UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE ENGENHARIA DE SOFTWARE

ALINE DE FREITAS COUTINHO

RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES: UM MAPEAMENTO SISTEMÁTICO

Itacoatiara – Amazonas
Novembro – 2020

ALINE DE FREITAS COUTINHO

RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES: UM MAPEAMENTO SISTEMÁTICO

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia de Software.

Orientador: Prof. Dr. Rainer Xavier de Amorim

Itacoatiara – Amazonas
Novembro – 2020

Coutinho, Aline de Freitas
C871r Recomendações de segurança da informação nas organizações: um mapeamento sistemático / Aline de Freitas Coutinho . 2020
98 f.: il. color; 31 cm.

Orientador: Rainer Xavier de Amorim
TCC de Graduação (Engenharia de Software) - Universidade Federal do Amazonas.

1. Segurança da Informação. 2. Organizações. 3. Recomendações de Segurança da Informação. 4. Políticas de Segurança da Informação. I. Amorim, Rainer Xavier de. II. Universidade Federal do Amazonas III. Título

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Curso de Bacharelado de Engenharia de Software

FOLHA DE APROVAÇÃO

ALINE DE FREITAS COUTINHO

RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES: UM MAPEAMENTO SISTEMÁTICO

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia de Software.

Aprovada em 24 de Novembro de 2020

BANCA EXAMINADORA

Prof. Dr. Rainer Xavier de Amorim, Presidente
Universidade Federal do Amazonas

Profa. Dra. Odette Mestrinho Passos, Membro
Universidade Federal do Amazonas

Bel. Romualdo Costa de Azevedo, Membro
Universidade Federal do Amazonas

Folha de Aprovação assinada pela Profa. Odette Mestrinho Passos, responsável pela disciplina de Trabalho de Conclusão de Curso (Período: 2020/ERE), onde atesta a defesa do(a) aluno(a) e a presença dos membros da banca examinadora.

rior,

Documento assinado eletronicamente por **Odette Mestrinho Passos, Professor do Magistério Supe** em 04/12/2020, às 17:22, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0375612** e código CRC **46EAD388**.

e o

Rua Nossa Senhora do Rosário - Bairro Tiradentes nº 3836 - Telefone: (92) (92) 99318-2549
CEP 69103-128 Itacoatiara/AM - ccesoicet@ufam.edu.br

À minha mãe, minha avó e meu avô que foram fundamentais para a minha formação acadêmica.

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a minha família, que é composta por minha mãe dona Nelcy de Freitas Coutinho, que sempre me apoiou e me motivou para continuar nesse caminho e lutar pelas coisas que almejo. A minha avó senhora Maria de Freitas Pedrosa e meu avô senhor Adamor Mendonça Coutinho que sempre fizeram o possível para que eu tivesse tudo que era necessário para não desistir.

Gostaria também de expressar minha total gratidão e respeito ao Prof. Dr. Rainer Xavier de Amorim, que sempre foi compreensivo e paciente, e que durante essa caminhada sempre me deu o total suporte que precisava, assim como os conhecimentos necessários para que pudesse finalizar mais essa etapa em minha vida.

Assim como agradecer a todos os amigos que fiz durante essa jornada, Clinton Hudson, Irene Jacaúna, Jéssica Farias, Joicilene Melo, Rodrigo Feitosa, Sabrina Rocha, Thiago Trindade e Thuan Matheus, a todos esses o meu muito obrigada, cada um contribuiu de uma forma única para meu crescimento pessoal.

"Ao infinito... e além!"

Buzz Lightyear "Toy Story, 1995".

RESUMO

Na era da informação, o grande problema que vem sendo enfrentado é conseguir manter as informações sigilosas de cada indivíduo. O grande avanço das tecnologias vem contribuindo para que sujeitos mal-intencionados consigam roubar informações que não lhe diz respeito. As organizações também enfrentam esse tipo de problema e conseguir manter os dados sigilosos das organizações vem se tornando cada vez mais difícil. As alternativas mais viáveis para conter o problema de Segurança da Informação são ferramentas de Segurança da Informação, além de adotar Políticas ou controles de segurança da Informação. Nesse sentido, o objetivo deste trabalho é verificar as recomendações de Segurança da Informação nas Organizações bem como esforços e políticas existentes na literatura para a proteção das informações. A metodologia adotada consiste em um mapeamento sistemático na literatura científica com o intuito de coletar as informações sobre as recomendações de segurança da informação nas organizações. Como resultados, pode se citar que foram encontradas 17 recomendações, que podem ser utilizadas da forma que melhor se encaixar para cada organização e até mesmo ameaça, vulnerabilidade/ou comportamento de risco, assim como também foram identificados 07 tipos de ameaças, que podem ser contornados com as recomendações encontradas.

Palavras-Chave: Segurança da Informação. Organizações. Recomendações de Segurança da Informação. Políticas de Segurança da Informação.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANS	Análise do Núcleo de Sentido
CID	Confidencialidade, Integridade e Disponibilidade
EIS	Executive Information System
GQM	Goal, Question, Metric
IEC	International Electrotechnical Commission (Comissão Eletrotécnica Internacional)
ISO	International Organization for the Standardization (Organização de Padronização Internacional)
MS	Mapeamento Sistemático
PSI	Política de Segurança da Informação
SAD	Sistemas de Apoio à Decisão
SAE	Sistemas de Automação de Escritórios
SI	Sistemas de Informação
SIE	Sistemas de Informação Executiva
SIG	Sistemas de Informações Gerenciais
SPT	Sistemas de Processamento de Transação
STC	Sistemas de Trabalho do Conhecimento
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Nesta Seção serão apresentados os tópicos de introdução, justificativa, objetivos, metodologia utilizada, assim como a organização deste trabalho, para o leitor se familiarizar com a temática que será abordada neste trabalho.

1.1 Contextualização

A informação é formada de uma coleção de dados que demonstram uma visão diferente, mostrando uma nova definição ou evidenciando semelhanças que antes não eram conhecidas sobre eventos ou objetos. Com isso, a informação tem significado e causa impacto em um nível menor ou maior, o que a torna o meio essencial da extração e concepção do conhecimento (CAMPOS, 2007).

Dessa forma, o mundo vivencia a era da informação, reivindicado das instituições uma administração competente, que pode ser simplificada com a aplicação de métodos inteligentes fornecidos pela Tecnologia da Informação (TI) e Sistemas de Informação (SI). A TI dispõe de recursos tecnológicos e computacionais com a finalidade de geração de informações, já os SI encontram-se cada vez mais aprimorados, sugerindo mudanças nos métodos, organização e plano de negócios (BARZZOTTI, GARCIA, 2006).

Assim, segundo Laudon e Laudon (1999), o SI é uma coleção de partes inter-relacionadas, elaborados para coletar, processar, armazenar e partilhar informação para simplificar a coordenação, a administração, a inspeção, a forma de visualização e o processo de tomada de decisão.

Com isso, a construção de SI segue como uma atividade de alto custo e alta complexidade. Esforços gigantescos são requeridos em todas as etapas do procedimento de desenvolvimento para suprir a qualidade das condições do cliente em meio ao orçamento e prazos mínimos (NETO e OLIVEIRA, 2013).

Logo, é inegável o fato de que a Web se tornou um dos mecanismos computacionais mais valiosos para a humanidade. Assim, E-mail eletrônico, E-commerce, redes sociais e transações online são uns dos meios que são ofertados, seja com a finalidade de lazer ou para negócios, favorecendo pessoas, empresas ou organizações (SILVA e GARCIA, 2015).

Portanto, dissertar sobre segurança da informação é de extrema relevância no mundo integrado em que vivemos, visto que tudo está voltado para a informação. Avisar empresas e usuários sobre as ameaças constantes que estão localizadas no mundo virtual e lhes fornecer

informações de como se defender de prováveis danos e/ou prejuízos que possam lhes ocorrer futuramente, com certeza, é de grande importância e colabora com a diminuição dos crimes virtuais (RODRIGUES, TORRES e FLORIAN, 2018).

De acordo com a ISO/IEC (2005), a segurança da informação é uma proteção das informações contra uma extensa gama de ameaças para que com isso possa se dar continuidade aos negócios, e tornar mínimos os prejuízos assim como aumentar o retorno das aquisições e oportunidades comerciais.

Com isso, a política de segurança estabelece um grupo de normas, técnicas e procedimentos empregados para a preservação da segurança da informação, de forma a ser formalizada e transmitida para todos os usuários que utilizam os ativos de informação (FERREIRA e ARAÚJO, 2008).

Sendo assim, todo computador necessita ter softwares de segurança, por exemplo, antivírus, antispyware e firewall, para assim controlar ameaças e impedir o roubo de informações do usuário. No entanto é de suma importância acentuar que resultados miraculosos não existem. Toda ferramenta deve ser utilizada tendo em vista suas restrições (NOVO, 2010).

Assim, segundo Fernandes (2013), pode se definir incidente como um efeito que pode paralisar os procedimentos normais de negócio, com a consequência de determinados aspectos de segurança ter sido infringido, de forma intencional ou não. Quando se discorre sobre problemas de segurança, há incontáveis fatores que podem levar a perda e/ou infração dos dados de uma empresa, como a má execução do sistema ou até mesmo quando a segurança está passando por ameaça, risco, vulnerabilidade, falhas e desastres.

A Segurança da Informação, neste caso, é adquirida por meio da implementação de um grupo de controles apropriados, contendo políticas, processos, procedimentos, infraestruturas organizacionais e funcionalidades de software e hardware. Estes controles necessitam ser determinados, implementados, vigiados, examinados de forma crítica e aperfeiçoados, quando necessário. Garantindo assim que os propósitos do negocio e de segurança da organização sejam acompanhados. Calha que isto venha a ser feito em parceria com outros métodos de gestão de negócio (ISO/IEC, 2005).

Segundo Soares e Silva (2018), o furto da informação está sendo um tema de matéria muito comum na mídia de forma geral, o que com certeza colaborou para alavancar a insegurança do uso de tecnologias de software. No entanto, há grupos de trabalho que agem

para colaborar com a implementação de aplicações web com graus mais altos de segurança. Contudo, é valido que tanto organizações quanto especialistas da engenharia de software precisem estar incessantemente estudando e pesquisando a respeito da segurança da informação.

1.2 Justificativa

As empresas, assim como suas redes de computadores e os seus SI estão expostos a inúmeros tipos de ameaças no que diz respeito à segurança da informação, o que inclui fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio até mesmo inundações. Estragos causados por código malicioso, hackers e ataques de negação de serviço (denial of services) estão sendo cada vez mais comuns, ousados e espantosamente mais aprimorados (ISO/IEC, 2005).

Segundo Ferreira, Cabral e Sonnenstrahl (2013), a segurança da informação objetiva o resguardo da confidencialidade, integridade e disponibilidade da informação. Complementarmente, outras particularidades, como por exemplo, autenticidade, responsabilidade, não repúdio e confiabilidade. Sendo assim, a segurança inclui desta forma a preservação das informações com relação aos mais variados tipos de ameaças, garantindo assim a continuação do empreendimento, diminuir o risco do negócio e aumentar os investimentos e as possibilidades de negócio.

Para Furnell e Thompson (2009), um dos contratempos mais comuns da preservação da segurança da informação é o comportamento indiferente e os atos e atitudes provenientes dos trabalhadores. Sabendo-se que a cultura corporativa de uma empresa molda as concepções e os valores de seus indivíduos. Logo, é de suma importância trabalhar a conscientização dos empregados e assegurar que a educação e capacidades relevantes sobre segurança sejam repassados.

Desta forma, os usuários são um dos elementos que é capaz de ocasionar vulnerabilidades e possíveis estragos nos SI. Sendo assim, é conveniente investigar se estão sensibilizados ao uso de práticas corretas seguras para a execução das suas obrigações (PIMENTA e QUARESMA, 2016).

Tendo isso em vista, para que se comece a implementar uma gestão de segurança, torna-se indispensável o desenvolvimento de uma política de segurança da informação, que é um grupo de regras no qual são determinados os procedimentos que devem ser executados

assim como os que não são sugeridos a se fazer, visando sempre proteger os recursos de TI e assegurar a integridade, disponibilidade, confidencialidade e autenticidade das informações salvas (MESQUITA, 2015).

Com isso, segundo o Tribunal de contas da união (2012) é necessário que a política de segurança da informação exceda o propósito contido pelas áreas de SI e recursos computacionais. Não é viável que a mesma fique limitada à área da informática. Muito pelo contrário, ela deve estar incorporada à visão, à missão e ao negócio, assim como as metas empresariais. O mesmo se aplica ao plano estratégico de informática e as políticas da organização, voltados à segurança em geral.

Portanto, mais de que procedimentos de trabalho claramente decididos, profissionais maduros e qualificados, a segurança da informação exige ferramentas singulares para a implantação das regras compostas nas políticas de segurança. A maioria dos requisitos de controle e precaução apenas podem ser alcançados com a utilização de soluções de hardware e software. Logo, a implementação de políticas de acesso depende constantemente de firewalls, servidores de autenticação e equipamentos de rede (PROMON, 2005).

Neste contexto, esta pesquisa justifica-se pela importância de apresentar as principais vulnerabilidades das empresas em geral. Além destes, é importante também levantar os comportamentos de risco que os funcionários de cada empresa podem ter, no sentido de expor os dados sigilosos da empresa que trabalham.

1.3 Objetivos

Geral

Verificar as recomendações de Segurança da Informação nas Organizações bem como esforços existentes na literatura para a proteção das informações.

Específicos

- Investigar as recomendações de segurança da informação relacionadas às práticas e controle de proteção de dados sigilosos no contexto das organizações.
- Identificar os tipos de ameaças, vulnerabilidades e/ou comportamento de risco, relatados nas recomendações de segurança da informação da literatura.

1.4 Metodologia

A metodologia de pesquisa que foi utilizada para este trabalho é o Mapeamento Sistemático (MS), é baseado no guidelines que foi desenvolvido por Kitchenham e Chartes (2007), essa metodologia tem como finalidade identificar, rotular e analisar proeminências que fazem analogia com questões de pesquisa específicas, tópicos ou qualquer outro contexto semelhante.

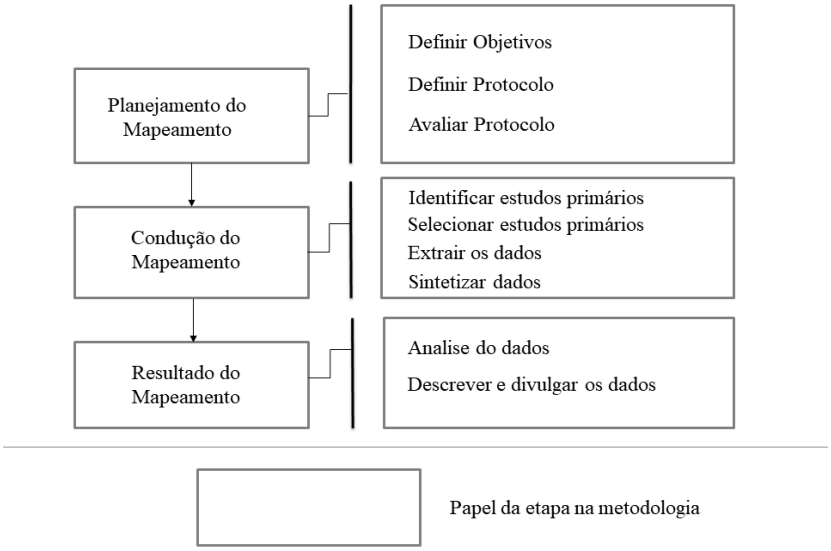
Segundo Petersen et al. (2008), o MS traz uma visão geral de uma área específica de pesquisa, identificando o quantitativo, quais os tipos de pesquisas alcançadas, os resultados disponibilizados, e ainda a frequência de publicações durante o período de tempo para que assim se possa identificar as tendências.

Kitchenham e Charters (2007) asseguram que estudos de MP na área de engenharia de software têm sido aconselhados, acima de tudo nas áreas de pesquisa em que há a dificuldade de se enxergar a abundância de materiais, com relevância e grande qualidade, que podem estar disponíveis. Sendo assim, a escolha dessa metodologia para a condução desta pesquisa, tem como justificativa que o objetivo é apenas identificar e empregar os resultados adquiridos para pesquisas futuras.

Ao longo do processo é possível ter uma gama de benefícios, por exemplo: (i) Uma redução significativa do gasto de tempo para atividades de pesquisa; (ii) Fácil compreensão da literatura no que se refere com as questões de pesquisa; (iii) Formulários e procedimentos são algumas das ferramentas que podem ser reutilizados; (iv) Maior facilidade de se encontrar trabalhos relacionados com o que está em desenvolvimento; (v) Permite o aprendizado de cada particularidade dos dados que serão adquiridos ao longo da execução do MS (KITCHENHAM et al., 2011).

De acordo com Kitchenham e Charters (2007), o processo do MS divide-se em três principais etapas, na qual as mesmas são coordenadas de maneira interativa, quer dizer, um processo que irá se reiniciar até alcançar algum resultado. A Figura 1 demonstra as principais etapas que compõem o MS:

Figura 1 - Etapas e Atividades do Mapeamento Sistemático



Fonte: Adaptado de Kitchenham; Charters (2007).

(a) Planejamento do Mapeamento: mostra a real necessidade, isto é, a razão central para desenvolver o MS. Nesta etapa, os objetivos da pesquisa são enumerados e então é determinado o protocolo, que será composto pelo estabelecimento das questões de pesquisa, estratégias de busca, fontes de pesquisas, string de busca e os critérios para seleção. A qualidade do protocolo é capaz de provocar um vasto impacto na condução do MS, tendo isso em vista foram realizados testes para averiguar a viabilidade da execução da revisão, isso possibilitará que mudanças possam ser feitas caso necessário.

(b) Condução do Mapeamento: no decorrer dessa etapa, as fontes para a condução do mapeamento são escolhidas, os estudos são apresentados, indicados e examinados conforme os critérios determinados no protocolo do mapeamento, no qual se deve distinguir os fatores essenciais que devem ser incluídos ou excluídos, depois desse processo, os dados adquiridos serão fundamentais para responder às questões de pesquisa que foram determinadas na etapa precedente.

(c) Resultado do mapeamento: nessa etapa, as informações dos estudos são extraídas e condensadas para serem divulgadas. É importante salientar que os resultados serão apresentados de acordo com o que foi estabelecido no procedimento de extração de dados.

1.5 Organização do Trabalho

Capítulo 1 – Introdução: apresentou os principais aspectos deste trabalho, descrevendo o seu contexto, justificativa, objetivos e metodologia adotada. Além desta introdução, outros cinco capítulos compõem este trabalho, organizados da seguinte forma:

Capítulo 2 – Fundamentação Teórica: é apresentado o referencial teórico que fundamenta os conceitos básicos utilizados nesta pesquisa e os trabalhos relacionados.

Capítulo 3 – Planejamento do Mapeamento Sistemático: Descreve toda a primeira etapa do MS, que é o planejamento do MS, como as questões de pesquisa, fontes, idiomas, expressões de busca, critérios de seleção e o procedimento de extração de dados.

Capítulo 4 – Condução do Mapeamento Sistemático: Descreve o processo de avaliação e seleção das publicações para se obter os resultados e responder às questões de pesquisa.

Capítulo 5 – Análise dos Resultados do Mapeamento Sistemático: Apresenta a extração de dados e os resultados obtidos, assim como a análise das informações extraídas.

Capítulo 6 – Conclusão e Perspectivas Futuras: Apresenta as considerações finais, resultados obtidos, contribuições do trabalho, as limitações e futuras perspectivas para a continuidade desta pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta Seção serão apresentados os principais conceitos relacionados que servirão de base para a pesquisa a ser realizada neste trabalho sobre as recomendações de Segurança da Informação no contexto das organizações.

2.1 Conceitos Relacionados

2.1.1 Sistemas de Informação

De acordo com Saracevic (1974), os SI correspondem à incorporação de uma variedade de elementos diversos, que podem ser especificados e caracterizados de diversos modos, elementos destacados de SI podem apresentar propriedades: físicas, biológicas, psicológicas e/ou sociológicas (no entanto, é necessário admitir que o sistema em sua totalidade pode ser distinto de outra propriedade de seus elementos, motivado pelas interações), detalhadas abaixo.

a) **Propriedades Físicas:** abrangem, entre outras, a natureza física dos sinais, símbolos ou parâmetros (eletromagnéticos, químicos, óticos etc.) utilizados para simbolizar as informações em um sistema, assim como, a maneira e disposição destes sinais, símbolos ou parâmetros (SHANNON e WEAVER, 1949; ZIPF, 1949), juntamente com os meios físicos em quais são catalogados. É significativo destacar que normalmente relaciona-se informação e energia por meio destas características físicas (TRIBUS e McHRVTNE, 1971).
b) **Propriedades Biológicas:** compreendem a estrutura e procedimentos do cérebro e do sistema nervoso, assim como os impactos destes na estrutura e restrições em outros SI criados pelo homem (HARMON, 1970). Logo, as características de informação dos sistemas, como: repetição, associação, ordenamento e relações derivam de estruturas biológicas (GOFFMAN e MORRIS, 1972). Dessa forma, é por meio dos princípios biológicos que o conhecimento e a vida são relacionados (PRIBRAM, 1969).
c) **Propriedades Psicológicas:** incluem estados que consentem aos indivíduos compreenderem e referir-se a outros elementos, além deles mesmos. Assim, é considerada a habilidade de aprender (ou seja, habilidade de adquirir, guardar, relacionar, alterar, rememorar e aplicar o conhecimento), assim como, a especialidade de conformidade entre os estados de conhecimento e o armazenamento como uma condição para a comunicação.
d) **Propriedades Sociológicas:** abrangem as circunstâncias do ambiente social na criação, repartição e utilização. Com isso, a linguagem é levada em consideração, observando-se a conduta do conhecimento do público, que pode incluir a distribuição de autores (lei de Lotka) e de registros (lei de Brad Ford), aglomeração etc. (BROOKES, 1973).

