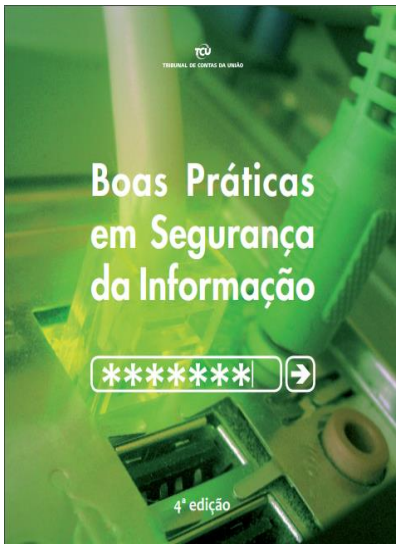
Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – site (2012)

3. Cartilha do Tribunal de Contas da União (TCU)[20]

A cartilha do TCU é focalizada na aplicação das políticas de SI e nos controles de acesso lógico. O diferencial do material é o enfoque dado para o plano de continuidade de negócios, na qual tem o objetivo de desenvolver técnicas e procedimentos para serem adotados por instituições que se deparam com problemas que comprometem o andamento normal dos processos. Aborda também a importância da análise de risco em SI, para que os processos da organização não sejam atingidos e muito menos a sua credibilidade no mercado.

[20] Disponível em: https://bit.ly/3iXzUNE

Figura 4 – Cartilha sobre Segurança da Informação do TCU



Fonte: Tribunal de Contas da União – site (2012)

Com o uso das cartilhas é possível disseminar o conteúdo técnico da legislação e normas vigentes, e principalmente as boas práticas de uso e de SI para colaboradores de empresas e usuários comuns da rede. Essas cartilhas podem ser utilizadas em treinamentos nas instituições, em campanhas conscientizadoras ou até mesmo para construção de novas cartilhas de boas práticas voltadas para instituições específicas.

3.2.3 Políticas de Segurança da Informação

As políticas voltadas para seguridade informacional devem levar em consideração a formalização de regras e legislações vigentes e o fator humano dentro de uma organização. Elas devem apresentar uma implementação realista, linguagem clara e a definição das responsabilidades dos colaboradores em relação SI dos dados utilizados. Tais políticas se alinham diretamente com as questões da cultura organizacional e com as práticas realizadas, sendo consideradas como um documento capaz de orientar as atividades de uma instituição.

Campos (2007, p. 131 pondera que: “atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma.”

Isso fica evidente uma vez que, as instituições compreenderam que a PSI ajuda no processo para garantir o resguardo informacional, contribuindo para diminuição de ameaças, colaborando para que a empresa não perca a credibilidade com seus clientes e capital financeiro.

As políticas de SI devem ser implementadas e desenvolvidas por uma equipe multidisciplinar compostas por juristas, profissionais das tecnologias da informação e principalmente profissionais da informação, como bibliotecários. Assim ao desenvolver uma política para determinada empresa será visto os mais distintos ângulos da informação e da proteção de dados. Dessa forma, torna-se relevante abordar o papel do profissional bibliotecário no contexto da SI, quais suas principais contribuições e perspectivas, na sessão a seguir serão trabalhados esses aspectos. Em seguida será repostado também ao aspecto das inter-relações possíveis entre a SI e o profissional bibliotecário.

4 O PROFISSIONAL BIBLIOTECÁRIO E A SEGURANÇA DA INFORMAÇÃO

O profissional bibliotecário caracteriza-se como um profissional capaz de lidar com a informação como elemento central e todos os aspectos relacionados a este recurso. Sua atuação incide desde localização, acesso, organização, tratamento e a elaboração de estratégias de controle, segurança e disseminação estratégica em ambientes variados, desde os mais formais, como as unidades de informação, até ambientes distintos em organizações de objetivos variados.

Conforme avança o tempo, surgem novas formas de se trabalhar a informação, pois se apresenta em formatos variados e complexos e em diferentes suportes. O fazer profissional é reflexo do tempo em que se circunscreve, é impactado pelos novos processos e sobretudo pelas tecnologias que surgem. Esse ponto de partida leva a pensar sobre as relações e possibilidades de ampliação desta atuação que com o tempo, se transforma por meio de mudanças paradigmáticas.