Dessa forma, deve-se levar em consideração as peculiaridades dos SI como um todo. Um sistema é constituído pela agregação de elementos específicos com as propriedades citadas acima. Quando combinados, estes elementos interatuam para fabricar um SI com um grupo singular de propriedades. Que são (i) repetição de informação; (ii) associação entre elementos de informação (classificação); (iii) ordenação dos elementos de informação e (iv) existência de relações entre elementos de informações. Sem essas propriedades não existe SI (ou o sistema pode não funcionar de forma eficiente, logo deixando de existir).

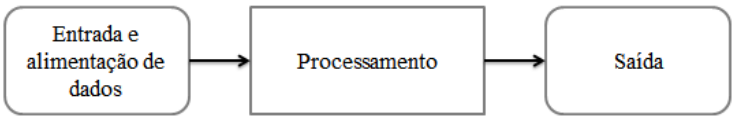
Segundo O'Brien e Marakas (2010), um SI necessita de recursos das pessoas (usuários finais e profissionais em SI), hardware (equipamentos e mídia), software (programas e processos), dados (informações e bases de conhecimentos) e redes (conjunto de meios de comunicação e suporte de rede) para realizar ações de entrada, processamento, saída, armazenamento e controle que modificam recursos específicos em produtos de informação.

Para Martins et al. (2012), os SI podem ser vistos como procedimentos administrativos que compreendem processos menores que interatuam entre si, integrando-se para guardarem informações e produzir dados para colaborar com as decisões. Os SI são produzidos empregando os conceitos da TI, que fornecem possibilidades para que assim a organização possa tomar decisões certas e exatas, fazendo assim com que a empresa sempre tenha um desempenho bom.

Neste contexto, serão apresentadas as categorias específicas de SI que dão suporte a cada um dos níveis hierárquicos: operacional, gerencial, estratégico e o de conhecimento. Este tipo categorização é a mais abordada na literatura especializada em SI (MÜLBERT e AYRES, 2005):

a. **Sistemas de Nível Operacional:** no nível operacional, os SI dão assistência no processamento e acompanhamento das atividades rotineiras, e transações habituais de uma organização, como: entrada de pedidos de venda, expedição de notas fiscais, solicitações de materiais, lançamentos de produção, registro de pessoal. Estes sistemas empresariais primordiais são frequentemente chamados de Sistemas de Processamento de Transação (SPT).
   A Figura 2 mostra um (SPT), que trata-se de um grupo organizado de indivíduos, processos, softwares, banco de dados e equipamentos utilizados para realizar e registrar as operações comerciais (STAIR e REYNOLDS, 2016).

Figura 2 - Visão Geral Simplificada de um Sistema de Processamento de Transação



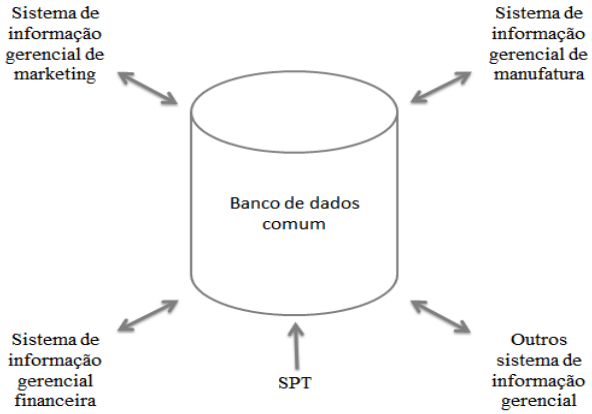
Fonte: Adaptado de Stair e Reynolds (2016).

b. **Sistema de Nível Gerencial:** no nível gerencial das organizações as atividades estão relacionadas com a monitoração e controle das atividades rotineiras. Esses sistemas são elaborados para servir de base a estas atividades. Assim como podem também, oferecer suporte a tomadas de decisões não rotineiras, por intermédio de simulações e estudo de cenários. Existem dois tipos de SI que se apresentam para dar suporte a essas atividades, como: Sistemas de Informações Gerenciais (SIG) e o Sistemas de Apoio à Decisão (SAD).

   Os SIG, como pode ser observado na

   Figura **3**, propiciam aos gerentes, a visualização de relatórios e verificações sobre o desempenho atual e os registros antigos da organização, para assim auxiliar as atividades de planejamento, controle e tomada de decisão. De maneira geral, os SIG, fornecem relatos sobre as operações básicas (transações operacionais) da organização. Os conceitos de transações básicas, guardados pelos SPT, são reunidos e expostos em um formato predeterminado.

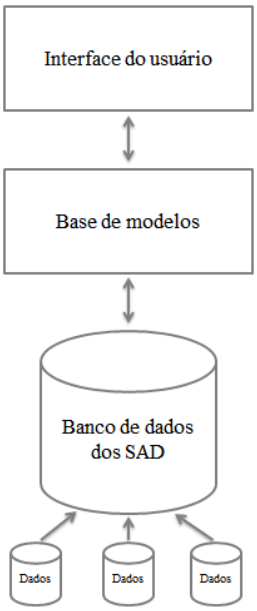
Figura 3 - Visão Geral Simplificada de um Sistema de Informação Gerencial



Fonte: Adaptado de Stair e Reynolds (2011).

Os SAD, diferente dos SIG, busca dar suporte a decisões menos rotineiras e estruturadas, e que não conseguem ser especificadas facilmente com antecedência. Os SAD fornecem assistência computacional dinâmico no decorrer do processo de tomada de decisão. Os usuários podem trocar deduções, fazer novos questionamentos e inserir novos dados, conforme pode ser observado na Figura 4.

Figura 4 - Visão Geral Simplificada de um Sistema de Apoio à Decisão

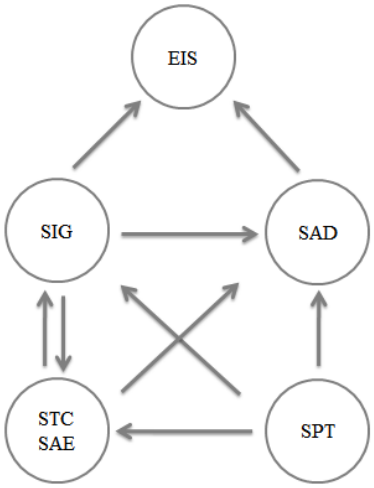


Fonte: Adaptado de Laudon e Laudon (2001).

c. **Sistema de Nível Estratégico:** o nível mais alto da administração usa uma categoria de SI denominado de Sistemas de Informação Executiva (SIE), ou como é mais conhecido *Executive Information System (*EIS). Os EIS fornecem um acesso mais rápido a informações atuais, de uma maneira muito amigável, fazendo uso intenso de recursos gráficos (cores, símbolos, ícones, botões, imagens e até mesmo gráficos), assim como a capacidade de multivisão (uso de mídias diversas, revelando em uma mesma tela, gráficos, textos e tabelas).
d. **Sistemas de Nível de Conhecimento:** nesse nível de conhecimento operam os sistemas que ajudam o processo de criação da informação, denominados de Sistemas de Trabalho do Conhecimento (STC). Além desse, se encaixa neste nível os conhecidos sistemas colaborativos, que alavancam as comunicações e o desempenho de equipes e grupos de trabalho, e são conhecidos como Sistemas de Automação de Escritórios (SAE).

Neste contexto, a Figura 5 demonstra à interação entre os tipos de SI supracitados. Demonstrando assim a integração desses tipos, considerando os níveis apresentados, que são: operacional, gerencial, estratégico e conhecimento.

Figura 5 - Integração Entre Sistemas de Informações



Fonte: Adaptado de Laudon e Laudon (2001).

2.1.2 Tecnologia da Informação

Dependendo da situação, sendo ela tanto de usuário como o simples uso de um dado sistema, a palavra "tecnologia" possui vários conceitos no decorrer de um *continuum* de significados inteiramente vinculados, de maneira que os significados consecutivos envolvem os antecedentes. Do lado estrito do *continuum*, a tecnologia estende-se apenas a máquinas ou mesmo ferramentas (na TI isso quer dizer computadores, equipamentos de transmissão, reprodução, equipamentos reprográficos, etc.) (SARACEVIC, 1974).

Segundo Silva (2004), os recursos de TI podem potencializar mais ainda a externalização, a internalização e a agregação do conhecimento compreensível. No momento em que partem de uma circunstância em que as recomendações e cuidados anteriormente mostrados já estão sendo levados em consideração.

De acordo com Alavi e Leidner (2001), o conhecimento pode ser guardado e utilizado, sendo assim, o objetivo da TI é juntar, guardar e transmitir o conhecimento. Do ponto de vista do pensamento processual, as autoras declaram que o papel da TI é fornecer ligações entre os agentes de conhecimento e gerar um fluxo amplo e profundo de conhecimento. No que se refere ao acesso de informação, a TI deve propiciar um mecanismo de busca e, por fim, quanto às competências, a sua função é suportar o desenvolvimento pessoal e institucional.

Para Saracevic (1974), tecnologia abrange também os processos, as especificações, modelos e regulamentos associados com o manuseio das máquinas (ou seja, "software", padrões de operações). Em um grau mais elevado, pode-se assimilar a tecnologia como os procedimentos empregados em computação e recuperação.

A TI atualizou o mundo dos negócios. Os procedimentos empresariais necessitam serem providos de confiabilidade, flexibilidade, competência e efetividade. A TI é empregada para aperfeiçoar o desempenho das atividades da organização, e por decorrência, apoiar a reestruturação dos procedimentos empresariais (BAZZOTTI e GARCIA, 2006).

Segundo Alves (2013), a coleção de todas as atividades e respostas fornecidas por recurso de computação é chamado de TI. Na realidade, as serventias para a TI são inúmeras, pois estão relacionadas a várias áreas, que existem muitas definições e nenhuma consegue defini-la por completo.

Uma conciliação perfeita entre telemática, componente de hardware, software, banco de dados e rede de computadores e dessa associação surgiu a TI. A TI pode ser conceituada como um sistema que verifica a informação precisa para a assistência no processo das tomadas de decisões na esfera empresarial pelos dirigentes, colaborando com o negócio no mercado competidor (PEREIRA et. al, 2011).

De acordo com Maia (2013), nos tempos atuais, a TI, como apoio ao SI, é vista como agente de incorporação de toda a cadeia de valor da organização e do seu âmbito externo, aumentando assim suas fronteiras empresariais e colaborando para o sucesso ou, quando implementada de forma errada, para o seu fracasso.

Com os aperfeiçoamentos concedidos pela TI, as organizações podem ter novas possibilidades comerciais, concedendo a expansão para novos negócios ou novos segmentos de mercados já existentes. Mesmo que isso indique enfrentar inúmeras dificuldades, especialmente no que desrespeita ao custo alto de investimento e dificuldade da TI (BAZZOTTI e GARCIA, 2006).

Segundo Oliveira, Moura e Araújo (2012), a TI pode ser conceituada como todo recurso tecnológico e computacional designado à coleta, manipulação, armazenamento e processamento de dados ou informação dentro de uma empresa. Outra definição para TI é que ela pode usar seus recursos computacionais para o desenvolvimento de SI. Seus elementos essenciais são hardware e software, assim como seus recursos de telecomunicações, que são conceituados a seguir:

- **Hardware:** equipamentos físicos digitais, com finalidade de receber, guardar e processar dados.
- **Software:** programas de computador, que tem por objetivo manusear, ordenar e inspecionar o hardware, dando-lhe instruções e comandos de funcionamento (NORTON, 1996).

- **Telecomunicações:** são transmissões eletrônicas de sinais para comunicações, que incluem meios como, por exemplo, telefone, rádios, televisão. A arquitetura é constituída por computadores que fazem a recepção e emissão de dados por intermédio de meios de comunicação. Com fios telefônicos ou ondas de rádio.

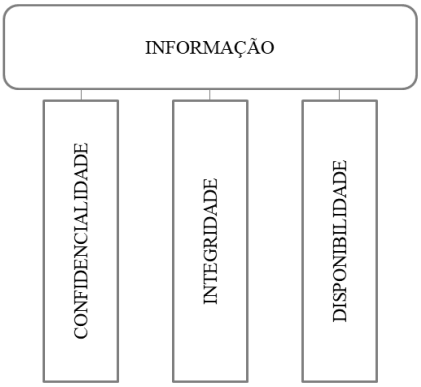
2.1.3 Segurança da Informação

A Segurança da informação é identificada pela utilização adequada de aparelhos de proteção acerca de um ativo ou de um grupo de ativos desejando preservar o seu valor para as empresas. A aplicabilidade dessas proteções tenta proteger a confidencialidade, integridade e a disponibilidade (CID), não sendo restringido apenas para sistemas ou aplicativos, e sim também a informações guardadas, ou veiculadas em vários meios além do eletrônico ou em papel (BASTOS e CAUBIT, 2009).

Segundo Torres (2015), de uma maneira clara e objetiva, a informação pode ser conceituada por um grupo de dados tratados e ordenados de tal maneira que tragam certo conceito ou definição dentro de certo contexto.

Um sistema de segurança da informação tem como base três princípios básicos, que são (CAMPOS, 2007): CID, de acordo com a disposição apresentada na Figura 6.

Figura 6 - Características de Segurança da Informação



Fonte: Adaptado de Campos (2007).

Se por ventura um ou mais desses princípios forem violados em qualquer momento, isso significa que a segurança da informação foi quebrada, o que também pode ser chamado de incidente de Segurança da Informação.

Neste contexto, existem três princípios básicos relacionados à Segurança da Informação, que são:

- **Confidencialidade:** O princípio da confidencialidade é assegurado quando somente os indivíduos explicitamente autorizados podem ter acesso à informação.

No momento em que uma informação é acessada por um indivíduo não autorizado, de forma intencional ou não, seja pela descoberta de uma senha, pelo acesso a registros ou de qualquer outra forma, isso se caracteriza como um incidente de segurança da informação por quebra de confidencialidade.

- **Integridade:** O princípio da integridade é assegurado quando a informação acessada está inteira, sem modificações e, consequentemente, válida. No instante em que uma informação é modificada indevidamente, intencionalmente ou não, assim como pela falsificação de um arquivo, da alteração de documentos em um banco de dados, ou qualquer outra coisa que mude a informação inicial de forma inadequada.
- **Disponibilidade:** O princípio da disponibilidade é assegurado quando a informação está disponível, para as pessoas autorizadas, sempre que houver a necessidade. No momento em que a informação não está acessível nem mesmo para quem é de direito, por exemplo, no caso da perda de arquivos, quando há sistemas de computador "fora do ar", ou, até mesmo, em função de ataques de negação de serviços á servidores de rede ou servidores Web, isto é, quando esses servidores estão impotentes como consequência de ataques e invasões, ou até mesmo às "quedas" de sistemas que não são provocadas, ou seja, as que não são intencionais, também são vistas como quebra da disponibilidade.

Além desses três princípios básicos, de acordo com Lyra (2008), conseguimos mencionar mais alguns aspectos adicionais que podem garantir a segurança da informação, que são:

- **Autenticação:** Certificar que um indivíduo é realmente quem se diz ser.
- **Não repúdio:** Competência do sistema de comprovar que um usuário realizou uma determinada operação.
- **Legalidade:** Certificar que o sistema esteja aderente às leis.
- **Privacidade:** Capacidade de um sistema de assegurar que um usuário permaneça anônimo, evitando o relacionamento entre o usuário e suas ações.
- **Auditoria:** Capacidade do sistema de auditar absolutamente tudo que os usuários realizaram, identificando assim fraudes ou tentativas de ataque.

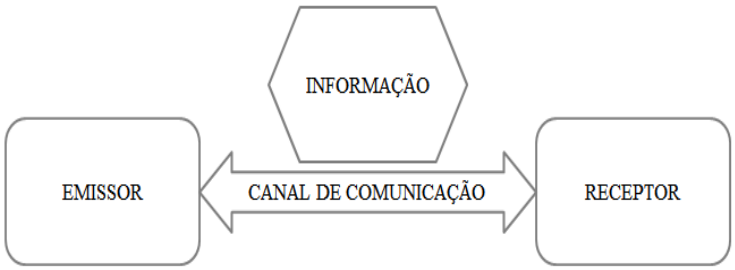
Para Caruso e Steffen (1999), segurança é mais que estrutura hierárquica, indivíduos e dispositivos. Ela abrange uma postura gerencial, o que excede a abordagem habitual da maioria das organizações. Logo, é necessário rodear o ambiente de informações com critérios que certifiquem sua segurança efetiva, a um custo acessível, tendo em vista que se torna impossível conseguir segurança absoluta, já que a partir de certo ponto, os custos se tornam inacessíveis.

Casualmente poderá ocorrer que um ou mais princípios de segurança da informação sejam quebrados. Isso se caracteriza como incidente de segurança da informação, para entender melhor sobre este incidente, é necessário conhecer os conceitos de ativo de

informação, vulnerabilidades e as ameaças, do ponto de vista de segurança da informação (CAMPOS, 2007), apresentados a seguir:

- **Ativo de Informação:** a informação em sua essência é um elemento abstrato, existindo de forma concreta quando suportada nos vários meios, como equipamentos, agendas, livros, no intelecto dos indivíduos, em cabos de redes de computadores, em ondas de rádios, e outros. Sendo assim, pode se afirmar que tão importante quanto à informação em si é o meio que a suporta, que a preserva, que a permite existir.
  Da mesma forma que a informação em si é abstrata e não existem sem as tecnologias, pessoas, ambientes e, do mesmo modo, os processos são estruturas conceituais que ajustam o comportamento dos indivíduos em relação a estas tecnologias e ambientes.
  a Figura 7 abaixo mostra o processo de comunicação no qual se pode-se fazer um paralelo no contexto de ativos da informação.

Figura 7 - Processo de Comunicação



Fonte: Adaptado de Campos (2007).

os elementos na Figura 7 são os mesmos que formam o tradicional processo de comunicação. Considerando assim esses elementos no contexto de ativos de informação, que são: a) informação; b) emissor, que pode ser as pessoas, procedimento, equipamentos, tecnologias (softwares), entre outros; c) meio de transmissão, que seria equipamentos, cabos de rede, ondas de rádio e TV, e outros; e d) receptor, que podem ser pessoas, processos, dispositivos, tecnologias, etc.
Conclui-se dessas classificações que a informação e tudo aquilo que a suporta ou utiliza pode ser classificado como um ativo de informação.

- **Vulnerabilidade:** os ativos de informação, que suportam os procedimentos de negócio, contêm vulnerabilidades. É de suma importância destacar que essas vulnerabilidades estão presentes nos próprios ativos, ou seja, que são característicos a eles, e não de origem externa.
  As vulnerabilidades são as fraquezas presentes nos ativos de informação que poderiam ser exploradas, propositadamente ou não, resultando assim na quebra de um ou mais dos princípios de segurança da informação. Os ativos podem ser classificados em tecnologias, pessoas, processos e ambientes, algumas vulnerabilidades são relacionadas a seguir, como exemplo:
  - **Tecnologias:** computadores são vulneráveis pelo fato de serem construídos para transferência e armazenamento de dados, quer seja por meio de disquetes, CD,

portas USB ou portas de acesso à rede local e Internet. Os dispositivos de armazenamento podem ser explorados por Vírus, *Worms*, Cavalos de Tróia, Negação de Serviço, e outros.

- Pessoas: as pessoas, por natureza, tendem a revelar informações de trabalho para outras pessoas de confiança, sejam pessoas da própria empresa, de uma empresa rival ou mesmo para amigos. Pessoas possuem sentimentos de todos os tipos, que podem se explorados por técnicas de engenharia social.

- Processos: por diversas vezes as empresas não criam normas e regras distintas para as relações dos funcionários com as informações da empresa. A falta de atribuição de responsabilidade pelos ativos de informação pode provocar a ausência de compromisso para como os ativos de informação.

- Ambientes: os ambientes estão propícios a incêndios, enchentes, terremotos e outras tragédias. Outra vulnerabilidade é o acesso, que acidentalmente pode ser realizado por individuo não autorizado.

Pode-se notar que essas vulnerabilidades pertencem aos ativos de informação e não podem ser facilmente anuladas, pelo menos não sem dificultar o objetivo fundamental do ativo. Tendo isso em vista, é provável que um ativo tenha uma vulnerabilidade que nunca será realmente explorada.

- **Ameaça:** a ameaça é um agente externo ao ativo de informação, que se beneficia de suas vulnerabilidades e assim poderá quebrar os três princípios da informação suportada ou utilizada por esse ativo. Alguns exemplos de ameaça são trapaceiros, olheiros, sabotadores, vândalos, sobrecargas no sistema elétrico (que podem causar incêndio), tempestades (que podem causar inundações), vírus, *spywares, worms,* e outros.

2.1.4 Políticas de Segurança da Informação

A Política de Segurança da Informação (PSI) deve apontar a forma como as coisas devem ocorrer na empresa no que diz respeito à segurança da informação. Logo a política é um conjunto de regras, leis e metodologias que define qual será o comportamento dos indivíduos que convivem com a empresa no que diz respeito ao tratamento da informação (CAMPOS, 2007).

A política de segurança impõe os princípios e as normas que comandam a segurança da informação, significativo para restringir a escolha de técnicas e a adoção de metodologias referente ao assunto. A cultura de segurança é uma das características mais frágeis e está relacionada ao treinamento e conscientização de todos os incluídos no processo computacional, sejam eles colaboradores, técnicos ou até mesmo acadêmicos. Sem esse cuidado, qualquer técnica de segurança será imprestável pelo simples fato de estar sujeito a ataques que explorem aquela vulnerabilidade, como os famosos ataques de engenharia social.

Os mecanismos de segurança sustentam a execução da política de segurança planejada, e devem estar engajados com suas exigências (SERAFIM, WEBER e CAMPELLO, 2002).

Nota-se que os indivíduos e empresas não estão prontos ou qualificados para conduzir as ferramentas tecnológicas sem que ocorra algum estrago à segurança informacional, pois com esse obstáculo/barreira o fator humano faz com que a segurança fique mais suscetível a ataques quando não se tem conhecimento preliminar sobre o assunto (OLIVEIRA, MOURA e ARAÚJO, 2012).

A gestão da segurança da informação compreende muito mais do que coordenar os recursos de tecnologia, hardware e software, abrange pessoas e processos, no entanto algumas organizações esquecem este fator. A política de segurança assim como a conscientização dos usuários são algumas das maneiras de se monitorar a segurança (NETTO e SILVEIRA, 2007).

A política, de preferência, deve ser elaborada antes da episodio de problemas referentes à segurança, ou depois, impedir reincidências. Ela é um mecanismo tanto para precaver problemas legais como para registrar a ligação ao processo de controle de qualidade (FERREIRA e ARAÚJO, 2008).

De acordo com Serafim, Weber e Campelo (2002), desenvolver uma PSI global para a empresa é o primeiro passo na legitimação de critérios de segurança. Esta política de alto nível auxiliará a determinação de linhas mestras para a gestão da Segurança da Informação que será desenvolvida. E documentos distintos mais detalhados são desenvolvidos mediante ao desenvolvimento destas linhas mestras. Na prática, esse desenvolvimento será dirigido pela análise de riscos e terá desde requisitos para a educação de segurança (cultura) até sequelas das violações da própria política.

Todos os atos realizados dentro de uma organização contribuem, ou no mínimo deveriam contribuir, para os propósitos maiores dessa organização. A PSI deve da mesma forma, contribuir para esses propósitos, caso contrário, será um instrumento sem valor para a empresa e, em consequência não será usada de fato (CAMPOS, 2007).

Ressalta-se que as políticas, normas e métodos de Segurança da Informação devem ser (FERREIRA e ARAÚJO, 2008):

- **Clara;**
- Compreensível (escritas de maneira simples e concisas);
- Autenticadas e assinadas pela Alta Gerência;
- Estruturadas de maneira que permita a sua implantação por fases;

- Alinhadas com as técnicas de negócio da organização, padrões e processos que já existem;
- Orientadas aos riscos (qualquer parâmetro de proteção das informações deve conduzir para as ameaças da organização);
- Adaptável (flexíveis aos novos requerimentos de tecnologia e negócio);
- Protetores dos ativos de informações, sobrepondo os de maior valor e de maior importância;
- Positiva e não somente concentradas em práticas proibitivas ou punitivas.

A PSI deve sempre estar sendo revisada, pois com o passar do tempo às necessidades mudam. Nota-se que a segurança por meio do desconhecimento (também conhecido na literatura como: Security Through Obscurity), está tendo um enfoque muito grande e com isso está sendo muito adotado atualmente, o que é considerado como uma postura muito perigosa. Ao adotar este enfoque, vários domínios confiam que estão seguros pelo simples fato de imaginarem que ninguém sabe a seu respeito (SERAFIM, WEBER e CAMPELLO, 2002).

Neste contexto existem alguns possíveis controles que podem ser implementados com a PSI, que são (CAMPOS, 2007):

- Inventário dos ativos de informação;
- Definição de proprietários para cada um dos ativos;
- Criação de normas para como utilizar os ativos;
- Regras para a classificação da informação;
- Rotulação e tratamento da informação.

2.1.5 Visão Geral das Ferramentas e Técnicas de Segurança

A segurança, em seu nível lógico, diz respeito ao acesso que pessoas têm às aplicações residentes em cenários informatizados, não importando o tipo de aplicação ou o tamanho do computador. As ferramentas de controle são, em sua maioria, “ocultas” aos olhos de indivíduos externos aos ambientes de informática, sendo reconhecidas somente no momento em que tem seu acesso obstruído pelo controle de acesso (CARUSO e STEFFEN, 1999).

Novos mecanismos, técnicas mais eficazes e regulamentos internacionais para a Gestão da Segurança da Informação são frequentemente desenvolvidos, estimulados por organismos governamentais e organizações apreensivas com o atual estágio de vulnerabilidade da maioria das instalações computacionais (SERAFIM, WEBER e CAMPELLO, 2002).

Espontaneamente, as atuais empresas vêm investindo cada vez mais em novas tecnologias, com o intuito de equipar o seu pessoal com as melhores ferramentas e sistemas,

principalmente, aqueles associados diretamente com o método de negócio. Esse olhar voltado aos métodos, indivíduos e tecnologia vem significando o sucesso de várias empresas no mercado atual, desta forma, tornou-se o centro das atenções, sobretudo, para a SI (RANGEL, 2015).

Neste contexto, irão ser mostradas algumas das técnicas e ferramentas mais importantes para tornar seguro sistemas (COULOURIS et al., 2013):

- **Criptografia:** criptografia é o processo de codificar uma mensagem de forma a esconder seu conteúdo. A criptografia contemporânea conta com inúmeros algoritmos de segurança para cifrar e decifrar mensagens embasadas no uso de segredos denominadas chaves. Uma chave de criptografia é um critério utilizado em um algoritmo de criptografia de tal forma que a criptografia não possa ser revertida sem a consciência da chave.
  Existem duas categorias principais de algoritmo de criptografia de modo geral. A primeira usa chaves secretas compartilhadas - o remete e o destinatário devem partilhar o conhecimento da chave e a mesma não deve ser divulgada a mais ninguém. A segunda categoria de algoritmos de criptografia utiliza pares de chave pública/privada o remetente de uma mensagem usa uma chave pública – que já foi reportada pelo receptor – para cifrar a mensagem. O destinatário utiliza uma chave privada equivalente, para decifrar a mensagem. Apesar de muitos outros possam inspecionar a chave pública, somente o destinatário pode decifrar a mensagem, já que apenas ele detém a chave privada.
- **Usos da criptografia:** a criptografia exerce três papéis de suma importância na implementação de sistemas seguros, que são a) segredo e integridade; b) autenticação e c) assinaturas digitais, vistas a seguir:
  - Segredo e integridade: a criptografia é utilizada para manter o segredo e a integridade da informação, no momento em que a informação é exposta a ataques em potencial, como durante a transmissão em redes vulneráveis à intromissão e á falsificação de mensagens. Este uso da criptografia refere-se à sua função clássica em atividades militares e de inteligência. É explorado o fato de que uma mensagem cifrada que possui uma chave de criptografia específica só pode ser decifrada pelo destinatário que tenha conhecimento da chave correspondente para decifrar.
  Desse modo se mantém o segredo da mensagem cifrada, contanto que a chave para decifrar não seja comprometida (revelada a quem não faz parte da comunidade) e que o algoritmo de criptografia seja eficiente o suficiente para neutralizar todas as tentativas prováveis de violá-lo. A criptografia também sustenta a integridade da informação cifrada, visto que é possível incluir e verificar algum tipo de informação repetida, como uma soma de verificação.
  - Autenticação: a criptografia é empregada no suporte de ferramentas de autenticação da comunicação entre pares de principais. Um principal (indivíduo que possui a chave) que cifra uma mensagem com sucesso, utilizando uma chave

em particular, pode supor que a mensagem é verdadeira se ela tiver uma soma de verificação correta, ou alguém outro valor previsto, se for usado o modo de criptografia com encadeamento de blocos.

Com isso, pode-se deduzir que o emissor da mensagem possui a chave de cifragem equivalente e, daí, concluir a identidade de remetente, contanto que a chave seja de conhecimento apenas das duas partes. Dessa forma, se as chaves forem mantidas em segredo, um procedimento de decifrar bem-sucedido autenticará a mensagem como sendo derivada de um remetente em especial.

- Assinaturas digitais: a criptografia é utilizada para implementar um mecanismo conhecido pelo nome de assinatura digital, isso aparenta a função das assinaturas convencionais, validando com um outro elemento se uma mensagem se uma mensagem, ou um documento, é uma réplica autêntica do que foi proveniente do signatário.

Logo, as técnicas de assinatura digital são fundamentadas em um vínculo irreversível na mensagem ou documento de um segredo que apenas o signatário tem conhecimento. Isto pode ser alcançado cifrando-se a mensagem, ou ainda melhor, um estado compactado da mensagem, conhecido como resumo (*digest*), utilizando apenas uma chave que seja de conhecimento apenas pelo signatário. Um resumo é um valor de comprimento fixo, calculado pela aplicação de uma função de resumo segura (*secure digest fuction).*

- **Certificados:** Um certificado digital é um documento que contém uma declaração (geralmente curta) assinada por um principal. Os certificados podem ser utilizados para determinar a autenticidade de vários tipos de declarações. Para tornar os certificados fundamentais, duas coisas são essenciais:

  - Um formato único e uma representação para eles, de maneira que os emissores e os usuários do certificado sejam capazes de ter êxito em construí-los e entendê-los.
  - Acordo sobre o modo pelo qual os encadeamentos de certificados são construídos e, em especial, sobre a noção de autoridade confiável.

- **Controle de acesso:** os servidores obtêm mensagens de pedidos da forma <op, principal, recurso>, em que op é a operação solicitada, principal é uma identidade ou um grupo de credenciais do principal que está realizando o pedido e recurso reconhece o recurso no qual a operação será realizada. O servidor deve primeiro autenticar a mensagem de requerimento e as credenciais do principal e, após, aplicar o controle de acesso, indeferindo qualquer pedido para o qual principal requerente não tenha os direitos de acesso necessários para efetuar a operação requerida no recurso especificado.

  As decisões de controle de acesso geralmente são deixadas para o código em nível de aplicativo, porém é propiciado suporte genérico para grande parte da ferramenta que suporta as decisões. O que inclui a autenticação de principal, a assinatura e autenticação dos pedidos e o gerenciamento de credenciais e informações sobre os direitos de acesso. Alguns conceitos que estão relacionados com o controle de acesso são os Domínios de proteção e a Implementação, que são:

  - Domínios de proteção é um ambiente de execução compartilhado por um grupo de processos, ele possui um conjunto de pares <recursos, direitos>, enumerando os

recursos que podem ser acessados por todos os processos em execução incluso no domínio e especificando as operações que são permitidas em cada um dos recursos, geralmente, um domínio de proteção está ligado a um principal.

- Implementação, as assinaturas digitais, credenciais e certificados de chave pública fornecem a base de criptografia para um controle de acesso seguro. Canais protegido oferecem benefícios para o desempenho, autorizando que inúmeros pedidos sejam manipulados se a necessidade de verificação repetida dos principais e credenciais (WOBBER et al., 1994).

- **Credenciais:** credenciais é um grupo de evidências oferecidas por um principal ao requerer acesso a um recurso. No caso mais simples, um certificado de uma autoridade importante informando a identidade do principal já basta, e isso seria utilizado para averiguar as permissões do principal em uma lista de controle de acesso. Geralmente, isso é tudo que é solicitado, ou fornecido, no entanto o conceito pode ser difundido para lidar requisitos bem mais sutis.

  Assim, não é interessante solicitar que os usuários interatuem com o sistema e autentiquem a si mesmo, toda vez que a sua autorização for requisitada para executar uma operação em um recurso protegido. Ao invés disso, é introduzida a consciência de que uma credencial simboliza um principal. Sendo assim, o certificado de chave pública de um usuário corresponde a esse usuário, qualquer processo que receba uma requisição autenticada com a chave privada do usuário pode considerar que a requisição foi feita por esse usuário.

  Dessa forma, uma maneira particularmente útil de credencial é aquela que favorece um principal ou então um processo que está atuando para um principal, a realizar uma ação com a autoridade de outro principal. Pode haver uma necessidade de delegação em qualquer circunstância em que um serviço necessite acessar um recurso protegido para finalizar uma ação em nome de seu cliente.

  Portanto, a delegação pode ser conseguida utilizando-se um certificado de delegação ou uma capacidade. O certificado é assinado pelo principal solicitante e ele viabiliza outro principal (um servidor de impressão, por exemplo) acessar um recurso nomeado (o arquivo a ser impresso).

- **Firewalls:** eles protegem intranets, fazendo ações de filtragem em comunicações recebidas e enviadas. O *firewall* é considerado um mecanismo de segurança.

  Com isso, a facilidade com que as mensagens de pedidos podem ser enviadas para qualquer servidor, em qualquer parte, e o fato de que inúmeros servidores não são criados para aguentar ataques maldosos de *hackers* e erros acidentais torna simples o vazamento de informações designadas para serem confidenciais. Elementos não desejáveis também podem adentrar na rede de uma empresa, deixando que programas *worms* e vírus acessem seus computadores.

  Os *firewalls* elaboram um ambiente de comunicação local em que toda a comunicação externa é interceptada. As mensagens são direcionadas para o destinatário local planejado somente para comunicações explicitamente autorizadas. O acesso às redes internas pode ser controlado por *firewalls* porém o acesso a serviços públicos na internet e sem restrições, já que seu objetivo é oferecer serviços para uma extensa gama de usuários.

2.2 Trabalhos Relacionados

Abaixo estão descritos os trabalhos de: (i) Mesquita (2015); (ii) Albuquerque e Santos (2015); (iii) Marinho et al. (2017); (iv) Galegale, Fontes e Galegale (2017) e (v) Souza et al. (2018). Estes trabalhos apresentam resultados relevantes para este trabalho, conforme descritos na Tabela 2 que mostra um comparativo da proposta com os trabalhos relacionados:

2.2.1 Mesquita (2015)

O trabalho de Mesquita (2015) apresentou a descrição de que no cenário atual todas as empresas precisam da tecnologia para poder gerir o negócio, seja, armazenando dados, realizando consultas ou fazendo transações, pode-se dizer que todas estão sujeitas a ataques cibernéticos ou até mesmo ataques por meio de engenharia social. Visando mitigar a perda de ativos e garantir uma maior segurança, as empresas precisam desenvolver uma PSI, onde descreve o que deve ser feito e o que não pode ser feito, levando em consideração os pilares da segurança de informação.

O objetivo do trabalho de Mesquita (2015) foi expor a importância da informação para a empresa, e mostrar como desenvolver um documento que guie os usuários de modo que traga segurança às informações e aos recursos de TI, documento este denominado como PSI. Sabendo da importância deste documento, é necessário saber entender como proceder no desenvolvimento e é neste ponto que o trabalho irá focar, esclarecendo os pontos que precisam ser utilizados como parâmetros, e apresentando um modelo de política da informação, que pode ser utilizado para desenvolver outros para qualquer outro tipo de organização.

A metodologia utilizada no trabalho de Mesquita (2015) não ficou clara, porém o autor relata os passos que seguiu, inicialmente foi realizado o levantamento de todos os ativos da organização, e os riscos que estão passíveis de sofrer. Após realizar a análise dos riscos da organização, obteve-se uma base sólida para desenvolver a política de segurança, porém foi necessário buscar embasamento em normas para mostrar que o documento além de necessário era um item comum nas organizações de médio à grande porte. Para o embasamento foi utilizado a norma ISO/IEC 27002:2005 que contribuiu para a elaboração do documento PSI.

Junto com a norma ISO/IEC 27002:2005, também foi utilizado como estrutura e forte aliado na apresentação para aceitação de política de alguns itens da constituição federal e Código Penal. A política de segurança desenvolvida foi separada em tópicos, para deixar mais

didático e para facilitar a busca de determinado item. A elaboração foi realizada apenas por uma pessoa, e iniciada sem uma autorização prévia da diretoria, a elaboração da PSI durou um mês (MESQUITA, 2015).

Sendo assim como resultado do trabalho de Mesquita (2015) obteve-se um modelo de PSI que foi desenvolvido realizando uma análise e verificação dentro de uma empresa do Distrito Federal, que comercializa um plano próprio de saúde ambulatorial.

2.2.2 Albuquerque e Santos (2015)

O trabalho de Albuquerque e Santos (2015) introduz que as organizações dispõem de uma série de medidas de Segurança da Informação recomendadas por normas internacionais e pela literatura, mas a adoção deve ser balizada pelas necessidades específicas identificadas pela Governança da Segurança da Informação de cada organização, embora possa ser influenciada por pressões do ambiente institucional em que as organizações estão inseridas.

O objetivo do trabalho de Albuquerque e Santos (2015) foi o de investigar se nos institutos de pesquisa públicos a adoção de medidas de Segurança da Informação é influenciada por fatores organizacionais, relativos à Governança da Segurança da Informação, e por fatores externos, relativos ao ambiente institucional em que estão inseridos.

A metodologia adotada para a identificação dos fatores que influenciam a adoção de medidas de Segurança da Informação foi feita uma pesquisa de opinião (*Survey*). A pesquisa documental consistiu em consultas a PSI, sistemas de gestão da Segurança da Informação e planos diretores de TI, documentos que formalizam a estrutura de Governança da Segurança da Informação ou que tratam do alinhamento estratégico da Segurança da Informação nas organizações. Para localizar os documentos, foram realizadas buscas nos websites dos 22 institutos de pesquisa e na ferramenta de busca Google (ALBUQUERQUE e SANTOS, 2015).

Para realizar o *Survey*, foram elaboradas perguntas sobre os indicadores, que foram incluídas em um formulário eletrônico. Na primeira parte do formulário, o participante deveria responder algumas informações com relação a temática que o trabalho se propôs. A segunda parte do formulário tinha 14 perguntas, uma para cada indicador do modelo de análise, exceto aqueles investigados através de pesquisa documental. As perguntas tinham o objetivo de verificar se os institutos de pesquisa estão sujeitos à influência dos indicadores do

modelo de análise para a adoção de medidas de Segurança da Informação (ALBUQUERQUE e SANTOS, 2015).

Como resultados obtidos, Albuquerque e Santos (2015) conseguiram mostrar que o ambiente institucional influencia a adoção de medidas de Segurança da Informação na maioria dos institutos de pesquisa públicos que participaram da pesquisa. Essa influência se dá principalmente por meio de leis, decretos e outros regulamentos publicados pelo Governo e da participação de profissionais de TI e Segurança da Informação em redes de troca de experiências e informações.

A Governança da Segurança da Informação também influencia a adoção de medidas, mas o principal indicador de influência é a definição e adoção de normas e padrões internos de Segurança da Informação. O trabalho mostrou também que as medidas de Segurança da Informação mais adotadas pelos institutos de pesquisa são principalmente técnicas ou físicas, como execução de rotinas de backup, utilização de no-breaks, sistemas anti-spam e ativos com partes redundantes (ALBUQUERQUE e SANTOS, 2015).

2.2.3 Marinho et al. (2017)

O trabalho de Marinho et al. (2017), visa mostrar que o valor da informação se mostra como um fator de sucesso para muitas organizações, pois as mesmas investem em equipamentos de segurança e softwares sofisticados com um intuito de fortalecer a segurança de suas informações, mas mesmo assim, enfrentam uma grande ameaça bastante recorrente: os ataques de Engenharia Social, realizados por indivíduos que buscam romper barreiras de segurança para ganhos próprios. A segurança da informação busca preservar o valor da informação, desta maneira, a Engenharia Social torna-se uma adversária muito perigosa que pode causar danos a ela.

O trabalho de Marinho et al. (2017), teve como objetivo descrever os resultados de uma investigação sobre as principais ameaças a Segurança da Informação nas organizações, além disso eles apresentaram o tema Engenharia Social e exporão quais são as principais técnicas utilizadas pelos engenheiros sociais.

No trabalho de Marinho et al. (2017), a metodologia científica adotada na pesquisa foi baseada em um estudo denominado MS que fornece uma visão geral de uma área de pesquisa, identificando a quantidade, os resultados disponíveis, além das frequências de publicações ao

longo do tempo para identificar tendências. As publicações utilizadas na identificação para responder às questões de pesquisa um e dois foram selecionadas após o 2º filtro.

Em relação aos resultados das questões, a primeira questão de pesquisa "Quais as principais ameaças à segurança da informação nas organizações?", foi possível perceber que quase todas as publicações citam a Engenharia Social como principal ameaça à segurança da informação. Sobre a segunda questão "Quais as técnicas utilizadas pela engenharia social?", foi identificado que há uma técnica predominante em todos os artigos: *Phishig*.

Como resultado foi obtido que a Engenharia Social é a principal ameaça à segurança da informação devido à facilidade de veiculação da informação e a ingenuidade e confiança das pessoas. No que se refere às técnicas, pode-se citar o *Phishing* como a mais utilizada, segundo as pesquisas selecionadas. Essa técnica estimula pessoas a fornecer dados pensando que serão disponibilizados a pessoas ou organizações de sua confiança, quando na verdade são fornecidos a engenheiros sociais que se aproveitam da ingenuidade das pessoas, pois sabem explorar com sutileza o fator humano (MARINHO et al., 2017).