Inicialmente a função primordial do bibliotecário era apenas de guardião dos materiais informacionais, posteriormente passando a ser agente disseminador da informação. Esse profissional está atrelado com o emprego das novas tecnologias da informação presentes pelo mundo. Conforme apresentado por Pinto (2005 *apud* FIGUEIREDO; SOUZA, 2007, p. 11)

> O campo da Biblioteconomia, mais do que qualquer outro, é atingido pelas mudanças que afetam a sociedade contemporânea. Estas mudanças estão relacionadas, principalmente, às grandes transformações que interferem significativamente na vida da sociedade atual, quais sejam: o acelerado desenvolvimento científico e tecnológico, a globalização e as chamadas Novas Tecnologias da Informação e da Comunicação Novas Tecnologias de Informação e Comunicação.

Conforme exposto, a atuação deste profissional pode ser realizada desde ambientes como centros de informação, bibliotecas, museus e arquivos, ou qualquer atividade que se volta para gestão e mediação consciente de materiais informacionais.

No Brasil o bibliotecário tem seu cargo e função regidos pelas Leis Nº 4.084/1962 e Nº 9.674/1998, na qual regulamentam seu exercício. Para desempenhar as suas funções se faz necessário um diploma de bacharel em Biblioteconomia, emanado por uma instituição de ensino reconhecida pelo Ministério de Educação e Cultura (MEC). Além

disso, se faz necessário a emissão de uma carteira proveniente do Conselho Regional de Biblioteconomia (CRB) que atesta o registro perante a entidade de classe profissional. Sobral (2012), ainda pondera que:

> De acordo com a Classificação Brasileira de Ocupações – CBO – o Bibliotecário pertence à família dos profissionais da informação. Suas principais atribuições são: disponibilizar a informação em qualquer suporte; gerenciar unidades como bibliotecas, centros de informação e correlatos, além de redes e sistemas de informação; tratar tecnicamente e desenvolver recursos informacionais; disseminar informação com objetivo de facilitar o acesso e geração do conhecimento; desenvolver estudos e pesquisas; realizar difusão cultural e desenvolver ações educativas. Para cumprir um trabalho de tamanha responsabilidade, é necessário, antes de tudo, **garantir a segurança da informação gerenciada, que não se trata apenas do conceito usual que temos de segurança**, que é garantir apenas que algo não seja perdido ou que caia nas mãos erradas. **A segurança da informação é também garantir que a informação esteja disponível quando necessária, e que se possa garantir a sua integridade**. (SOBRAL, 2012, grifo da autora)[21]

A passagem acima deixa evidente que uma das responsabilidades do bibliotecário é trabalhar o ciclo da informação e para além disso, garantir que este recurso esteja disponível e sobretudo seguro, alinhando com os princípios da CID. A seguridade informacional deve ser uma preocupação da alta gestão e do profissional bibliotecário, que deve cuidar da gestão da informação em unidades de informação e no contexto de instituições e empresas. Quando não há sensibilização dos gestores sobre esse tipo de segurança, ocorre um processo de vulnerabilidade e com isso as organizações estão sujeitas a graves problemas. Por isso se faz importante que o profissional bibliotecário, junto com uma equipe multidisciplinar, trabalhe para mitigar os riscos de segurança informacional.

Entretanto, para uma atuação do bibliotecário efetiva no mercado, é importante que esse profissional tenha um perfil caracterizado por boas relações interpessoais, flexibilidade, planejamento, agilidade, criatividade, inovação, domínio quando necessário de processos de gestão da informação e do conhecimento bem como gestão da SI.

Essas características nem sempre são apreendidas e absorvidas no primeiro ciclo de formação do profissional, assim é de bom tom a continuidade da aprendizagem, com vistas ao melhor desempenho na prática profissional voltada para SI, e assim lidar com

[21] Disponível em: http://biblioo.info/segurancada-informação

alta volatilidade dos saberes e das necessidades do mercado de trabalho. Isso pode ser corroborado por Faria *et al* (2005, apud FIGUEIREDO; SOUZA, 2007, p.14)

> [...] o profissional deve ter educação continuada. O banco acadêmico dá a formação do momento e o bom profissional tem que continuar estudando e se atualizando, pois os processos são os mesmos, o que mudou são as formas de execução com os novos suportes de armazenagem da informação. Os currículos acompanham determinada tendência da época.