2.2.4 Galegale, Fontes e Galegale (2017)

O trabalho de Galegale, Fontes e Galegale (2017) visa compreender os controles citados nas PSI das organizações, o cenário do valor da informação para as organizações, a importância de proteger tais informações, os avanços tecnológicos e a exposição a tais ameaças, bem como a multiplicidade de controles disponíveis.

O trabalho teve como objetivo identificar a existência de controles recorrentes. Para melhor direcionar o estudo, o problema da pesquisa foi assim enunciado: Há controles citados nas políticas de segurança da informação das organizações de forma recorrente? Quais? O objetivo principal do trabalho foi responder a essa questão (GALEGALE, FONTES e GALEGALE, 2017).

A metodologia utilizada no trabalho de Galegale, Fontes e Galegale (2017) foi a abordagem de pesquisa qualitativa, com objetivo descritivo e como procedimentos, pesquisa bibliográfica. No trabalho foi utilizado o estudo de casos múltiplos com dez organizações brasileiras selecionadas de forma intencional, portanto não probabilística. O convite às organizações para participar da pesquisa foi decorrente da condição de possuírem maturidade na política considerada, de pelo menos três anos de uso. Foram realizadas entrevistas com o profissional que tem a responsabilidade pela segurança da informação de cada organização.

Os profissionais entrevistados de todas as organizações possuíam mais de cinco anos de experiência profissional em atividades de segurança da informação, evidenciando com isto a maturidade profissional das informações coletadas nas entrevistas. Em relação à formação formal de especialização na área de segurança da informação, 50% dos profissionais possuem certificações internacionais. Todas as organizações pesquisadas possuíam políticas há vários anos, sendo que 90% há mais de cinco anos e apenas 10% há menos de cinco anos (GALEGALE, FONTES e GALEGALE, 2017).

Nos resultados obtidos do trabalho de Galegale, Fontes e Galegale (2017) teve como base que os levantamentos de campo por meio do estudo de casos, apoiado pela pesquisa bibliográfica, possibilitaram uma coleta de informações detalhada e aprofundada, permitindo a compilação dos controles das políticas de segurança da informação de modo sistematizado. Foram identificados 40 controles citados de forma recorrente em políticas, os quais também foram associados à principal referência da literatura da área, descritos e agrupados em quatro extratos de frequência: 12 controles citados por 100% das políticas, 15 por 90%, 16 por 80% e 40 por 70%.

2.2.5 Souza et al. (2018)

O trabalho de Souza et al. (2018), apresenta um contexto sobre a relevância do assunto da segurança da informação presente nos ambientes organizacionais. Afirmando que mundo está cada vez mais sistematizado com o avanço dos recursos tecnológicos da informação. Esses recursos deixaram de ser parte exclusiva de grandes corporações e atualmente fazem parte da vida de cidadãos comuns e, consequentemente, de organizações de pequeno e médio porte. As tecnologias digitais visam reinventar e mudar a forma como antigas e atuais tarefas eram e são realizadas, através do uso de aplicações e recursos de softwares, hardwares, redes etc.

O trabalho teve como objetivo geral compreender os mecanismos de segurança da informação utilizados na atuação de possíveis ameaças no ambiente organizacional de uma empresa que atua ofertando serviços de planos de saúde na cidade de Mossoró, Rio Grande do Norte e como seus objetivos específicos: a identificação de possíveis ameaças presentes no ambiente do negócio; conhecer os mecanismos usados que visam combater essas ameaças; analisar esses mecanismos em função das ameaças que visam combater (SOUZA et al., 2018).

A metodologia utilizada para o trabalho de Souza et al. (2018) foi uma pesquisa do tipo descritiva e qualitativa. A pesquisa foi realizada em uma organização que atua com

serviços de planos de saúde, localizada na cidade de Mossoró, Rio Grande do Norte. Para a realização da pesquisa os autores elaboraram um questionário contendo 10 questões, objetivando identificar os mecanismos de segurança utilizados e as possíveis ameaças presentes na organização.

A pesquisa foi realizada por meio de um dos pesquisadores, onde foi realizada uma entrevista presencial com um analista de sistemas e um gestor do departamento de TI. A coleta dos dados se deu por meio de gravações das falas, sendo realizadas no mês de setembro de 2017. Apesar de a pesquisa ter sido realizada em um ambiente organizacional de planos de saúde, vale ressaltar que os participantes foram profissionais da área de TI, como se pode observar na Tabela 1.

Tabela 1 - Caracterização dos sujeitos e pesquisa

Código do entrevistado	Sexo	Idade	Estado civil	Escolaridade	Cargo	Tempo de trabalho na organização
E1	M	38	Casado	Pós-graduado	Gerente de TI	14 anos e 2 meses
E2	M	37	Casado	Bacharelado em Sistemas de Informação	Analista de sistemas	3 anos e 5 meses

Fonte: Adaptado de Souza et al. (2018).

O trabalho de Souza et al. (2018) utilizou o método ANS – Análise do Núcleo de Sentido para a análise dos dados.

Como resultado do trabalho de Souza et al. (2018) foi possível concluir que a organização alvo da pesquisa utiliza mecanismos de segurança comuns, os quais se encontram presentes na maioria das organizações, porém a mesma possui limitações em demonstrar que não inovam em recursos de segurança, e acabam dependendo apenas dos já existentes.

Assim como identificar que setor de TI da organização não realiza tarefas importantes para diminuir a exposição de riscos que venham a surgir com mudanças nos requisitos das atividades do negócio, não seguindo nenhum conjunto de normas, e apresentando também pouco conhecimento sobre o assunto conforme mostram as falas dos entrevistados, mantendo assim um processo informal de segurança de informação, e mostrando a necessidade de aprofundamento no assunto por parte do setor de TI da organização (SOUZA et al., 2018).

2.2.6 Comparativo da Proposta com os Trabalhos Relacionados

A Tabela 2 abaixo mostra as principais características dos trabalhos relacionados com o intuito de demostrar um comparativo com a proposta desse trabalho.

Tabela 2 - Comparativo com os trabalhos relacionados

Trabalhos Relacionados	Comparativo com a proposta
Mesquita (2015)	O trabalho de Mesquita (2015) buscou mostrar a importância da informação para a empresa e mostrar como desenvolver um documento que guie os usuários, chamado de PSI. O trabalho teve o foco de mostrar os pontos que precisam ser utilizados para a criação do PSI, a metodologia utilizada por Mesquita (2015) não fica clara, no entanto ele relata que ocorreu um levantamento dos ativos da organização, assim como os riscos passíveis a esses ativos e foi utilizada a ISO/IEC 27002:2005 para o embasamento do documento PSI. Este trabalho utilizou a metodologia de MS para levantar as principais publicações relacionadas ao tema, especialmente sobre as recomendações de segurança da informação no contexto das organizações. Principais assuntos abordados: A importância da informação para a empresa e um modelo de PSI.
Albuquerque e Santos (2015)	O trabalho de Albuquerque e Santos (2015) busca investigar se nos institutos de pesquisa públicos a adoção de medidas de Segurança da Informação é influenciada por fatores organizacionais e por fatores externos. A metodologia utilizada para alcançar respostas para as questões foi por meio de uma pesquisa de opinião (*Survey*) que continha algumas questões sobre o tema do trabalho e contava com 14 questões sobre cada indicador do modelo de análise, e uma pesquisa documental, para a localização de tais documentos foi realizadas buscas nos websites dos 22 institutos de pesquisa e na ferramenta de busca do Google. A proposta também trata do problema de adoção de medidas de Segurança da Informação, no entanto não se trata de institutos de pesquisa, e nem dos fatores para essa adoção e sim sobre as medidas que podem ser realizadas (recomendações apresentadas na literatura sobre Segurança da Informação) por meio de pesquisas publicadas em bibliotecas digitais e fontes manuais, que esta pesquisa se propôs a fazer. Principal assunto abordado: Influência de inúmeros fatores para a adoção de medidas de Segurança da Informação.
Marinho et al. (2017)	O trabalho de Marinho et al. (2017) investigou dois dos maiores problemas da área de Segurança da Informação no que se refere as organizações, que são: (i) principais ameaças a Segurança da Informação e (ii) sobre a Engenharia Social e quais as principais técnicas utilizadas pelos engenheiros sociais. Foi proposta a metodologia MS para a investigação das respostas das questões de pesquisa (i) e (ii). Este trabalho também trata da questão das ameaças a Segurança da Informação, mas não se limita a apenas isso, o MS também foi utilizado para fornecer resposta sobre as recomendações para as organizações, com o objetivo de contribuir no combate às ameaças existentes. Principais assuntos abordados: Ameaças a Segurança da Informação nas organizações e Engenharia social.

Galegale, Fontes e Galegale (2017)	O trabalho de Galegale, Fontes e Galegale (2017), buscou compreender os controles citados nas PSI das organizações, onde seu maior objetivo foi identificar a existência de controles recorrentes, para o melhor direcionamento do estudo o problema da pesquisa ganhou um enunciado que foi: (i) Há controles citados nas PSI das organizações de forma recorrente? Quais? O método utilizado foi uma pesquisa qualitativa e uma pesquisa bibliográfica e a amostra da pesquisa qualitativa foi de dez organizações brasileiras. Este trabalho também visa identificar controles, no entanto não se trata de compreender os que são citados nas PSI, e sim identificar quais são os controles que podem ser implantados nas organizações. Os resultados foram obtidos por meio do MS para a identificação de publicações que relatam sobre tais controles. Principal assunto abordado: Controles citados nas PSI.
Souza et al. (2018)	O trabalho de Souza et al. (2018) buscou compreender os mecanismos de Segurança da Informação utilizados na atuação de possíveis ameaças no ambiente organizacional, o trabalho contou com três questões principais que foram: (i) a identificação de possíveis ameaças presentes no ambiente do negócio (ii) conhecer os mecanismos usados que visam combater essas ameaças e (iii) analisar esses mecanismos em função das ameaças que visam combater. O alvo de pesquisa do trabalho foi uma empresa que atua oferecendo serviços de planos de saúde, localizada na cidade de Mossoró, Rio Grande do Norte. Foi utilizada uma pesquisa tanto descritiva quanto qualitativa na respectiva empresa, contou com um questionário de 10 questões e entrevista presencial com dois profissionais da área de TI. Este trabalho também busca identificar mecanismos que são utilizados para combater ameaças, no entanto a estratégia para obter esses resultados é completamente diferente, já que foi utilizada a metodologia MS, que contou com todas as publicações que fazem referência ao tema como base de análise para responder as questões do trabalho, tendo isso em vista o resultado é mais expressivo, pois serão identificados mais ameaças e mecanismos de defesa. Principal assunto abordado: Segurança da Informação em uma empresa.

Fonte: A autora (2019).

3 ESTUDO REALIZADO E RESULTADOS OBTIDOS NO MAPEAMENTO SISTEMÁTICO

Nesta seção, será apresentado o Planejamento do MS, os objetivos da pesquisa são listados e é definido o protocolo, onde será composto pela definição das questões de pesquisas, estratégias de busca, fontes de pesquisa, string de busca e critérios de seleção. Assim como a condução do MS.

3.1 Planejamento do Protocolo

3.1.1 Definição do Objetivo e Questões de Pesquisa

O objetivo dessa pesquisa está estruturado segundo o paradigma GQM (*Goal/Question/Metric*) (BASILI et al., 1994), apresentado na Tabela 3 a seguir.

Tabela 3 - Objetivo segundo o paradigma GQM

Verificar	As recomendações sobre segurança da informação que podem ser utilizadas nas organizações
Com o propósito de	Identificar
Com relação a	Vulnerabilidades, esforços e políticas existentes na literatura para a proteção das informações
Do ponto de vista do	Pesquisador
No contexto	Organizacional

Fonte: A autora (2020).

Baseados no objetivo da pesquisa foram formuladas duas questões de pesquisa principais, as quais são apresentadas a seguir:

- Q1 – Quais são as recomendações sobre Segurança da Informação indicadas para manter a proteção dos dados no contexto das organizações?
- Q2 – Quais são as ameaças, vulnerabilidades e/ou comportamento de riscos relatados nas recomendações de segurança da informação da literatura?

3.1.2 Fontes de Pesquisa e String de busca

Os idiomas escolhidos são o Inglês (devido à sua adoção pela maioria das conferências, periódicos e editoras da área de pesquisa) e o Português (para incluir trabalhos técnicos publicados em conferências nacionais).

A busca foi restringida usando-se palavras-chave específicas para encontrar as publicações de interesse. A expressão de busca foi definida de acordo com dois dos quatro aspectos indicados em [Peterson et al., 2008]: População e Intervenção, conforme a Tabela 4.

Tabela 4 - Expressão de busca utilizada para identificar as publicações

Para investigação por busca manual (no idioma Português):

- **População:** Publicações que fazem referências à Segurança da informação nas organizações (e sinônimos)
  - *Palavras-chave:* "indústria" OR "organização".
- **Intervenção:** Ameaças, vulnerabilidades, técnicas de segurança, políticas de segurança, controles (e sinônimos)
  - *Palavras-chave:* ("mecanismos de segurança da informação" OR "ameaças de segurança da informação" OR "invasão a segurança da informação" OR "vulnerabilidades à segurança da informação" OR "técnicas de segurança da informação" OR "políticas de segurança da informação" OR "conscientização sobre segurança da informação".

Para investigação por expressão de busca (no idioma Inglês):

- **População:** Publicações que fazem referências à Segurança da informação nas organizações (e sinônimos)
  - *Palavras-chave:* "industry" OR "organization".
- **Intervenção:** Ameaças, vulnerabilidades, técnicas de segurança, políticas de segurança, controles (e sinônimos)
  - *Palavras-chave:* "information security mechanisms" OR "information security threats" OR "invasion of information security" OR "information security vulnerabilities" OR "information security techniques" OR "information security policies" OR "information security awareness".

Fonte: O autor (2019).

Como pode ser observado na Tabela 4 acima, os termos referentes à população e intervenção apresentaram variações de singular e plural.

As fontes de pesquisa para a obtenção dos resultados utilizada foram bibliotecas digitais e fontes manuais, conforme listadas abaixo:

1. Bibliotecas digitais:
   - Scopus: <https://www.scopus.com>;
   - IEEE: <https://ieeexplore.ieee.org>;
2. Fontes Manuais
   - SBSeg: Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais;
   - SBSI: Simpósio Brasileiro de Sistemas de Informação;
   - SBRC: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.

A String de busca utilizada para as bibliotecas é genérica, houve adaptações para a forma que cada biblioteca recebe as strings, a seguir veremos a string da Tabela 4 adaptada para as bibliotecas na Tabela 5.

Tabela 5 - String de busca por base

Base	String
IEEE	(("All Metadata":"industry" OR "organization") AND "All Metadata":"information security mechanisms" OR "information security threats" OR "invasion of information security" OR "information security vulnerabilities" OR "information security techniques" OR "information security policies" OR "information security awareness")
Scopus	(TITLE-ABS-KEY ("industry" OR "organization") AND TITLE-ABS-KEY ("information security mechanisms" OR "information security threats" OR "invasion of information security" OR "information security vulnerabilities" OR "information security techniques" OR "information security policies" OR "information security awareness"))

Fonte: A autora (2020).

3.1.3 Critérios de Seleção

A pesquisa se restringiu à análise de publicações disponíveis entre a data dos anos de 2013 – 2020 e as publicações deveriam estar disponíveis na Web ou por meio do contato com os autores. A seleção das publicações foi realizada em quatro etapas:

(1) Busca preliminar das publicações coletadas nas fontes definidas.
(2) Análise do título, do resumo e das palavras-chave e aplicando o critério de seleção "CS1: possuir informações sobre recomendações de Segurança da Informação que podem ser utilizadas nas organizações".
(3) Leitura completa das publicações e aplicando o critério de seleção CS1, assim como o critério de seleção "CS2: possuir informações sobre ameaças, vulnerabilidades e/ou comportamento de riscos relacionados à segurança da informação".
(4) Extração dos dados.

Qualquer estudo que não satisfez a todos os critérios citados foi excluído.

3.1.4 Procedimento de Extração de Dados

Foram extraídas informações de publicações relevantes para a pesquisa, que foram registradas em tabelas, conforme os campos abaixo, descritos na Tabela 6.

Tabela 6 - Campos de coleta de dados

Identificador	Indica o ID para o trabalho
A) Dados da publicação:	
Título:	Indica o título do trabalho
Autor (es):	Nome dos autores
Fonte de Publicação:	Local de publicação
Ano de Publicação:	Ano de Publicação
Resumo:	Texto contendo uma descrição do resumo
B) Dados derivados do objetivo:	
Tipo de recomendação:	Categoria de Segurança da Informação identificada: prática, controle, técnica, ferramentas e etc.
Recomendação de Segurança da Informação:	Descrição sobre a(s) recomendação(ões) relacionada(s) à Segurança da Informação mencionada na publicação
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Relato sobre as principais ameaças, vulnerabilidades e comportamento de risco identificados na publicação
Informações Adicionais:	Relatos de experiência ou informações relevantes sobre recomendações de Segurança da Informação

Fonte: Adaptado de Kitchenham e Chartes (2007).

3.2 Condução do Mapeamento

A primeira fase que foi realizada na condução do MS foi a busca nas bibliotecas digitais que foram selecionadas na etapa anterior, para tal foi utilizada a string que foi definida para cada base. As buscas foram realizadas entre setembro e novembro de 2020. A quantidade de trabalhos encontrados foi de 1037. Abaixo se tem a Tabela 7 que mostra esses trabalhos por cada base.

Tabela 7 - Publicações encontradas por base

Base	Número de Publicações
IEEE	317
Scopus	720

Fonte: A autora (2020).

Não houve a retirada de publicações duplicadas, elas foram deixadas para que não impedissem a validade do mapeamento, no entanto eles são contados apenas como uma na extração de dados.

A fase seguinte foi definida pelo uso do primeiro critério de seleção que foi estabelecido na etapa precedente do MS, que consiste na análise do título, resumo e palavras-chave das publicações para o seguinte critério: possuir informações sobre recomendações de Segurança da Informação que podem ser utilizadas nas organizações.

Ao final desta fase foram selecionados 200 artigos, sendo assim houve a exclusão de 822 dos encontrados, destes, 15 eram duplicados, abaixo temos a Figura 8 (gráfico de Venn), que mostra exatamente como estão distribuídos os artigos restantes após a fase da aplicação do CS1, todos esses artigos estão dispostos no apêndice A.

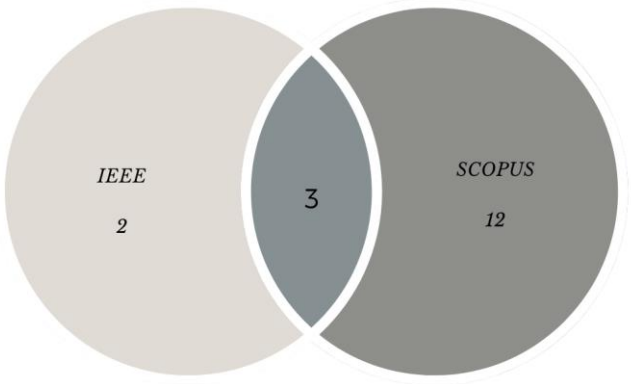
Figura 8 - Publicações Retornadas Após o 1º Critério

Fonte: A autora (2020).

A próxima fase foi definida pelo uso do segundo critério de seleção que foi estabelecido na etapa do protocolo do MS, que se refere à leitura completa das publicações aplicando o seguinte critério: possuir informações sobre ameaças, vulnerabilidades e/ou comportamento de riscos relacionados à segurança da informação.

Desta fase restaram 20 publicações eliminando assim, 198 dos que haviam restado após a aplicação do primeiro critério, desse total 03 eram duplicados, abaixo se tem a Figura 9 que demonstra como as publicações ficaram distribuídas.

Figura 9 - Publicações Retornadas Após o 2º Critério



Fonte: A autora (2020).

Além da busca de publicações nas bibliotecas digitais, também foram estabelecidas buscas por anais de evento, foram escolhidos 03 anais, os que mais se encaixavam com a proposta deste trabalho, os critérios assumidos para as buscas nos anais foram os mesmos adotados com as bibliotecas.

Foi estabelecido que a busca nos anais de evento seria feita entre os anos de 2013 até 2020, no entanto alguns eventos não tinham todos os anos de seus anais disponibilizados. No SBRC estavam disponíveis apenas de 03 anos sendo eles 2017, 2018 e 2019 respectivamente, houve um total de 253 publicações e após a aplicação do primeiro critério restou apenas um artigo, excluído assim 252 dos que foram encontrados, seguindo assim com um artigo para a análise do segundo critério no qual infelizmente não foi atendido.

Para o SBSeg foi encontrado os anais de todas os anos, exceto de 2020 pois o evento ainda não havia acontecido na data em que ocorreu o estudo, havia um total de 185 artigos, a soma total de todos os anos encontrados. Após a análise do primeiro critério restaram 03 artigos, e após a aplicação do segundo critério não foi retornado nenhum artigo que cumprisse com o mesmo.

O último evento que foi realizado o mapeamento foi o SBSI, que contava apenas com os anais de 2013 até 2018, com um total de 454 artigos em sua soma de todos os anos, após a execução do critério CS1 sobrou um total de 04 artigos. No entanto com a execução do critério CS2 não restou nenhum artigo.