Então, como se percebe tanto a sociedade quanto o mercado de trabalho estão em constante evolução. E para que o profissional possa estar em consonância com a nova realidade, precisa acompanhar as mudanças em curso da melhor forma possível, seja por meio da educação continuada ou por um comportamento prospectivo no ambiente em que atua. As organizações ou instituições necessitam no momento, de um corpo profissional que consiga lidar com as demandas das normas e legislações voltadas para SI, e com isso pode-se incluir as necessidades de adequação voltadas para a LGPD. Além disso, é importante equilibrar os elementos relativos à gestão das pessoas, processos e tecnologias.

É nesse contexto que se insere a figura do profissional da informação com potencial de atuação na área de SI. Assim o bibliotecário deve garantir que a informação esteja disponível apenas para as pessoas que precisam dela para exercer suas atividades profissionais na organização, e ainda que as informações manuseadas sejam utilizadas de maneira segura e consciente, trabalhando com os colaboradores a ideia da responsabilidade individual, mas que impacta na segurança informacional do coletivo.

Esse profissional bibliotecário poderá desenvolver atividades voltadas para a gestão da SI, trabalhando como gerente nessa temática ou até mesmo compondo um grupo multidisciplinar com a finalidade de assegurar as informações. Ainda poderá ajudar no processo de decisão sobre os níveis de permissão de acesso de colaboradores que utilizam os sistemas informatizados de uma empresa para exercerem suas funções.

Além das atribuições para gerir as informações e garantir sua segurança, o bibliotecário também pode desenvolver outras atividades, com isso a autora pensou em algumas atividades, fazeres e contribuições práticos que podem ser realizados por esse profissional. Uma das primeiras possibilidades pensadas foi a de o bibliotecário dar suporte ou realizar o processo de treinamento de colaboradores, os preparando para compreender as normas e legislações vigentes de SI, adotadas pela organização

fortalecendo e alinhando assim as necessidades normativas da empresa com a capacitação profissional e instrutiva de seus colaboradores.

Além disso, O profissional bibliotecário tem em sua formação intrínseca as atribuições para realizar pesquisas qualificadas e confiáveis, assim poderá atuar em busca de novas tecnologias que possam ser implementadas nas empresas, auxiliando na diminuição de gargalos da SI e trabalhando em busca de novas técnicas que possam também impactar a prática diária dos colaboradores e assim contribuir para o resguardo informacional. Ainda sobre esse quesito o agente bibliotecário poderá colaborar na análise e desenvolvimento de artifícios que propiciem o melhoramento dos processos realizados pelos colaboradores, desse modo auxiliando com mecanismos para garantir a SI de clientes.

Outro ponto de contribuição do bibliotecário é no processo de organização da informação dos clientes nos sistemas de busca, para que as informações sejam encontradas pelos colaboradores no processo de recuperação é fundamental que estejam organizadas, classificadas e bem descritas. Dessa forma, perder informações, porque não foram bem classificadas e descritas, é inadmissível para organizações que levam a seguridade das informações a sério, com isso a atuação e prática dos fazeres biblioteconômicos é fundamental.

O bibliotecário poderá liderar ou compor o grupo que trabalhará com o *Compliance* e a gestão de normas e legislações que a instituição deve adequar-se, ainda contribuindo para a produção de políticas de SI realistas e bem pensadas, e na produção dos relatórios de análise de risco, ainda ajudando a buscar novas opções para sanar os gargalos encontrados pelo relatório.

Por fim, mas não finalmente, esse profissional pode ajudar nos processos de controle e avaliação dos serviços ofertados pelos colaboradores e, principalmente, verificar se as atividades estão sendo desenvolvidas visando a seguridade das informações da empresa.