Sendo assim, pode-se notar que a busca realizada nos anais de evento não trouxe nenhum artigo que pudesse responder as questões que este trabalho pretende responder. Portanto, as 20 publicações que restaram das bibliotecas digitais foram às utilizadas para a extração de dados. É importante ressaltar que dessas 20 publicações, 03 eram duplicadas, no entanto 17 é o número total de artigos das bibliotecas utilizadas, sendo assim as publicações repetidas foram extraídas apenas uma vez, os formulários de coleta de dados pode ser encontrado no apêndice B.

A seguir é apresentada na Tabela 8 as informações pertinentes sobre as publicações que serão utilizadas para a obtenção das respostas deste trabalho, assim como um gráfico (Figura 10) que mostra a quantidade de publicação sobre o referido assunto por ano.

Tabela 8 - Dados sobre as publicações

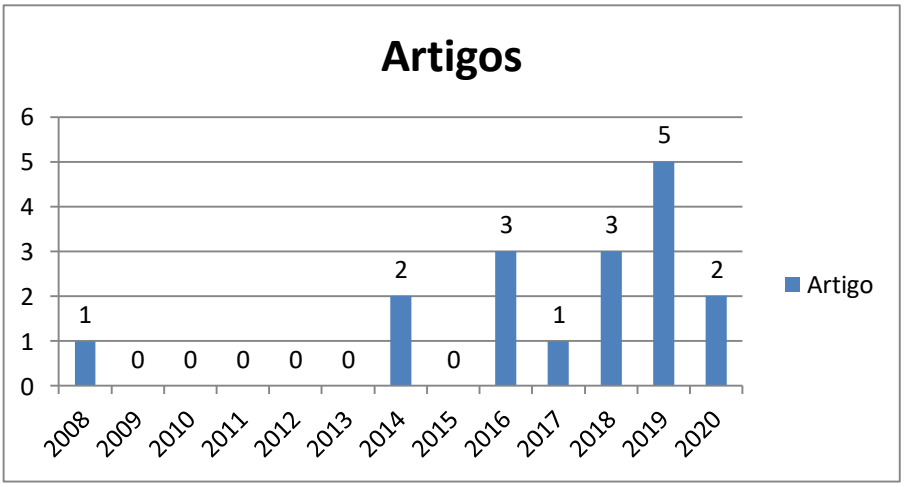
ID	Título	Autor(es)	Base/Ano
PN01	A Symptomatic Framework to Predict the Risk of Insider Threats	Joris Ikany and Husin Jazri	IEEE/Scopus/2019

PN02	Anomaly-based Insider Threat Detection using Deep Autoencoders	Liu Liu, Olivier De Vel, Chao Chen, Jun Zhang e Yang Xiang.	IEEE/Scopus/2018
PN03	Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat	Oliver Buckley, Jason R. C. Nurse, Philip A. Legg, Michael Goldsmith e Sadie Creese	IEEE/Scopus/2014
PN04	Implementation of a Socially Engineered Worm to Increase Information Security Awareness	Erlo Meister e Elmarie Biermann F'Satie	IEEE/2008
PN05	Social Engineering Attack Strategies and Defence Approaches	Ibrahim Ghafir, Vaclav Prenosil, Ahmad Alhejailan e Mohammad Hammoudeh	IEEE/2016
PN06	A Framework to Mitigate Social Engineering through Social Media within the Enterprise	Heidi Wilcox e Maumita Bhattacharya	Scopus/2016
PN07	AHP-based Security Decision Making: How Intention and Intrinsic Motivation Affect Policy Compliance	Ahmed Alzahrani e Christopher Johnson	Scopus/2019
PN08	An Evaluation of the Proposed Framework for Access Control in the Cloud and BYOD Environment	Khalid Almarhabi, Kamal Jambi, Fathy Eassa E Omar Batarfi	Scopus/2018
PN09	An Information Security Awareness Program to Address Common Security Concerns in IT Unit	Shadi Al Awawdeh e Abdallah Tubaishat	Scopus/2014
PN10	An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector	Melissa K. Chinyemba e Jackson Phiri	Scopus/2018
PN11	Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions	Hussain Aldawood e Geoffrey Skinner	Scopus/2020
PN12	Contagion in cyber security attacks	Adrian Baldwin, Iffat Gheyas, Christos Ioannidis, David Pym e Julian Williams	Scopus/2016
PN13	Demographic Factors in Cyber Security: An Empirical Study	Shweta Mittal e P. Vigneswara Ilavarasan	Scopus/2019
PN14	Deterrent Effects of Punishment and Training on Insider Security Threats: a Field Experiment on Phishing Attacks	Bora Kim, Do-Yeon Lee e Beomsoo Kim.	Scopus/2019
PN15	Developing an Information Security Policy: A Case Study Approach	Fayez Hussain Alqahtani	Scopus/2017

PN16	Identification of Information Security Threats Using Data Mining Approach in Campus Network	Norkhushaini Awang, Ganthan Narayana Samya, Noor Hafizah Hassana, Nurazean Maaropa, Pritheega Magalingama e Norshaliza Kamaruddina	Scopus/2020
PN17	Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues	Hussain Aldawood e Geoffrey Skinner	Scopus/2019

Fonte: A autora (2020).

Figura 10 - Publicações por ano de publicação



Fonte: A autora (2020).

4 ANÁLISE DOS RESULTADOS DO MAPEAMENTO SISTEMÁTICO

Após a etapa da condução do MS, foi realizada a última fase da metodologia aplicada para este trabalho, que se trata da apresentação dos resultados, bem como a sua análise. Primeiramente, a resposta da primeira questão de pesquisa será apresentada, juntamente com a análise e discussão desses resultados, logo em seguida será realizado o mesmo procedimento para a segunda questão de pesquisa.

Sendo assim, após a conclusão destas análises e discussões das questões de pesquisas, será possível também concluir o objetivo geral, dando-se assim como concluído o Mapeamento Sistemático realizado nesta pesquisa.

- **Com relação à Primeira Questão de Pesquisa: *"Quais são as recomendações sobre Segurança da Informação indicadas para manter a proteção dos dados no contexto das organizações?"***

A primeira questão de pesquisa busca conhecer quais são as recomendações sobre Segurança da Informação indicadas para manter a proteção dos dados no contexto das organizações, sendo assim, com a extração de dados foi possível identificar tais recomendações.

Foram encontradas várias recomendações dentre as publicações, no caso, cada publicação selecionada continha um tipo, nas publicações era observado um tipo de ameaça, vulnerabilidade, entre outros. Após todo o estudo acerca de tal empecilho, havia uma recomendação para que se pudesse, a partir desta ser desenvolvido algum tipo de ferramenta ou algo similar para proteger as organizações de uma dada ameaça.

A partir disso, houve a construção da Tabela 9, nela pode-se verificar a descrição da recomendação, ou seja, do que se trata tal recomendação e para o que ela pode ser utilizada, assim como qual seria a implementação final da recomendação.

Tabela 9 - Dados sobre as recomendações identificadas

ID	Descrição da Recomendação	Formas de Implementação
PN01	Criação de um quadro de ameaças que demonstrou que avaliar as ameaças internas utilizando uma análise de base sintomática funciona bem e é eficaz para detectar precocemente sintomas de possíveis ameaças internas	Framework

PN02	Criação de sistema que implemente a detecção de anomalias usando um conjunto de Autocodificadores Profundos.	Sistema
PN03	Especialização de um quadro para capturar pontos de dados pertinentes que podem então ser reduzidos a um conjunto de causas, vetores de ataque e impactos.	Modelo
PN04	Implementar de um worm de engenharia social para aumentar a conscientização sobre segurança da informação	Prática
PN05	Categorizar as diferentes ameaças, engenharias sociais e táticas usadas na segmentação de funcionários e as abordagens para se defender contra tais ataques.	Prática
PN06	Fornecer um ponto de referência para a governança das mídias sociais para demonstrar um nível aceitável de segurança da informação nessas tecnologias e dentro da cultura de segurança dos usuários.	Framework
PN07	Processo de hierarquia analítica é usado como orientação na tomada de decisão da política de segurança da informação, identificando os fatores de influência e seus pesos para a conformidade da política de segurança da informação.	Modelo
PN08	Uma estrutura que reduz as restrições do sistema ao mesmo tempo em que aplica políticas de controle de acesso para ambientes BYOD e de nuvem, utilizando uma plataforma independente.	Framework
PN09	Um sistema de segurança da informação programa de conscientização (ISAP)	Sistema
PN10	Um modelo expediente de mitigação interna com ênfase na conscientização do usuário e controle de acesso, considerando que é difícil modelar o comportamento humano.	Modelo
PN11	Medidas contra os desafios de segurança da informação enfrentados pelas organizações no contexto da Engenharia Social.	Medida
PN12	Um sistema de equação vetorial de ameaças para 10 importantes serviços de IP, usando dados SANS padrão da indústria sobre ameaças a vários componentes das informações	Sistema
PN13	Sugestões para programas de treinamento de conscientização de segurança da informação para lidar com as inadequações	Recomendações
PN14	Medidas de dissuasão eficazes e políticas para segurança da informação organizacional no que se refere a Phishing.	Medida
PN15	Explorar a implementação de ISPs em uma grande organização para avaliar a adequação da política e determinar o usuário conscientização e cumprimento de tais políticas.	Abordagem

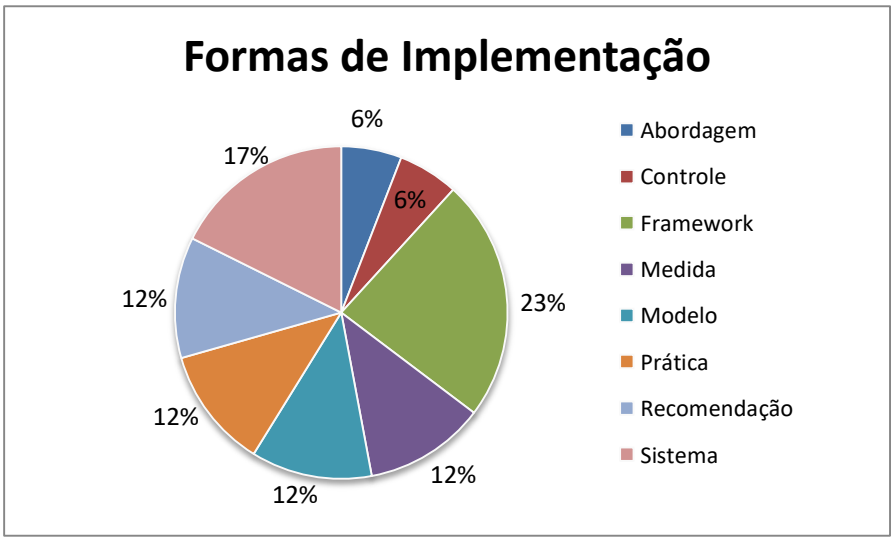
PN16	Orientar o administrador da rede a desenvolver um plano de resposta para incidentes apropriados com base nas ameaças identificadas do risco atividade de avaliação.	Controle
PN17	Recomendar estratégias para enfrentar os desafios do ponto visão dos tomadores de decisão de segurança nas organizações dentro as Engenharia Social.	Recomendações

Fonte: A autora (2020).

Pode-se observar na Tabela 9, que mostra os tipos de recomendações, que se trata de uma pequena descrição sobre a finalidade de cada recomendação quanto às vulnerabilidades levantadas por cada autor, ou seja, pode-se definir para quais tipos de ameaças, e outras questões, estas recomendações podem ser utilizadas. Assim, a literatura descreve vários tipos de recomendações, algumas delas para o mesmo tipo de ameaças.

Assim, é apresentado um gráfico (Figura 11) com as formas de implementação de cada recomendação citados nas publicações identificadas. Sendo assim, pode-se notar quais foram os tipos de recomendações que são os mais desenvolvidos ou utilizados.

Figura 11 - Formas de Implementação de cada recomendação



Fonte: A autora (2020).

Analisando a Figura 11, pode-se observar que foram levantados 08 (oito) tipos de implementações quanto às formas de implementação das recomendações identificadas. Nela pode-se notar os vários tipos de recomendações em suas várias formas. Foram obtidos dois tipos que apareceram apenas uma vez, 6% dos casos, que foram Abordagem e Controle. Logo em seguida tem-se as seguintes implementações: Medida, Prática, Recomendação e Modelo, cada uma com 12%, ou seja, cada uma apareceu em duas publicações.

Com a citação em três publicações tem-se o seguinte: Sistemas, com um total de 17%, e o que foi mais utilizado dentre as formas de implementação das recomendações foi o Framework com 23%, sendo indicado em quatro publicações.

Sendo assim, pode-se notar que a maioria das recomendações foram elaboradas e construídas para serem utilizadas em forma de Framework. Pode-se destacar também os Modelos que foram os segundos mais utilizados para a realização das recomendações. Este dado é bem interessante pelo fato de que as organizações podem escolher qual seria a melhor forma de implementar uma dada recomendação, tendo em vista que algumas recomendações tratam do mesmo problema, porém foram implementadas de formas diferentes.

Será realizada uma breve discursão sobre algumas publicações que continham dados mais profundos sobre recomendações, algumas das publicações relatavam de forma mais sucinta e explicativa sobre as ameaças que estavam sendo estudada por tal.

A publicação PN01 relata sobre ataques de Insider (Ameaça Interna), informam em uma tabela quais foram os sinais vitais dessa ameaça identificadas pelos autores, após a revisão da literatura realizada. Ressaltando que nesta tabela não se encontram todos os sinais relativos á ameaças internas maliciosas, porém já era o suficiente para o que o estudo se propunha pode se observar na Tabela 10.

Tabela 10 - Dados da PNO1

Atividades Maliciosas	Intenções Maliciosas
Roubo de propriedade	Alta frequência de copiar/mover arquivos para drives USB
	Uma frequência estranha de copiar/mover arquivos para a nuvem
Sabotagem de TI	A Violação da Política de Segurança de Rede
	O uso incomum de contas de administrador/root local
Espionagem	Alta frequência de recebimentos de e-mails de remetentes desconhecidos com endereços estrangeiros
	Discutir informações críticas relacionadas a ativos em publico ou em um telefone não seguro
Fraude	Alta frequência de desconsideração das políticas de computador da empresa
	Alta frequência de desconsideração das Políticas de Segurança da Informação

Fonte: Adaptado de Ikany e Jarzi (2019).

A PN05 relata sobre as técnicas de engenharia social assim como estratégias para conter tais técnicas, os autores discorrem sobre e ressaltam que essas técnicas podem ser classificadas em duas categorias que seriam ataques baseados em locais físicos (computadores) e ataques baseados em meios de psicologia (humanos). Essas informações serão relatadas na Tabela 11 na qual poderá se observar esses tipos de técnicas bem como as estratégias relatas pelo autor, elas descrevem as ações que podem ser tomadas para evitar essas técnicas e não necessariamente uma em específico.

Tabela 11 - Dados da PN05

Categorias	Técnicas	Estratégias
Locais Físicos (Computadores)	Local de trabalho: Por meio de falsificação de identidade	Melhoria da segurança física: Pode ser um grande impedimento contra invasores externos
	Telefone: O invasor ataca os sistemas PBX ou as linhas de ajuda de atendimento ao cliente das organizações	
	Online: É baseado em várias plataformas online	Políticas de segurança mais fortes: A política deve ter diretrizes claras sobre o pessoal e quando as informações podem ser liberadas para o público
Métodos Psicológicos (Humanos)	Autoridade: Por meio de implicações e afirmações de autoridade, contra funcionários novos ou desavisados	
	Inclinação natural para ajudar: Por meio do aproveitamento da boa vontade de um funcionário	Resposta a violações de segurança: Envolve a implementação de técnicas de treinamento de resistência para as pessoas chave
	Gosto e semelhança: Desenvolver conexões pessoais	
	Compromisso e consciência: Por meio da exploração de ser visto como confiáveis e comprometidos com a execução de seus ataques	Procedimentos de tratamento de incidência: As duas técnicas utilizadas para esse procedimento são: colocação de minas terrestres de engenharia social (SELMs) e resposta a incidência.
	Reciprocidade: Por meio da engenharia social reversa	
	Pouco envolvimento: Utiliza-se o pouco envolvimento do funcionário.	

Fonte: Adaptado de Ghafir et al. (2016).

A PN03 o qual discorre sobre Insider Accidental, cum o objetivo de coletar e avaliar a eficácia da política de segurança corporativa para lidar com o risco de comprometimento do Insider Accidental. O método de coleta dos casos se deu pelas fontes como: artigos de notícias, relatórios oficiais e outros artigos relevantes, não foram definidos critérios de seleção

para os casos, ao final foram recolhidos 60 casos de incidentes que foram relatados nos últimos 10 anos.

Foi utilizado um framework com as caracterizações de ameaça interna para fornecer a base para análise dos dados coletados. Ele foi criado para gravar todos os principais dados que se associam aos casos de ameaça interna, sendo intencional ou não, ajudando assim a destacar os fatores mais pertinentes relacionados aos casos coletados, o que forneceu um conjunto de dados consistentes, e foi utilizado um único codificado neste framework.

Foram encontradas 10 políticas de segurança da informação que estavam disponíveis na internet, e estão ligados a diferentes setores, sendo 03 de (academia), 03 de (governo local), saúde, finanças, ciência e tecnologia e aplicação da lei com 01 cada. Além das políticas do mundo real também foram utilizados modelos de políticas disponível online, e todas as politicas que foram utilizadas de empresas forma de forma anônima.

O erro humano apareceu em 80% das politicas estudadas constavam esse fator, e relatavam recomendações para tal, uma das politicas cita que controles devem ser aplicados para a proteção em relação a está clausula , como por exemplo, o endereçamento incorreto ou desorientação, e a confiabilidade geral e disponibilidade do serviço, umas da estratégias que podem ser utilizadas é o recebimento de treinamento em qualquer aplicativo que os funcionários seriam obrigados a acessar e a outro qualquer pacote de software que não necessariamente são obrigados a usar, porem nenhuma das politicas justifica a adequação ou eficácia de tal método.

No caso de política não seguida, foram identificadas duas razões para o não cumprimento desta clausula, a política era incompleta ou mal definida, ou funcionário não estava ciente da política de segurança, outras também citam que a política pode não ter sido comunicada de forma correta ou que elas acabaram tornando às atividades dos funcionários mais difíceis de desempenhar.

O uso do e-mail foi citado em 60% das políticas, citando que o uso de e-mail pessoal deve ser permitido, no entanto, apenas nos horários livres e com pouco volume de uso, assim como o uso errôneo da anexação de arquivos e envio para destinatários incorretos.

Sobre o descarte incorreto de recursos 73% das políticas relatavam sobre, no entanto foi mais discutindo sobre o descarte de papel do que o de hardware, as recomendações para o descarte do papel eram que eles fossem descartados nos lugares certos, material restrito ou confidencial jogado em latas de lixo com o rotulo confidencial e os materiais secretos devem

ser picotados. Quando ao descarte em hardware uma política citou que o descarte deveria ser feito pelo próprio funcionário, ao apagar os dados de forma segura assim que sair.

O termo transporte de dados não foi muito abrangido pelas políticas coletadas, apenas 13% relataram como fazer isso de forma segura, uma delas estipulou que o transporte confiável ou mensageiro confiável deve ser utilizado, a embalagem deve proteger o conteúdo de qualquer possível dano físico causado durante o processo de transporte.

Apenas 33% das políticas continham orientações sobre a forma de evitar ataques de engenharia social, duas delas citavam a confiabilidade de e-mail, ou seja, que não se pode confiar no que se recebe por e-mail, em particular nunca se deve responder um e-mail que peça um nome de usuário ou senha.

A proteção contra malware/vírus apareceu em todas as políticas, e as recomendações são para que se tenha mantido software antivírus instalados. Em relação aos dados protegidos indevidamente 73% das políticas abordavam sobre a recomendação principal é para que as organizações assim como os funcionários cumpram a Lei de Proteção de Dados, a configuração correta de um servidor web também é descrita como uma forma de proteger os dados.

Dados copiados para dispositivo inseguro foi abordado por todas as políticas, a primeira recomendação é que seja proibido que os dados sejam copiados para dispositivos removíveis e a segunda é todos os dispositivos moveis que tivesse informações sigilosas fossem criptografados antes de sair da empresa.

A PN07 apresenta algumas recomendações que podem ser utilizadas na criação de um programa de conscientização de segurança adequado que pode ajudar com a melhoria da conformidade com as políticas.

Autonomia, o ataque cibernético tem o valor de prioridade mais auto sobre outras áreas de foco de conscientização, por isso é recomendado que as empresas desenvolvam programas de conscientização adequados com o foco em ataque cibernéticos, ameaças e engenharia social para que assim os funcionários estejam mais capacitados para enfrentar ataques do mundo real.

Competências, as características ligadas a essa área da conscientização são uso de e-mail e internet, resposta a incidentes e conformidades com as políticas, ela mede a percepção do funcionário é recomendado que as organizações de concentrem nessas três áreas para que assim o conhecimento dos funcionários sobre segurança aumente.

Parentesco, é recomendado que o programa de conscientização atenda a alguns requisitos como a necessidade do individuo de pertencer, que pode ser alcançado por meio de aulas online sobre segurança, estimulando o debate sobre o tema entre os funcionários, logo fazendo com eles se tornem conscientes e mais propensos a cumprir a política de segurança da informação da organização.

Intenção, é recomendável que as organizações desenvolvam programas de conscientização voltados para as áreas de uso de e-mail e internet, resposta a incidentes e conformidades com as políticas, com o principal objetivo de aprimorar o comportamento dos funcionários assim como estabelecer boas práticas de segurança.

PN08 se propõe a construir uma nova ferramenta de gerenciamento de segurança chamado de Softwares as a Service (AaaS) que poderá ser utilizado em provedores de nuvem públicas. Essa estrutura oferece a capacidade de usar o gerenciamento de nuvem para realizar verificações de segurança antes que se possa permitir o acesso do BYOD ao ambiente de nuvem. O framework é dividido em três partes. Abaixo serão citados essas partes e seus agentes e para o que eles servem.

A primeira parte trata – se do Proprietário/Dispositivo de política de administrador, que se refere que quem for o responsável pela política de acesso de controle do usuário BYOD controla essa parte. Esse dispositivo pode ser um dispositivo pessoal ou um PC que contenha um sistema operacional confiável, para que assim se possa definir o nível de classificação de segurança, e os dados iniciais para o controle de acesso. Esta parte conta com dois agentes que são: Política MAC (Controle de acesso obrigatório) e Dados.

- Política MAC: dita os limites de acesso estritos que são difíceis de serem burlados, intencionalmente ou não. Essa política é eficaz, pois estabelece um nível de autorização para cada usuário;
- Dados: inclui todos os recursos que queiram ser armazenados na nuvem.

A outra parte se trata da Gerência de Segurança, que é a parte central da ferramenta, a sua tarefa é gerenciar todas as partes que se fazem necessárias para a operação da política MAC. A ferramenta tem 04 funções que são: verificar a segurança do dispositivo BYOD, aplicar a política de segurança de acesso, trabalhar com plataformas independentes e por fim proteger a política de proteção de acesso. Esta para possui onze agentes.

- Agente Controlador: este agente é estático é controla todos os outros agentes, sua interface é uma API (Application Programming Interface), ele cria instancias de agentes móveis e envia para dispositivos utilizando endereços individuais de IP.

- Agente de Verificação de requisitos de segurança: esse agente é criado pelo agente anterior, ele verifica se os BYODs atendem aos requisitos da política se segurança da organização para ser um dispositivo confiável. Isso é possível, pois esse agente faz uma verificação se há softwares antivírus atualizado, impressões digitais assim como uma conexão VPN e instala um gerenciador de agente.
- Agente de Autenticação: esse agente é iniciado no momento em um dispositivo atenda aos requisitos da política de segurança, cada usuário necessita de uma identidade única, esse agente usa dois tipos de autenticação extra para permitir o acesso ao usuário.
- Agente de Verificação de Permissão: após o término da verificação do agente anteriormente citado, o agente de verificação busca no banco de dados a classificação de segurança que foi atribuída ao nome do usuário. Este agente funciona para acelerar o processo caso o acesso do usuário seja negado antes de enviar para a nuvem.
- Agentes de Assinatura e Verificação de Assinatura: são agentes móveis, eles são responsáveis por analisar se uma solicitação de acesso ao sistema vem de um usuário conhecido e que não foi alterado no caminho.
- Agente de Criptografia e Descriptografia: garente que apenas usuários e agentes com autorização tenham acesso e leiam as informações transmitidas, seu trabalho pe manter em segredo a informação.
- Agente de Aplicação da Política: ele é estático e tem como função principal aplicar políticas de controle de acesso para assim determinar quem pode ter acesso a nuvem, seu objetivo é fortificar o controle de acesso.
- Agentes de Monitoramento de Política e Verificação de Integridade: verificam se há modificações em uma política MAC no decorrer da transmissão e se só foi enviada pelo administrador da política.
- Agente de Auditoria: é um agente estático ele deve registrar todas as tentativas, bem e mal sucedida de acesso ao sistema. Ele é responsável por registra todas às decisões do agente de aplicação da política sobre as decisões de concessão bem como a negação de acesso.
- Agente de Criptografia e Descriptografia de Política: deve criptografar e descriptografa todas as informações que transmite.
- Agente de políticas de Banco de Dados: é estático e se comunica com outros bancos de dados. Este agente troca os dados á medida que são transmitidos por variados estilos e padrões de arquitetura de software.

A última etapa da ferramenta é do Dispositivo BYOD Cliente, os clientes não são restritos a trabalhar em local ou a “horas de trabalho”. Eles podem trabalhar de qualquer lugar e a qualquer hora. Esta etapa conta com dois agentes.

- Criação e Modificação de Políticas e Dados: após o trabalho de todos os agentes citados na etapa anterior, essa serve para que o usuário possa salvar, políticas e

dados novos e alterados nos sistemas a partir da realização da tarefa dos agentes da outra etapa.

- Monitorando a Política MAC: este monitoramento do MAC é a função mais relevante para proteger a integridade das políticas no decorrer das etapas de processamento e armazenamento.

Logo, foi possível mapear e fazer uma tabela, que resume os tipos de ameaças que estas recomendações se referem, que pode ser consultado na Tabela 12. Nesta tabela pode-se observar que existem vários tipos de implementação, podendo ser mais de uma para uma dada ameaça. Cada empresa deverá analisar qual é a mais indicada para o seu contexto, assim como a melhor forma de implementação.

- **Com relação à Segunda Questão de Pesquisa: *"Quais são as ameaças, vulnerabilidades e/ou comportamento de riscos relatados nas recomendações de segurança da informação da literatura?"***

A segunda questão de pesquisa busca identificar quais são as ameaças, vulnerabilidades e/ou comportamentos de riscos relatados nas recomendações de segurança da informação da literatura, sendo assim, após a extração de dados foi possível identificar algumas dessas ameaças.

Nas publicações foi possível encontrar várias dessas ameaças, portanto elas foram catalogadas e colocadas em uma tabela para uma melhor análise na qual mostra que foram encontradas 07 ameaças, a Tabela 13 apresenta um ranking das ameaças de forma decrescente de ocorrências nas publicações identificadas.

Tabela 12 - Dados sobre as implementações utilizadas para as ameaças

Publicações	Implementação/ Ameaça	Abordagem	Controle	Framework	Medida	Modelo	Prática	Recomendação	Sistema
PN12	Ataques a SSH e Secure Web Server								✓
PN13 e PN09	Ativos							✓	✓
PN15 e PN07	Conscientização	✓				✓			
PN06, PN11, PN04, PN05 e PN17	Engenharia Social			✓	✓		✓	✓	
PN01, PN03, PN10 e PN02	Insider			✓		✓			✓
PN16 e PN14	Phishing		✓		✓				
PN16 e PN08	Softwares Maliciosos		✓	✓					

Fonte: A autora (2020).

Tabela 13 - Ranking de Ameaça, Vulnerabilidade e/ou comportamento de risco

Quantidade de Ameaça, Vulnerabilidade e/ou Comportamento de Risco	Posição	Tipo de Ameaça, Vulnerabilidade e/ou Comportamentos de Risco	Quantitativo de Publicações
01	1º	Engenharia Social	PN04, PN05, PN06, PN11 e PN17
02	2º	Insider	PN01, PN02, PN03 e PN10
03	3º	Ativos	PN09 e PN13
04	3º	Conscientização	PN07 e PN15
05	3º	Phishing	PN14 e PN16
06	3º	Softwares Maliciosos	PN08 e PN16
07	4º	Ataques a SSH e Secure Web Server	PN12

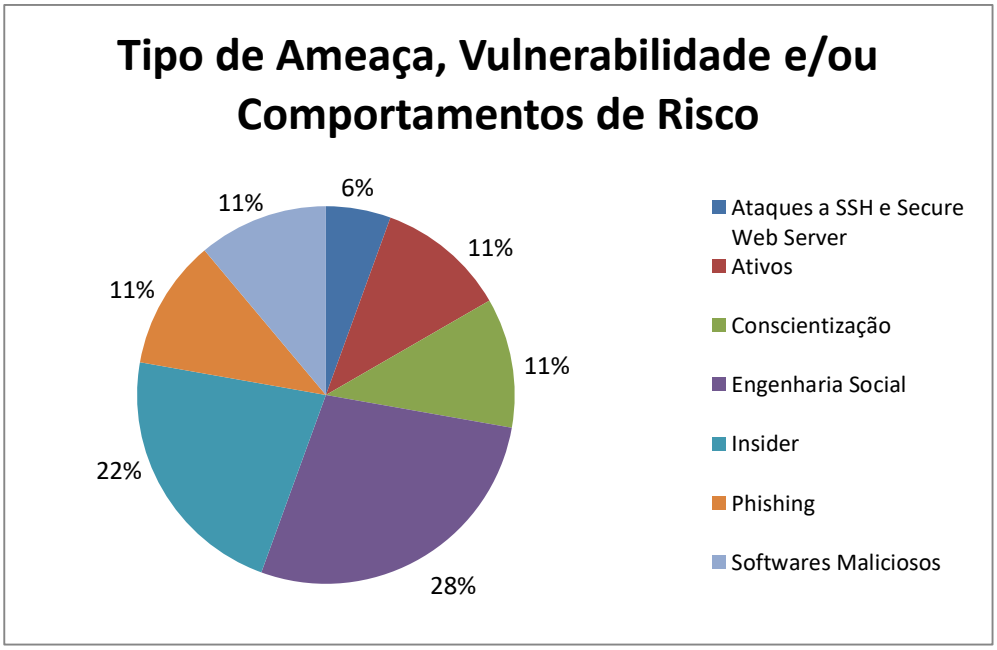
Fonte: A autora (2020).

A Tabela 13 possuí as informações necessárias e que podem auxiliar as organizações e afins, é importante ressaltar que a classificação para as posições foi na ordem das Ameaças, Vulnerabilidades e/ou Comportamentos de Risco que mais tiveram reincidência dentre as publicações. No entanto, várias obtiveram o mesmo quantitativo de repetições, dessa forma, a ordem baseou-se na ordem alfabética do tipo de Ameaça, Vulnerabilidade e/ou Comportamentos de Risco.

A partir desta tabela foi gerado um gráfico, que mostra em % o quanto cada um desses tipos das Ameaças, Vulnerabilidades e/ou Comportamentos de Risco apareceram, com base neste gráfico foi possível fazer uma análise mais sucinta destes resultados, assim como aprofunda um pouco mais o que os autores relatam sobre estes em suas respectivas publicações.

Com isso, é apresentado o gráfico da Figura 12 os tipos de Ameaças, Vulnerabilidades e/ou Comportamentos de Risco de cada recomendação citados nas publicações identificadas. Sendo assim, pode-se obter a porcentagem de cada um desses tipos.

Figura 12 - Tipo de ameaça, vulnerabilidade e/ou comportamento de risco



Fonte: A autora (2020).

A partir da Figura 12 pode-se analisar que as Ameaças, Vulnerabilidades e/ou Comportamentos de Risco que mais se fez presente foi a Engenheira Social que aparece com 28%. Mas, vale ressaltar que outras ameaças e afins também se encaixam em ataques do tipo Engenharia Social, no entanto, das publicações analisadas foi observado que dentre as que citavam a Engenharia Social, este termo era mencionado de uma forma bem mais ampla, sem citar um tipo de ataque específico. Portanto, foi utilizado esse critério, de forma a não agrupar os tipos de ameaças, tendo em vista que poderia confundir quem fosse escolher as publicações com relação à Engenharia Social.

Observando a Figura 12 também é possível notar que a segunda Ameaça, é o *Insider* com o total de 22%, dentre as publicações onde é citado pelos autores, fazem uma ressalva de que nem sempre é algo proposital, em alguns casos pode ser apenas pela alta vontade do funcionário fazer seu trabalho de maneira impecável, que é denominado *Insider* Acidental. No entanto, não se descarta a possibilidade de se tornar uma ameaça à medida que o uso das informações que ele possui traga malefícios para as organizações.

Têm-se também os Ativos com 11%. Com isso, é importante ressaltar a diferença entre dois tipos de ameaças, que é o *Insider* citado acima e os ativos, tendo em vista de que pode haver um tipo de má interpretação ou até mesmo uma associação errada a esses dois casos, a principal diferença entre eles é que o *Insider* é considerado como aquele que possui acesso a informações privilegiadas dentro das organizações/empresas.

Por outro lado, o(s) ativo(s) que podem ser considerados os ativos da informação, o que não são necessariamente pessoas/objetos que possuem tais informações, são considerados como um todo, sendo assim, pode ou não influenciar em tomadas de decisões, visto que uma máquina pode apenas guardar as informações. Nota-se na Tabela 13 que esses dois estão em posições diferentes, os Ativos aparecem menos dentre as publicações, no entanto, é importante fazer tal diferenciação.

A partir daí tem-se as que tiveram as mesmas quantidades. Destacando-se os Ativos, Conscientização, *Phishing* e Softwares Maliciosos ambos com 11%, todos com duas aparições cada, lembrando que o *Phishing* é uma técnica de Engenharia Social.

No entanto, as publicações em que foi citado, foram de forma bem específica, onde foi citado que o *phishing* é arriscado porque pode desativar a defesa organizacional de sistemas de TI, atacando os usuários desses sistemas. Consequentemente, programas para educar os funcionários a evitar golpes de *phishing* são extremamente importantes para proteger valiosas informações organizacionais, este fato é citado na publicação que relata especificamente sobre *phishing*. Os ataques de *phishing* também são citados de forma combinada com algumas outras ameaças que seriam os softwares maliciosos.

Nas publicações identificadas, a conscientização é relatada de forma a explorar a implementação de PSIs (Políticas de Segurança da Informação), que é abordado em duas publicações diferentes. No entanto, as publicações destacam questões semelhantes em relação aos ataques que podem necessitar a maior atenção dos funcionários. As duas publicações tratam da adequação da política e determina a conscientização do usuário e cumprimento de tais políticas, de forma a tratar o comportamento de risco.

Para os softwares maliciosos, a abordagem ocorreu de maneira em que continha esses tipos de softwares, em uma publicação em que foram colocados de modo em que seriam mais utilizados em ambientes *Bring your own device* (BYOD) e de nuvem, ou seja, com um pouco mais de especificidade e na outra era um pouco mais ampla, pois se tem alguns outros tipos de ameaças como o *Phishing*, no entanto, também seriam mais voltados para essas ameaças na rede.

Por fim, tem-se a que teve a menor quantidade de citações dentre as publicações, ficando assim na última posição da Tabela 13, que foi o, Ataques a SSH e *Secure Web Server* 6%, que foi citado em apenas uma publicação. Os autores citam que os serviços como ssh e DNS são habilitadores para a maioria das operações da internet e, como tal, são alvos

altamente atrativos para atacantes que desejam interromper outros serviços, assim como a *Secure Web Server* que é normalmente usada para transações altamente sensíveis.

De toda forma não se deve relaxar, e acreditar que as que tiveram menor visibilidade e foram às menos citadas, devem ser deixadas de lado, pois é certo que dentro de uma organização e até mesmo fora, todo cuidado é pouco e não se deve descartar nenhum tipo de ameaça, vulnerabilidade e/ou comportamento de risco, por mais que seu índice de efetividade ou quantidade seja baixo ou quase nulo.

5 CONCLUSÃO E PERSPECTIVAS FUTURAS

5.1 **Considerações Finais**

Diante dos avanços da TI, a informação vem se tornando cada vez mais presente e valiosa, principalmente no que se refere às informações de uma organização, os métodos de ataque a essas informações estão cada vez mais sofisticados, logo, os meios de defesa para tais devem ser melhorados e aprimorados a cada momento, tendo em vista que a perda ou o comprometimento de tal informação pode ter graves consequências para seus proprietários.

Os avanços tecnológicos podem ser usados tanto para defesa, como para o ataque, nesse ponto que as organizações devem ligar o alerta, e averiguar cada requisito e não deixar que nada passe para assim manter a segurança da informação dentro de seus limites, usando seus recursos de forma adequada para escolher as melhores formas de se prevenir de qualquer ataque que possa ocorrer.

Tendo isso em vista, o objetivo geral deste trabalho foi o de analisar as principais recomendações de Segurança da Informação nas Organizações bem como esforços existentes na literatura para a proteção das informações. Para tal, a metodologia que foi utilizada foi um MS.

Sendo assim, os resultados obtidos dos objetivos específicos foram, do primeiro que era, investigar as recomendações de segurança da informação relacionadas às práticas e controle de proteção de dados sigilosos no contexto das organizações, no qual se pode conhecer um total de 17 recomendações. As mesmas podem ser utilizadas de várias formas para contextos diferentes, dependendo do que melhor se encaixa ao perfil da organização. Tendo em vista que as recomendações foram implementadas de maneiras diversificadas.

Para o segundo objetivo específico, que era identificar os tipos de ameaças, vulnerabilidades e/ou comportamento de riscos relatados nas recomendações de segurança da informação da literatura. Foram encontradas 07 dessas ameaças, algumas com a maior frequência que outras, que podem ser encontradas em fatores variados e de formas diferentes, o que não diminui os seus riscos.

A literatura apresenta várias recomendações, assim como ameaças, claro que esse estudo está limitado de várias formas, tanto pela metodologia aplicada, quanto as questões que eram a prioridade para serem respondidas.

Com isso, este estudo conseguiu o objetivo que se propôs, trazendo como contribuição novas recomendações que foram encontradas na leitura, que podem ser utilizadas da maneira mais adequada para cada caso. Além do mais, vale ressaltar que, dentre todos os tipos de ataques citados, independente da frequência citada nas publicações identificadas, devem ser alvo de atenção nas organizações, pois todos são perigosos.

5.2 **Limitações**

As limitações deste trabalho estão relacionadas à:

- Os locais de busca limitados, que não estavam disponíveis para a realização deste estudo, tendo em vista que não obtive acesso a uma das bibliotecas digitais das que foram selecionadas;
- A indisponibilidade de todos os anais de eventos dos quais haviam sidos selecionados, fazendo assim com que o número de artigos desta fonte fosse reduzido.
- Apenas um pesquisador para identificar os resultados.

5.3 Trabalhos Futuros

Com o propósito de estender e aprimorar os resultados obtidos, algumas das perspectivas de trabalhos futuro são apresentados a seguir:

- Ampliar a pesquisa para outras fontes de busca, como outras bibliotecas digitais e anais para identificar mais recomendações.
- Realizar uma pesquisa nas organizações para saber quais ataques são os mais recorrentes dentro das mesmas.
- Aplicar um questionário com funcionários de empresas para identificar quais recomendações eles mais tendem a seguir.

REFERÊNCIAS

ALAVI, M.; LEIDNER, E. **Review: knowledge management and knowledge management systems: conceptual foundations and research issues.** MIS Quarterly, v. 25, n. 1, p. 107-133, 2001.

ALBUQUERQUE, A. e SANTOS, E. **Adoption of Information Security Measures in Public Research Institutes.** Journal of Information Systems and Technology Management (JISTEM), v. 12, n.2, p. 289-316, 2015.

ALVES, C. **A importância da Tecnologia da Informação nas Empresas.** Revista Científica Semana Acadêmica, v. 01, n. 000024, p. 01-11, 2013.

BASILI, V.; CALDEIRA, G.; ROMBACH, H. *The Experience Factory*. In: Encyclopedia of Software Engineering, New York, 1994.

BASTOS, A. e CAUBIT, R. **Gestão de Segurança da Informação.** ISO 27001 e 27002 Uma Visão Prática. Rio Grande do Sul. Zouk, 2009.

BAZZOTTI, C. e GARCIA, E. **A importância do Sistema de Informação Gerencial na Gestão Empresarial Para Tomada de Decisões.** Ciências Sociais Aplicadas em Revista, v. 11, n. 6, p. 1- 18, 2006.

Boas Práticas em Segurança da Informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BROOKES, C. **Numerical Methods of Bibliographic Analysis**. Library Trends, v. 22, n. l, p. 18-43, 1973.

CAMPOS, A. **Sistemas de Segurança da Informação: Controlando os Riscos.** Florianópolis: Visual Books, 2007.

CARUSO, C. e STEFFEN, F. **Segurança em Informática e de Informações** – São Paulo: Editora SENAC São Paulo, 1999.

COULOURIS, G.; DOLLIMORE, J.; KINDBERG, T.; BLAIR, G. **Sistemas Distribuídos: Conceitos e Projeto**. Porto Alegre: Bookman, 2013.

FERNANDES, N. **Segurança da Informação.** Cuiabá: Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, 2013.

FERREIRA, A. e CABRAL, H. e SONNENSTRAHL, T. **Política de Segurança da Informação.** Santa Maria: Instituto Federal de Educação, Ciência e Tecnologia Farroupilha, 2013.

FERREIRA, F. e ARAÚJO, M. **Politica de Segurança da Informação – Guia Prático para Elaboração e Implementação.** Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

FURNELL, S. e THOMSON, K. **From Culture to Disodedience: Recognonising the Varying User Acceptance of IT Security.** Computer Fraud & Security, p. 5-10, 2009.

GALEGALE, N.; FONTES, E.; GALEGALE, B. **Uma Contribuição para a Segurança da Informação: Um Estudo de Casos Múltiplos com Organizações Brasileiras.** Revista Perspectivas em Ciência da Informação, v. 22, n. 03, p.75-97, 2017.

GOFFMAN, W. & MORRIS Jr., T. G. - **Quasi-Metric Spaces and Information Systems.** Proceedings of the International Congress of General Systems and Cybemetics. London, 1972.

HARMON, G. **Human Memory as a Factor in the Formation of Disciplinary Systems**. 1970. 132 f. Dissertação (PHD) - School of Library Science, Case Western Reserve University, 1970.