As possibilidades de atuação e de contribuição são infinitas, assim o bibliotecário deverá entrar nesse novo mercado com disposição e foco, para mostrar o valor e importância do seu trabalho para instituições que, muitas vezes, se quer conhecem as potencialidades de tal profissional. Nesse contexto, é de suma importância a divulgação, disseminação e troca de experiências entre profissionais da área da biblioteconomia que trabalham com a seguridade informacional em unidades diferentes das tradicionais, assim

aumentando o engajamento e desenvolvendo as práticas e conhecimentos da área. Com isso a divulgação entre pares e a disseminação das práticas realizadas por esse profissional voltadas para SI serão o combustível para transformação de bibliotecários em larga escala.

CONSIDERAÇÕES FINAIS

A sociedade atual vivencia as consequências trazidas pelo avanço das tecnologias digitais, inaugurando um novo paradigma e era da Sociedade da Informação. Essa, por sua vez, caracteriza pela valorização e concentração de ativos chave, tais como informação. A informação tem se tornado um recurso essencial que quando bem utilizada tem o potencial de geração, inovação e progresso em variados campos desde o social, político, organizacional e científico.

Atualmente a informação é tratada como bem e recurso valioso para instituições, para pessoas e seus governos. Esse paradigma iniciado com a evolução da tecnologia no século passado reflete nas relações interpessoais, no mercado e principalmente na confiabilidade de organizações perante seus clientes e colaboradores.

A partir disso, a preocupação com a resguardo informacional e a destinação final desse recurso precisa ser preocupação de todos. Garantir a confidencialidade, integridade e disponibilidade da informação é mais que necessário para a continuação do atendimento dos objetivos organizacionais, bem como é fundamental ao pensar na gestão dos recursos informacionais de uma organização levar em consideração as pessoas, os processos e as tecnologias utilizadas.

É de suma importância a utilização de tecnologias capazes de colaborar para seguridade da informação, mas que o elo mais fraco de SI são as pessoas, pois o recurso pessoal de uma empresa por mais que seja treinado, não será uniforme. As pessoas são diferentes, possuem perspectivas e experiências diferentes, assim, o alinhamento com os colaboradores sobre boas práticas nesse tipo de segurança deve ser muito bem trabalhado, desde o momento que o colaborador vai ser contratado até o momento do seu desligamento da empresa.

O corpo de recursos humanos deve ser treinado para identificar possíveis riscos no fazer profissional, e deve se comprometer a resguardar as informações utilizadas no fazer profissional. No processo de contratação de pessoas é fundamental que seja apresentado a esse grupo as políticas de SI implementadas naquela instituição, essas políticas são norteadoras no processo de resguardo e segurança do ativo informacional, reunindo boas práticas, técnicas e procedimentos que devem ser seguidas na empresa em questão.

Diante do que foi discutido neste trabalho se torna evidente que o bibliotecário se reveste como um profissional responsável pela gestão da SI em diferentes ambientes. Nesse sentido, suas práticas vão desde a coleta, organização de seus fluxos até mesmo o seu descarte.

Esse profissional pode fazer grande diferença no processo de gestão da seguridade informacional, uma vez que tem domínio suficiente sobre as necessidades de organização e dos diferentes tipos de informação e dados, em seus diferentes suportes. Atrelar o bibliotecário a uma equipe multidisciplinar é primordial para o desenvolvimento de políticas de SI e conscientização de boas práticas no cenário organizacionais, especialmente na medida em que esse profissional tem seu olhar voltado para o fator humano, que são os por exemplo, os colaboradores de uma instituição.

Por fim, torna-se fundamental a existência de estudos adicionais que debatam e analisem criticamente a posição e possíveis contributos do profissional da informação no contexto de atuação ligados a SI e de sua gestão.

É fundamental que existam mais pesquisas que produzam avanços por meio de novos conhecimentos científicos, bem como análises de diferentes realidades em forma de estudo de casos que representem de fato como foi essa entrada desse profissional nessa seara, quais as contribuições dadas, as dificuldades encontradas e principalmente olhares futuros. Para além do foco prático, também é importante trabalhar com as novas competências do profissional da informação, inserindo o ensino destas competências em nível de graduação e pós-graduação, preparando melhor o profissional para as exigências atuais do mercado.