ISO/IEC. **ISO/IEC 17799: Tecnologia da Informação – Técnicas de Segurança – Codigo de Prática para a Gestão da Segurança da Informação.** Associação Brasileira de Normas Técnicas, 2005.

KITCHENHAM, B.; BRERETON, O.; BUDGEN, D. **Using Mapping Studies as the Basis for Further Research – A Participant-Observer Case Study**. Information and Software Technology, vol. 53, p. 638-651, 2011.

KITCHENHAM, B.; CHARTERS, S. **Guidelines for Performing Systematic Literature Reviews in Software Engineering**. Relatório Técnico Evidence-Based Software Engineering (EBSE), v. 2.3, 2007.

LAUDON, K. e LAUDON, J. **Sistemas de Informação: Com Internet.** 4.ed. Rio de Janeiro: LTC, 1999.

LAUDON, K. LAUDON, J. **Gerenciamento de sistemas de informação.** Rio de Janeiro: LTC, 2001.

LYRA, M. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro. Ciência Moderna, 2008.

MAIA, M. **A Tecnologia da Informação Como Fator de Sobrevivência e Vantagem Competitiva.** Revista Eletrônica Machado Sobrinho, v. 7, p. 01-10, 2013.

MARINHO, F.; SANTOS, E.; RODRIGUES, R.; PASSOS, O. **Ameaças à Segurança da Informação nas Organizações.** XI Semana Nacional de Ciência e Tecnologia ICET/UFAM e IFAM (SNCT), 2017.

MARTINS, P.; MELO, B.; QUEIROZ, D.; SOUZA, M.; BORGES, R. **Tecnologia e Sistemas de Informação e suas Influências na Gestão e Contabilidade.** IX Simpósio de Excelência em Gestão e Tecnologia (SEGeT), 2012.

MESQUITA, L. **Política de Segurança da Informação – Desenvolvimento de um Modelo para uma Empresa de Plano de Saúde Ambulatorial.** 2015. 43 f. Dissertação (Pós-graduação em Redes de Computadores com Ênfase em Segurança) – Centro Universitário de Brasília, 2015.

MÜLBER, L. e AYRES, N. **Fundamentos para Sistemas de Informação.** Palhoça: UnisulVirtual, 2005.

NETO, V. e OLIVEIRA, J. **Evolução de uma Arquitetura de Framework de Aplicação para Sistemas de Informação com Desenvolvimento Dirigido por Modelos.** Simpósio Brasileiro de Sistemas de Informação, n. 9, p. 320-331, 2013.

NETTO, A. e SILVEIRA, M. **Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas.** Revista de Gestão da Tecnologia e Sistemas de Informação, v. 4, n. 3, p. 375-397, 2007.

NORTON, P. **Introdução à Informática.** São Paulo: Makron Books, 1996.

NOVO, J. **Softwares de Segurança da Informação.** Manaus: Centro de Educação Tecnológica do Amazonas, 2010.

O'BRIEN, J. e MARAKAS. G. **Introduction to Information Systems**. New York: McGraw-Hill Irwin, 2010.

OLIVEIRA, G.; MOURA, R.; ARAÚJO, F. **Gestão da Segurança da Informação: Perspectivas Baseadas na Tecnologia da Informação.** XV Encontro Regional de Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação (EREBD), Cariri, 2012.

PEREIRA, D.; ZAHAIKEVITCH, E.; CRUZ, J.; FASCINA, M. **A Tecnologia da Informação como Suporte no Processo de Tomada de Decisões.** Revista Eletrônica Saber, v. 13, n. 1, p. 01-09, 2011.

PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATISSON, M. **Systematic Mapping Studies in Software Engineering.** In Proceedings of the Evaluation and Assessment in Software Engireening (EASE), Bari, Italy, 2008.

PIMENTA, A. e QUARESMA, R. **A Segurança dos Sistemas de Informação e o Comportamento dos Usuários.** Revista de Gestão e Tecnologia e Sistemas de Informação, v. 13, n. 3, p. 533-552, 2016.

PRIBRAM, K. ed. ***On the Biology of Leaming.*** N. Y., Harcourt, 1969.

PROMON. Promon Business & Technology Review – **Segurança da Informação: Um Diferencial Determinante na Competitividade das Corporações**, 2005.

RANGEL, A. **Transparência Versus Segurança da Informação: Uma Análise dos Fatores de Risco Exposto na Comunicação entre o Governo e a Sociedade.** 2015. 143 f. Dissertação (Mestrado em Ciência da Informação) – Universidade de Brasília, 2015.

RODRIGUES, F. e TORRES, M. e FLORIAN, F. **Segurança dos Sistemas de Informação.** Revista Cientifica Semana Acadêmica, v. 1, p. 1-25, 2018.

SARACEVIC, T. **Tecnologia da Informação, Sistemas de Informação e Informação como Utilidade Pública.** Revista Ciência da Informação, v. 3, n. 2, p. 57-67, 1974.

SERAFIM, V.; WEBER, R.; CAMPELLO, R. **Técnicas de Segurança da Informação: da Teoria à Prática**. In: Sociedade Brasileira de Computação0; Universidade Federal de Santa Catarina. (Org.). Anais do XXII Congresso da Sociedade Brasileira de Computação - XXI JAI - Livro Texto. 1ed.Florianópolis: SBC, 2002, v. 2, p. 129-192.

SHANNON, E. & WEAVER, W. **Mathematical Theory of Communication.** University of Illinois Press, Urbana, 125 p. 1949.

SILVA, C. e GARCIA, V. **Uma avaliação da Proteção de Dados Sensíveis Através do Navegador Web.** Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, n. 15, p. 86-99, 2015.

SILVA, S. **Gestão do Conhecimento: uma revisão crítica orientada pela abordagem da criação do conhecimento.** Revista Ciência da Informação, v. 33, n.2, p. 143-151, 2004.

SOARES, C. e SILVA, P. **Uma Avaliação sobre o Conhecimento em Segurança da Informação.** Revista Expressão Científica, v. 3, n. 1, p. 70-79, 2018.

SOUZA, M.; CAVALCANTE, A.; SILVA, A.; SOUSA, J.; SAMPAIO, R. **Ameaças e Mecanismos de Segurança da Informação em um Ambiente Organizacional de Planos de Saúde.** Revista Conhecimento Contábil, v. 06, n.01, p. 70-80, 2018.

STAIR, R. e REYNOLDS. G. **Princípios de Sistemas de Informação.** São Paulo: Cengage Learning, 2016.

STAIR, R. e REYNOLDS. G. **Princípios de Sistemas de Informação.** São Paulo: Cengage Learning, 2011.

TORRES, F. **Conceitos e Princípios da Segurança da Informação.** In: Lyra, M. (Org.). **Governança da Segurança da Informação**. Edição do Autor: Brasília, 2015. p. 09-20.

TRIBUS, M. & McHRVTNE, G. **Energy and Information. Scientific American**, v. 2 2 5, n. 9, p.178-188, 1971.

WOBBER, E.; ABADI, M.; BURROWS, M.; LAMPSON, B. **Authentication in the Taos Operating System.** ACM Transactions on Computer Systems, v, 12, n. 01, p. 3-32, 1994.

ZIPF, G. **Human Behavior and the Principie of Least Effort.** Cambridge, Addison Wesley, 1949.

APÊNDICES

APÊNDICE A – PUBLICAÇÕES IDENTIFICADAS NO 1º FILTRO

#	Título	Autores	Ano	Local de Busca
01	Provendo Segurança e Privacidade em Coordenação Distribuída e Extensível	Edson Floriano S. Junior; Eduardo Alchieri; Diego F. Aranha; Priscila Solis	2018	SBRC
02	An Ontological Approach to Mitigate Risk in Web Applications	Marcius M. Marques; Célia G. Ralha	2014	SBSeg
03	CSIHO: An Ontology for Computer Security Incident Handling	Guilherme Baesso Moreira; Vanusa Menditi Calegario; Julio Cesar Duarte; Anderson Fernandes Pereira dos Santos	2018	SBSeg
04	Técnica para Retenção e Recuperação de Conhecimento na Resolução de Incidentes de Segurança	Marcelo Colomé; Raul Ceretta Nunes; Luis Alvaro de Lima Silva	2019	SBSeg
05	Insiders: Um Fator Ativo na Segurança da Informação	Gliner Dias Alencar; Anderson A. L. Queiroz; Ruy José G. Barretto de Queiroz	2013	SBSI
06	Um Estudo Empírico Sobre o uso de Métricas de Segurança em Ambientes Reais	Rodrigo S. Miani; Bruno B. Zarpelão; Leonardo S. Mendes;	2014	SBSI
07	Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas	Gonçalo M. da Silva Neto; Gliner Dias Alencar; Anderson Apolonio L. Queiroz	2015	SBSI
08	BYOD Manager Kit - Integração de Ferramentas de Administração e Segurança BYOD	Vinícius Lahm Perini; Maria de Fátima Webber do Prado Lima	2018	SBSI
09	A Conceptual Model of Information Security Compliant Behaviour Based on the Self-Determination Theory	Yotamu Gangire; Adéle Da Veiga; Marlien Herselman	2019	IEEE/SCOPUS
10	A Gap Analysis of the ISO/IEC 27000 Standard Implementation in Namibia	Diana Jogbeth TJIRARE; Fungai BHUNU SHAVA	2017	IEEE/SCOPUS
11	A Methodology for Conversion of Enterprise-Level Information Security Policies to Implementation-Level Policies/Rule	Anirban Sengupta; Chandan Mazumdar; Aditya Bagchi	2011	IEEE/SCOPUS

12	A Symptomatic Framework to Predict the Risk of Insider Threats	Joris Ikany; Husin Jazri	2019	IEEE/SCOPUS
13	Anomaly-based Insider Threat Detection using Deep Autoencoders	Liu Liu; Olivier De Vel; Chao Chen; Jun Zhang; Yang Xiang	2018	IEEE/SCOPUS
14	Embedding Organizational Culture Values towards Successful Business Continuity Management (BCM) Implementation	Noorul Halimin Mansol; Najwa Hayaati Mohd Alwi; Waidah Ismail	2014	IEEE/SCOPUS
15	Enhanced Information Security Management System Framework Design Using ISO 27001 And Zachman Framework: A Study Case of XYZ Company	Andre Aginsa; Ian Yosef Matheus Edward; Wervyan Shalannanda	2016	IEEE/SCOPUS
16	Explaining Opposing Compliance Motivations towards Organizational Information Security Policies	Paul Benjamin Lowry; Greg D. Moody	2013	IEEE/SCOPUS
17	Information Security Governance Control Through Comprehensive Policy Architectures	Rossouw Von Solms; Kerry-Lynn Thomson; Prosecutor Mvikeli Maninjwa	2011	IEEE/SCOPUS
18	Information Security Management – Defining Approaches to Information Security Policies in ISMS	Zoran Cosic; Marija Boban	2010	IEEE/SCOPUS
19	Intrusion Detection with Autoencoder Based Deep Learning Machine	Oğuz KAYNAR; Ahmet Gürkan YÜKSEK; Yasin GÖRMEZ; Yunus Emre IŞIK	2017	IEEE/SCOPUS
20	Merging Prioritized Security Policies	Rania EL BAIDA	2006	IEEE/SCOPUS
21	On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center	Dedy Achmadi; Yohan Suryanto; Kalamullah Ramli	2018	IEEE/SCOPUS
22	Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat	Oliver Buckley; Jason R. C. Nurse; Philip A. Legg; Michael Goldsmith; Sadie Creese	2014	IEEE/SCOPUS
23	The Enemy Within: A Behavioural Intention Model and an Information Security Awareness Process	Tapiwa Gundu; Stephen V Flowerday	2012	IEEE/SCOPUS
24	A Mathematical Framework for	Alexander M. Melin;	2013	IEEE/SCOPUS

	the Analysis of Cyber-Resilient Control Systems	Erik M. Ferragut; Jason A. Laska; David L. Fugate; Roger Kisner		
25	A Proposal of Information Security Policy Agreement Method for Merger and Acquisition Using Assurance Case and ISO 27001	Nobuyuki Kobayashi; Aki Nakamoto; Maki Kawase; Makoto Ioki	2019	IEEE
26	A Software Gateway to Affordable and Effective Information Security Governance in SMMEs	Jacques Coertze; Rossouw von Solms	2013	IEEE
27	A Study on Information Security Level Evluation using Fuzzy AHP	Taewon Kyung; Kyunghun Kim; Sangkuk Kim; Youngjae Song	2011	IEEE
28	Advanced Security Policy Implementation for Information Systems	Sattarova Feruza Yusufovna	2008	IEEE
29	An Ontology-based Approach to the Formalization of Information Security Policies	Fernando Náufel do Amaral; Carlos Bazílio	2006	IEEE
30	Automating Information Security Policy Compliance Checking	Debashis Mandal; Chandan Mazumdar	2018	IEEE
31	Conceptual Information Modelling Within the Contemporary Information Security Policies	Aleksandar Klaic; Marin Golub	2013	IEEE
32	Crowd Energy Information Security Culture - Security Guidelines for Smart Environments	Stephanie Teufel; Bernd Teufel	2015	IEEE
33	Current Taxonomy of Information Security Threats in Software Development Life Cycle	Alexander V. Barabanov; Alexey S. Markov; Maksim I. Grishin; Valentin L. Tsirlov	2018	IEEE
34	Enforcing Business Rules and Information Security Policies through Compliance Audits XISSF - A Compliance Specification Mechanism	Frederick Yip; Pradeep Ray; Nandan Paramesh	2006	IEEE
35	Evaluation of Vulnerability Risk Factor: Critical ICT Outsourcing Project Characteristics	Nik Zulkarnaen Khidzir; Azlinah Mohamed; Noor Habibah Arshad	2014	IEEE
36	Examining the Effects of Knowledge, Attitude and Behaviour on Information	Jasber Kaur; Norliana Mustafa	2013	IEEE

	Security Awareness: A Case on SME			
37	Ignorance to Awareness: Towards an Information Security Awareness Process	T. Gundu; S.V. Flowerday	2013	IEEE
38	Impact of Information Security Policies on Email-Virus Propagation	YUAN Hua; CHEN Guoqing	2005	IEEE
39	Implementation of a Socially Engineered Worm to Increase Information Security Awareness	Erlo Meister; Elmarie Biermann F'Satie	2008	IEEE
40	A Segurança da Informação nas Sociedades de Revisores Oficiais de Contas Portuguesas	Isadora Lima; Isabel Pedrosa; Sónia Rito	2020	IEEE
41	Information Security threats and attacks with conceivable counteraction	Preeti sinhá; Amit kumar rai; Bharat Bhushan	2019	IEEE
42	Integrating Your Information Security Vulnerability Management Capabilities Through Industry Standards (CVE & OVAL)	Robert A. Martin	2003	IEEE
43	Machine Learning Model of an Intelligent Decision Support System in the Information Security Sphere	Fyodor O. Fedin; Oleg V. Trubienko; Sergey V. Chiskidov	2020	IEEE
44	Managing Security of Critical Information Infrastructure	S. D. Erokhin	2019	IEEE
45	Mathematical Modeling of the Assessing Process the of Security Level of the Complex Organizational and Technical Systems of Industrial Enterprises	Ritov M.Y; Gorlov A.P; Eryomenko V.T	2016	IEEE
46	Nicter: An Incident Analysis System toward Binding Network Monitoring with Malware Analysis	Daisuke Inoue; Masashi Eto; Katsunari Yoshioka; Shunsuke Baba; Kazuya Suzuki; Junji Nakazato; Kazuhiro Ohtaka; Koji Nakao	2008	IEEE
47	Ontology-based Decision Support for Information Security Risk Management	Andreas Ekelhart; Stefan Fenz; Thomas Neubauer	2009	IEEE
48	Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review	Mohammed Abdullah Bawazir; Murni Mahmud; Nurul Nuha Abdul Molok; Jamaludin Ibrahim	2016	IEEE

49	Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology	Bao Hongrui; He Haiguang; Liu Zhe; Liu Zhongwei	2019	IEEE
50	Social Engineering Attack Strategies and Defence Approaches	Ibrahim Ghafir; Vaclav Prenosil; Ahmad Alhejailan; Mohammad Hammoudeh	2016	IEEE
51	The Development of Method for Evaluation of Information Security Threats in Critical Systems	Anton N. Kamenskih; Mikhail A. Filippov; Alexander A. Yuzhakov	2020	IEEE
52	The Iterated Weakest Link	Michael Lesk; Jeffrey MacKie-Mason	2010	IEEE
53	Theorem Proving for Modeling and Conflict Checking of Authorization Policies	Devrim Unal; M. Ufuk Qaglayan	2006	IEEE
54	Threats Modeling and Quantitative Risk Analysis in Industrial Control Systems	Irina Mashkina; Ildar Garipov	2018	IEEE
55	Towards a Holistic Understanding of Security Process: Formal Controls and Informal Relationships	Max Soyref; Philip Seltsikas	2014	IEEE
56	Towards Metamodel-based Approach for Information Security Awareness Management	Ahmed Yousuf Jama; Maheyzah Md Siraj; Rashidah Kadir	2014	IEEE
57	Towards the Intelligent Application of Security Controls	George O. M. Yee	2020	IEEE
58	Using Sequential Exploratory Mixed Methods Design to Explore Readability of ISPs	Yazeed Alkhurayyif; George R S Weir	2018	IEEE
59	A Conceptual Model of Information Security Compliant Behaviour Based on The Self-Determination Theory	Yotamu Gangire; Adéle Da Veiga; Marlien Herselman	2019	SCOPUS
60	Uma Contribuição para a Segurança da Informação: Um Estudo de Casos Múltiplos com Organizações Brasileiras	Napoleão Verardi Galegale; Edison Luiz Gonçalves Fontes; Bernardo Perri Galegale	2017	SCOPUS
61	A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Informatio Security Awareness	Hwee-Joo Kam; Thomas Mattson; Sanjay Goel	2019	SCOPUS
62	A Framework for Reporting and Dealing with End-User Security Policy Compliance	Mutlaq Jalimid Alotaibi; Steven Furnell; Nathan Clarke	2018	SCOPUS

63	A Framework to Mitigate Social Engineering through Social Media within the Enterprise	Heidi Wilcox; Maumita Bhattacharya	2016	SCOPUS
64	A Human Dimension of Hacking: Social Engineering Through Social Media	Heidi Wilcox; Maumita Bhattacharya	2020	SCOPUS
65	A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research	Simon Trang; Benedikt Brendel	2019	SCOPUS
66	A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses	Agata McCormac; Dragana Calic; Marcus Butavicius; Kathryn Parsons; Tara Zwaans; Malcolm Pattinson	2017	SCOPUS
67	Abductive Innovations in Information Security Policy Development: An Ethnographic Study	Marko Niemimaa; Elina Niemimaa	2019	SCOPUS
68	AHP-based Security Decision Making: How Intention and Intrinsic Motivation Affect Policy Compliance	Ahmed Alzahrani; Christopher Johnson	2019	SCOPUS
69	An Evaluation of the Proposed Framework for Access Control in the Cloud and BYOD Environment	Khalid Almarhabi; Kamal Jambi; Fathy Eassa; Omar Batarfi	2018	SCOPUS
70	An Examination of Factors that Influence the Number of Information Security Policy Violations in Qatari Organizations	Hasan M. Al-Mukahal; Khaled Alshare	2015	SCOPUS
71	An Impact of Information Security Investment on Information Security Incidents: A Case of Korean Organizations	Hansol Lee; Eunkyung Kwon; Kyeongwon Yoo; Sangmi Chai	2016	SCOPUS
72	An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network	Nachaat AbdElatif Mohamed; Aman Jantan; Oludare Isaac Abiodun	2018	SCOPUS
73	An Information Security Awareness Program to Address Common Security Concerns in IT Unit	Shadi Al Awawdeh; Abdallah Tubaishat	2014	SCOPUS
74	An Information Security Maturity Evaluation Mode	Xiao-yan; YUAN Yu-qing; LU Li-lei	2011	SCOPUS
75	An Information Security Policy Development Life Cycle	Tite Tuyikeze; Dalenca Pottas	2010	SCOPUS

76	An Integrative Behavioral Model of Information Security Policy Compliance	Sang Hoon Kim; Kyung Hoon Yang; Sunyoung Park	2014	SCOPUS
77	An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective	JinYoung Han; Yoo Jung Kim; Hyungjin Kim	2016	SCOPUS
78	An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector	Melissa K. Chinyemba ; Jackson Phiri	2018	SCOPUS
79	Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions	Hussain Aldawood; Geoffrey Skinner	2020	SCOPUS
80	Applications of Social Network Analysis in Behavioural Information Security Research: Concepts and Empirical Analysis	Duy Dang-Pham; Siddhi Pittayachawan; Vince Bruno	2016	SCOPUS
81	Are You Ready When It Counts? IT Consulting Firm's Information Security Incident Management	Maja Nyman; Christine Große	2019	SCOPUS
82	Assessing Information Security Vulnerabilities and Threats to Implementing Security Mechanism and Security Policy Audit	Mohammed A.M. Afifi	2020	SCOPUS
83	Behaviour of Outsourced Employees as Sources of Information System Security Threats	David Oyebisi; Kennedy Njenga	2020	SCOPUS
84	Benchmarking Methodology for Information Security Policy (BMISP): Artifact Development and Evaluation	Martin (Dae Youp) Kang; Anat Hovav	2018	SCOPUS
85	Big Data Security Analytics in Clinical Data using Cryptographic Algorithms	Steena Gracious; Geethu Nandanan; Dagma K. R; Hari Narayana	2019	SCOPUS
86	Building an Awareness-Centered Information Security Policy Compliance Model	Alex Koohang; Jonathan Anderson; Jeretta Horn Nord; Joanna Paliszkiewicz	2020	SCOPUS
87	Can Cyberloafing and Internet Addiction Affect	Lee Hadlington; Kathryn Parsons	2017	SCOPUS