REFERÊNCIAS

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

BENTES PINTO, V. A biblioterapia como campo de atuação para o bibliotecário. Transinformação, Campinas, v. 17, n. 1, p. 31-43, jan./abr., 2005. Disponível em: http://revistas.puc-campinas.edu.br/transinfo/viewarticle.php?id=79. Acesso em 10 set. 2018.

BRASIL. Superior Tribunal de Justiça. Secretaria de Controle Interno. Coordenadoria de Auditoria de Tecnologia da Informação. Cartilha de Segurança da Informação. Brasília, [2014]. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/Cartseginf/article/view/3504/3627. Acesso em: 10 de jul. de 2021.

CAMPOS, A. **Sistemas de segurança da informação.** 2 ed. Florianópolis: Visual Books, 2007.

CINCO coisas que você deve saber sobre Engenharia Social. We live Ssecurity, 2016. Disponível em: https://www.welivesecurity.com/br/2016/08/19/sobre-engenharia-social/. Acesso em: 05 de jun. de 2021.

CÓDIGOS maliciosos (Malware). **Fundação Joaquim Nabuco**, 2020. Disponível em: https://www.fundaj.gov.br/index.php/area-de-imprensa/13552-codigos-maliciosos-malware. Acesso em: 10 de jun. de 2021.

CONHEÇA 5 tendências de Segurança da Informação para o futuro. **Strong Security**, 2018. Disponível em: https://www.strongsecurity.com.br/blog/conheca-5-tendencias-de-seguranca-da-informacao-para-o-futuro/. Acesso em: 09 de jun. de 2021.

CUNHA, Marcella. Multas da LGPD começam a ser aplicadas em 1º agosto. Senado federal, 2021. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2021/07/29/multas-da-lgpd-comecam-a-ser-aplicadas-em-1o-de-agosto. Acesso em: 10 de ago. de 2021.

FERREIRA, Fernando Nicolau Freitas. **Segurança da informação**. Rio de janeiro: Ciência Moderna, 2003.

FIGUEIREDO, Marco Aurélio Castro de; SOUZA, Renato Rocha. Aspectos profissionais do bibliotecário. **Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação**, n. 24, v. 12, p. 10-31, 2007. Disponível em: https://www.brapci.inf.br/_repositorio/2010/09/pdf_4f47718632_0011961.pdf. Acesso em: 10 de jul. 2021.

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

GIL, A. C. **Como classificar as pesquisas**: como elaborar projetos de pesquisa, São Paulo: Cortez 2002.

GUERRA, Fernando C. G. D. Cultura de Segurança da Informação: o desafio de integrá-la à cultura organizacional. 2019. Disponível em: https://www.ticbrasil.inf.br/posts/a-seguranca-de-dados-como-tendencia-e-as-novas-abordagens-nos-processos-educacionais/cultura-de-seguranca-da-informacao-43.html. Acesso em: 22 de mar. de 2020.

HISTÓRIA Segurança da Informação. Professor Bruno Soares. **Youtube. 0**6 de jun. de 2020. 27min14s. Disponível em: https://www.youtube.com/watch?v=rvmS5uYPfYI&t=652s. Acesso em: 10 de jul. 2021.

INFODEMIA, já ouviu falar?. **Governo do estado de São Paulo- Secretaria da Educação**, [s.d]. Disponível em: http://www.escoladeformacao.sp.gov.br/portais/Default.aspx?tabid=4572&EntryId=4711. Acesso em: 10 de jul. 2021.

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

LINO, Ricardo. **Segurança da Informação em Pessoas, Processos e Tecnologias.** Portal Gestão da Segurança da Informação,2016. Disponível em: https://portalgsi.com.br/2016/07/07/voce-sabe-o-que-e-seguranca-da-informacao-parte-2/ . Acesso em: 10 de agosto de 2021.

LYMAN, Peter; VARIAN, Hal R.. **How much information?** Barkeley: Universidade de Barkeley, 2009. 207 p. Disponível em: https://groups.ischool.berkeley.edu/archive/how-much-info/how-much-info.pdf. Acesso em: 08 jul. 2021.

PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018**: uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. 35 f. TCC (Doutorado) - Curso de Direito, Setor de Ciências Jurídicas, Universidade Federal do Paraná, Paraná, 2019. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/68114/TCC%20FINAL%20-%20lgpd.pdf?isAllowed=y&sequence=1. Acesso em: 01 jul. de 2020.

PRIVACY TECH. **Hacker X Cracker qual a diferença?.** [S.l.]. 2020. Disponível em: https://www.privacytech.com.br/protecao-de-dados/hacker-x-cracker-qual-a-diferenca,359858.jhtml. Acesso em: 10 de jul. de 2021.

QUAL a importância do complaince para a Segurança da Informação?. **Fsense blog**, [202-]). Disponível em: https://fsense.com/pt/qual-e-a-importancia-do-compliance-para-a-seguranca-da-informacao/. Acesso em: 09 de jun. de 2021.

RIBEIRO, Cristiano da Silva. **Segurança da Informação**: o desenvolvimento de uma política de Segurança da Informação em conformidade com a norma ABNT *ISO/IEC* 27002. 2016. 35 f. Trabalho de Conclusão de Curso de Sistema de Informação – FAIR Faculdades Integradas de Rondonópolis, 2016. Disponível em: https://monografias.brasilescola.uol.com.br/imprimir/15966. Acesso em: 15 de jul. de 2021.

SANTINO, Renato. Polêmicas, dinheiro e crimes: quem foi John McAfee, pioneiro do antivírus. Canaltech, 2021. Disponível em: https://canaltech.com.br/seguranca/polemicas-dinheiro-e-crimes-quem-foi-john-mcafee-pioneiro-do-antivirus-188105/
Acesso em: 12 de jul. de 2021.

SANTINO, Renato. **Segurança da informação**: Custo ou investimento?. Olhar digital, 2016. Disponível em:
https://olhardigital.com.br/2016/11/23/seguranca/seguranca_da_informacao_custo_ou_investimento/. Acesso em: 12 de jul. de 2021.

SCHUTLTZ, Felix**. Segurança da informação**: Por que a segurança dos dados é importante para a sua empresa? Milvus, 2020. Disponível em: https://blog.milvus.com.br/seguranca-da-informacao/. Acesso em: 12 de jul. de 2021.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. Cortez editora, 2017.
SILVA, Eliane Ferreira da**. Boas práticas em Segurança da Informação**. Rio de Janeiro: Edições Dalagaia, 2020. 68 p. ISBN: 9786500067477.

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

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. Cortez editora, 2017.

SILVA, Eliane Ferreira da**. Boas práticas em Segurança da Informação**. Rio de Janeiro: Edições Dalagaia, 2020. 68 p. ISBN: 9786500067477.

SILVA, Eliane Ferreira da (Org). **Segurança da informação**: temas para uma prática. Natal: EDUFRN, 2008. 117 p. ISBN: 9788572733977.

SOBRAL, Fábio. Segurança da Informação: como garantir a confiabilidade e a integridade? Biblioo: cultura informacional, 5 mar. 2012. Disponível em: http://biblioo.info/segurancada-informação. Acesso em: 10 de ago. de 2021.

SOUSA, Rainer Gonçalves. **Escrita Egípcia**. Mundo Educação, [s.d.]. Disponível em: https://mundoeducacao.uol.com.br/historiageral/escrita-egipcia.htm l. Acesso em: 10 de ago. de 2021.

TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil**: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. 195 p. Disponível em: http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf. Acesso em: 10 jul. 2020.

TOKEN // Dicionário do Programador. [S.L.]: Código Fonte Tv, 2020. (8 min.), son., color. Disponível em: https://www.youtube.com/watch?v=LtVb9rhU41c. Acesso em: 10 de mar. De 2021.

TRUZZI, Gisele. **Vazamento de informações**: meu ex-funcionário levou informações da minha empresa. E agora?. Isto é dinheiro, 2019. Disponível em:
https://www.istoedinheiro.com.br/vazamento-de-informacoes-meu-ex-funcionario-levou-informacoes-da-minha-empresa-e-agora/. Acesso em: 12 de jul. de 2021.