	Organizational Information Security?			
88	Can Individuals' Neutralization Techniques be Overcome? A Field Experiment on Password Policy	Mikko Siponen; Petri Puhakainen; Anthony Vance	2019	SCOPUS
89	Can Perceptual Differences Account for Enigmatic Information Security Behaviour in an Organisation?	WD Kearney; HA Kruger	2016	SCOPUS
90	Choosing Controls to Protect Against Targeted Attacks. Application of the Analytical Threat Intelligence.	S Filshtinskiy	2013	SCOPUS
91	Conceptualization of User's Rage Assessment Using Chatbot Interface by Implementing Kansei Engineering Methodology for Information Security	Noor Afiza Mat Razali; Khairul Khalil Ishak; Nurjannatul Jannah Aqilah MdSaad; Norulzahrah Mohd Zainudin; Norasiakin Hasbullah; Mohd Fahmi Mohamad Amran	2020	SCOPUS
92	Consensus Ranking – An ICT Security Awareness Case Study	H.A. Kruger; W.D. Kearney	2008	SCOPUS
93	Contagion in Cyber Zecurity Attacks	Adrian Baldwin; Iffat Gheyas; Christos Ioannidis; David Pym; Julian Williams	2016	SCOPUS
94	Critical Impact of Organizational and Individual Inertia in Explaining Non-Compliant Security Behavior in the Shadow IT Context	Mario Sillic	2018	SCOPUS
95	Demographic Factors in Cyber Security: An Empirical Study	Shweta Mittal; P. Vigneswara Ilavarasan	2019	SCOPUS
96	Design and Validation of Information Security Culture Framework	Areej AlHogail	2015	SCOPUS
97	Deterrent Effects of Punishment and Training on Insider Security Threats: A Field Experiment on Phishing Attacks	Bora Kim; Do-Yeon Lee; Beomsoo Kim	2019	SCOPUS
98	Developing an Information Security Policy: A Case Study Approach	Fayez Hussain Alqahtani	2017	SCOPUS
99	Development of Methods and Models of Computer-Aided	V E Trushnikov; N N Baranova; M V Grishin	2020	SCOPUS

	Design of Security System Against Information Threats for Aviation-Instrumentmaking			
100	Do Employees in a “Good” Company Comply Better with Information Security Policy? A Corporate Social Responsibility Perspective	Hyungjin Lukas Kim; Jinyoung Han	2018	SCOPUS
101	Do I Really Belong?: Impact of Employment Status on Information Security Policy Compliance	Shwadhin Sharma; Merrill Warkentin	2018	SCOPUS
102	Eating the Forbidden Fruit: Human Curiosity Entices Data Breaches	Dustin Ormond; Hwee-Joo Kam; Philip Menard	2019	SCOPUS
103	Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures	Anthony Vancea; Mikko T. Siponenb; Detmar W. Strauba	2019	SCOPUS
104	Employee Security Behaviour: The Importance of Education and Policies in Organisational Settings	Lena Y. Connolly; Michael Lang; Doug J. Tygar	2018	SCOPUS
105	Employees' Information Security Policy Compliance: A Norm Activation Perspective	Adel Yazdanmehr; JingguoWang	2016	SCOPUS
106	Enemies within: Redefi Ning the Insider Threat in Organizational Security Policy	David S. Wall	2013	SCOPUS
107	Enhancing Information Security Education and Awareness: Proposed Characteristics for a Model	Eric Amankwa; Marianne Loock; Elmarie Kritzinger	2015	SCOPUS
108	Establishing Information Security Policy Compliance Culture in Organizations	Eric Amankwa; Marianne Loock; Elmarie Kritzinger	2018	SCOPUS
109	Establishment of Methods for Information Security System Policy Using Benchmarking	Martin Kang; Ted Lee; Sungyong Um	2018	SCOPUS
110	Evaluating the Conformity of an Access Control Architecture for Virtual Organizations with ISO/IEC 17799	M.Kamel; A.Benzekri; F.Barrere; R.Laborde	2007	SCOPUS
111	Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security	Mohammad I. Merhia; Punit Ahluwaliab	2019	SCOPUS
112	Factors Affecting Individual Information Security Practices	Santos M. Galvez; Joshua D. Shackman; Indira R. Guzman;	2015	SCOPUS

		Shuyuan Mary Ho		
113	Factors Contributing to the Success of Information Security Management Implementation	Mazlina Zammani; Rozilawati Razali; Dalbir Singh	2019	SCOPUS
114	Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective	Xiaofeng Chen; Liqiang Chen; Dazhong Wu	2018	SCOPUS
115	Fear of the Unknown with Healthcare IoT Devices: An Exploratory Study	Christian Graham	2020	SCOPUS
116	Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory	Tim-Benjamin Lembcke; Kristin Masuch; Simon Trang; Sebastian Hengstler; Patience Plics; Mustafa Pamuk	2019	SCOPUS
117	Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research	Sal Aurigemma; Thomas Mattson	2019	SCOPUS
118	HI-risk: A Method to Analyse Health Information Risk Intelligence	William J Buchanan; Nicole van Deursen	2016	SCOPUS
119	How Paternalistic Leadership Influences IT Security Policy Compliance: The Mediating Role of the Social Bond	Gengzhong Feng; Jiawen Zhu; Nengmin Wang; Huigang Liang	2019	SCOPUS
120	How to Train People to Increase Their Security Awareness in IT	Agata Niescieruk; Bogdan Ksiezopolski; Radoslaw Nielek; Adam Wierzbicki	2017	SCOPUS
121	Identification of Information Security Threats Using Data Mining Approach in Campus Network	Norkhushaini Awang; Ganthan Narayana Samya; Noor Hafizah Hassana; Nurazean Maaropa; Pritheega Magalingama; Norshaliza Kamaruddina	2020	SCOPUS
122	Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance	Ioanna Topa; Maria Karyda	2015	SCOPUS
123	Identifying Gaps in IT Retail Information Security Policy Implementation Processes Towards developing a Secure	Ileen E. van Vuuren; Elmarie Kritzinger; Conrad Mueller	2015	SCOPUS

	IT Enterprise Built on Trust			
124	Identifying Linkages Between Statements in Information Security Policy, Procedures and Controls	Vinod Pathari; Rajendra Sonar	2012	SCOPUS
125	Impact of Employees' Demographic Characteristics on the Awareness and Compliance of Information Security Policy in Organizations	Hui Na Chuaa; Siew Fan Wonga; Yeh Ching Lowa,; Younghoon Changb	2018	SCOPUS
126	Impact on the Information Security Management Due to the Use of Social Networks in a Public Organization in Ecuador	Moisés Toapanta Toapanta ; Félix Gustavo Mendoza Quimi ; Leslie Melanie Romero Lambogglia; Luis Enrique Mafla Gallegos	2020	SCOPUS
127	Improving Performance of Intrusion Detection System Using OpenCL Based General-purpose Computing on Graphic Processing Unit (GPGPU)	Ahmad Rinaldi Widianto; Charles Lim; I. Eng Kho	2015	SCOPUS
128	Individual differences and Information Security Awareness	Agata McCormac; Tara Zwaans; Kathryn Parsons; Dragana Cali; Marcus Butavicius; Malcolm Pattinson	2016	SCOPUS
129	Information Security Culture Critical Success Factors	Mohammed A. Alnatheer	2015	SCOPUS
130	Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study	Akhyari Nasir; Ruzaini Abdullah Arshah; Mohd Rashid Ab Hamid	2020	SCOPUS
131	Information Security: Definitions, Threats and Management in Dubai Hospitals Context	Mahmoud Bakkar; Ammar Alazab	2019	SCOPUS
132	Governance Practices and Critical Success Factors Suitable for Business Information Security	Yuri Bobbert; Hans Mulder	2015	SCOPUS
133	Information Security Management: An Information Security Retrieval and Awareness Model for Industry	E. Kritzingera; E. Smithb	2008	SCOPUS
134	Information Security of Smelter Automated Process Control System for Pulverized Coal Preparation	V.A. Goltsev; A.R. Bondin; S.Ya. Zhuravlev	2019	SCOPUS

135	Information Security Optimization: From Theory to Practice	David Simms	2009	SCOPUS
136	Information Security Policies: A Review of Challenges and Influencing Factors	Mutlaq Alotaibi; Steven Furnell; Nathan Clarke	2016	SCOPUS
137	Information Security Policy: A Management Practice Perspective	Moneer Alshaikh; Sean B. Maynard; Atif Ahmad; Shanton Chang	2016	SCOPUS
138	Information Security Policy: An Organizational-Level Process Model	Kenneth J. Knappa; R. Franklin Morris Jr; Thomas E. Marshall; Terry Anthony Byrdc	2009	SCOPUS
139	Information Security Policy Compliance: Leadership and Trust	Joanna Paliszkiewicz	2019	SCOPUS
140	Information Security Policy Compliance Model at Indonesian Government Institutions: A Conceptual Framework	Hadi Syahrial; Harjanto Prabowo; Dyah Budiastuti; Ford Lumban Gaol	2019	SCOPUS
141	Information Security Policy Development and Implementation: The What, How and Who	Stephen V. Flowerday; Tite Tuyikeze	2016	SCOPUS
142	Information Security Policy Perceived Compliance Among Staff in Palestine universities: An Empirical Pilot study	Yousef Mohammad Iriqat; Abd Rahman Ahlan; Nurul Nuha Abdul Molok	2019	SCOPUS
143	Information Security Practice in Saudi Arabia: Case Study on Saudi Organizations	Zakarya Alzamil	2018	SCOPUS
144	Information System Security: Human Aspects	Zaied Shouran; Tri Kuntoro Priyambodo; Ahmad Ashari	2019	SCOPUS
145	Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts	A. J. Burns	2017	SCOPUS
146	Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs About Effective Cyber Protection	James Nicholson; Lynne Coventry; Pam Briggs	2018	SCOPUS
147	Issues and Trends in Information Security Policy Compliance	Surayahani Hasnul Bhaharin; Umi Asma' Mokhtar; Rossilawati Sulaiman; Maryati Mohd Yusof	2019	SCOPUS

148	Keeping Secure to the End: a Long-Term Perspective to Understand Employees' Consequence-Delayed Information Security Violation	Ying Li; Nan Zhang; Mikko Siponen	2019	SCOPUS
149	Key Success Factors of Information Systems Security	Krunoslav Arbanas; Nikolina Žajdela Hrustek	2019	SCOPUS
150	Knowing is Doing: An Empirical Validation of the Relationship Between Managerial Information Security Awareness and Action	Namjoo Choi; Dan Kim; Jahyun Goo; Andrew Whitmore	2008	SCOPUS
151	Lessons Learned from an Organizational Information Security Awareness Campaign	Juan-Marc Scrimgeour; Jacques Ophoff	2019	SCOPUS
152	Main Considerations in Elaborating Organizational Information Security Policies	Todor Tagarev; Dimitrina Polimirova	2019	SCOPUS
153	Managers' and Employees' Differing Responses to Security Approaches	Puzant Balozian; Dorothy Leidner; Merrill Warkentin	2019	SCOPUS
154	Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach	Mukul Gupta; Jackie Rees; Alok Chaturvedi; Jie Chi	2004	SCOPUS
155	Mathematical modeling method based on genetic algorithm and its applications	L V Stepanov; A S Koltsov; A V Parinov; A S Dubrovin	2019	SCOPUS
156	Measurement of Employee Information Security Awareness: Case Study at A Government Institution	Eka Ayu Puspitaningrum; Ferizka Tiara Devani; Vidya Qoriah Putri; Achmad Nizar Hidayanto; Solikin; Ika Chandra Hapsari	2018	SCOPUS
157	Measuring Information Security Awareness on Employee Using HAIQS-Q: Case Study XYZ Firm	Alvin Cindana; Yova Ruldeviyani	2018	SCOPUS
158	More Than the Individual: Examining the Relationship Between Culture and Information Security Awareness	Ashleigh Wiley; Agata McCormac; Dragana Cali	2019	SCOPUS
159	Motivating Information Security Policy Compliance: Insights from Perceived	Yuxiang Hong; Steven Furnell	2019	SCOPUS

	Organizational Formalization			
160	National Information Security Policy and its Implementation: A Case Study in Taiwan	Cheng-YuanKu; Yi-WenChang; DavidC.Yen	2009	SCOPUS
161	Neural Correlates of Decision Making Related to Information Security: Self-Control and Moral Potency	Robert West; Emily Budde; Qing Hu	2019	SCOPUS
162	Optimizing Investment Decisions in Selecting Information Security Remedies	Dov Shirtz; Yuval Elovici	2011	SCOPUS
163	Outsourcing Deviance: When 3rd Party Technology Innovativeness Becomes a Threat to Information Systems	Kennedy Njenga; David Oyebisi	2018	SCOPUS
164	Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance	Adel Yazdanmehr; Jingguo Wang; Zhiyong Yang	2019	SCOPUS
165	Persona-Driven Information Security Awareness	Duncan Ki-Aries; Shamal Faily; Kristian Beckers	2016	SCOPUS
166	Persuasive Information Security: Techniques to Help Employees Protect Organizational Information Security	Marc Busch; Sameer Patil; Georg Regal; Christina Hochleitner; Manfred Tscheligi	2016	SCOPUS
167	Preparing for Cyber Threats with Information Security Policies	Ilona Ilvonen; Pasi Hellsten	2015	SCOPUS
168	Productivity vs. Security: Mitigating Conflicting Goals in Organizations	Peter Mayer; Nina Gerber; Ronja McDermott; Melanie Volkamer; Joachim Vogt	2017	SCOPUS
169	Proposing SETA Program Design Based on Employee Motivational Fit	Philip Menard	2016	SCOPUS
170	Protecting Intellectual Property From Insider Threats A Management Information Security Intelligence Perspective	Hyungjin Lukas Kim; Anat Hovav; Jinyoung Han	2019	SCOPUS
171	Protective Measures and Security Policy Non-Compliance Intention: IT Vision Conflict as a Moderator	Kuo-Chung Chang; Yoke May Seow	2019	SCOPUS
172	Readability as a Basis for Information Security Policy Assessment	Yazeed Alkhurayyif; George R S Weir	2017	SCOPUS

173	Research on the Security Analysis and Management of the Network Information System Based on the Big Data Decision Making	Weigang Liu	2020	SCOPUS
174	Rethinking the Prevailing Security Paradigm: Can User Empowerment with Traceability Reduce the Rate of Security Policy Circumvention?	Soohyun Jeon; Anat Hovav; Jinyoung Han; Steven Alter	2018	SCOPUS
175	Review of Information Security Guidelines for Awareness Training Program in Healthcare Industry	Arash Ghazvini; Arash Ghazvini	2017	SCOPUS
176	Reviewing Cyber Security Social Engineering Training and Awareness Programs - Pitfalls and Ongoing Issues	Hussain Aldawood; Geoffrey Skinner	2019	SCOPUS
177	BYOD Security Risks and Mitigations	Melva Ratchford; Ping Wang; Raed Omar Sbeit	2018	SCOPUS
178	Risk Model Development for Information Security in Organization Environment Based on Business Perspectives	Prajna Deshanta Ibnugraha; Lukito Edi Nugroho; Paulus Insap Santosa	2020	SCOPUS
179	Scope and Limitations of Ethical Hacking and Information Security	Rakshitha C M	2020	SCOPUS
180	Security Access Control Research Trends	Mohamed Fathy; Marianne Azer; Moustapha Bahgat; Ayman Yehia	2013	SCOPUS
181	Security Monitoring and Information Security Assurance Behaviour Among Employees: An Empirical Analysis	Zauwiyah Ahmad; Thian Song Ong; Tze Hui Liew; Mariati Norhashim	2019	SCOPUS
182	Security Policy Opt-in Decisions in Bring-Your- Own-Device (BYOD) – A Persuasion and Cognitive Elaboration Perspective	Xue Yang; Xinwei Wang; Wei Thoo Yue; Choon Ling Sai; Xin (Robert) Luo	2019	SCOPUS
183	Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study	Dhoha Almubayedh; Mashael Al khalis; Ghadeer Alazman; Manal Alabdali; Rouqaiah Al-Refai; Naya Nagy	2018	SCOPUS
184	Shaping Intention to Resist Social Engineering Through	Waldo R. Flores; Mathias Ekstedt	2016	SCOPUS

	Transformational Leadership, Information Security Culture and Awareness			
185	Smartphone Information Security Awareness: A victim of Operational Pressures	Sean Allam; Stephen V. Flowerday; Ethan Flowerday	2014	SCOPUS
186	Social Control Through Deterrence on the Compliance with Information Security Policy	Myeonggil Choi; Jeongseok Song	2018	SCOPUS
187	Specification and Validation of Enterprise Information Security Policies	Anirban Sengupta; Chandan Mazumdar; Aditya Bagchi	2012	SCOPUS
188	Stakeholder Perceptions of Information Security Policy: Analyzing Personal Constructs	Spyridon Samonasa; Gurpreet Dhillon; Ahlam Almusharraf	2020	SCOPUS
189	Strategic Planning for Information Security – DID Mechanism to Befriend the Cyber Criminals to Assure Cyber Freedom	M.K.Jayanthi	2017	SCOPUS
190	Study on E-Government Information Misuse based on General Deterrence Theory	Jing Fan; Pengzhu Zhang	2011	SCOPUS
191	The Dark Side of Social Networking Sites: Understanding Phishing Risks	Mario Silic; Andrea Back	2016	SCOPUS
192	The Impact of Audit Firms' Characteristics on Audit Fees Following Information Security Breaches	Ju-Chun Yen; Jee-Hae Lim; Tawei Wang; Carol Hsu	2018	SCOPUS
193	The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study	Adéle Da Veiga	2015	SCOPUS
194	The Influence of Security Control Management and Social Factors in Deterring Security Misbehaviour	H.A.Hamid; M.M.Yusof; N.R.S.Mohd Dali	2019	SCOPUS
195	The Perception of Information Security Threats Surrounding the Cloud Computing Environment	Heba Mohammed Fadhil	2018	SCOPUS
196	The Role of Organizational Factors to the Effectiveness of ISMS Implementation in Malaysian Public Sector	Noralinawati Ibrahim; Nor'ashikin Ali	2018	SCOPUS
197	The Sufficiency of the Theory of Planned Behavior for	Teodor Sommestad; Henrik Karlzén; Jonas	2015	SCOPUS

	Explaining Information Security Policy Compliance	Hallberg		
198	The Use of AHP in Security Policy Decision Making: An Open Office Calc Application	Irfan Syamsuddin; Junseok Hwang	2010	SCOPUS
199	Towards a User-Centric Theory of Value-Driven Information Security Compliance	Neil F. Doherty; Sharul T. Tajuddin	2018	SCOPUS
200	Understanding Commitment and Apathy in is Security Extra-Role Behavior from a Person Organization Fit Perspective	Hao Chen; Wenli Li	2019	SCOPUS
201	Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective	John D'Arcy; Tejaswini Herath; Mindy K. Shoss	2014	SCOPUS
202	Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity	Chunghun Lee; Choong C. Lee; Suhyun Kim	2016	SCOPUS
203	Understanding the Value of Countermeasure Portfolios in Information Systems Security	Ram L. Kumar; Sungjune Park; Chandrasekar Subramaniam	2008	SCOPUS
204	Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors	John M Blythe; Lynne Coventry; Linda Little	2015	SCOPUS
205	Violators Versus Non-Violators of Information Security Measures in Organizations—A Study of Distinguishing Factors	Habib Ullah Khan; Khalid A. AlShare	2019	SCOPUS
206	Which are the Most Effective Measures for Improving Employees' Security Compliance?	Martin Kretzer; Alexander Maedche	2015	SCOPUS
207	Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace	Duy Dang-Pham; Siddhi Pittayachawan; Vince Bruno	2016	SCOPUS
208	Work-Related Groups and Information Security Policy Compliance	Teodor Sommestad	2018	SCOPUS

APÊNDICE B – TABELA DE EXTRAÇÃO DE DADOS

Identificador	[PN01]
A) Dados da publicação:	
Título:	A Symptomatic Framework to Predict the Risk of Insider Threats
Autor (es):	Joris Ikany and Husin Jazri
Fonte de Publicação:	IEEE
Ano de Publicação:	2019
Resumo:	A constante mudança de tecnologias trouxe às organizações de infraestrutura crítica inúmeras ameaças à segurança da informação, como ameaças internas.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Ferramenta (Framework)
Recomendação de Segurança da Informação:	O quadro de ameaças demonstrou que avaliar as ameaças internas utilizando uma análise de base sintomática funciona bem e é eficaz para detectar precocemente sintomas de possíveis ameaças internas prevalecentes em organizações de infraestruturas críticas e as medidas preventivas podem ser tomadas rapidamente assim que estas áreas específicas forem identificadas.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Insiders (Roubo de uma propriedade, Sabotagem de TI, Espionagem e Fraude)
Informações Adicionais:	Esses insiders passam a ser ameaças quando o uso indevido, acidental ou deliberadamente desse acesso de forma prejudicial de maneira que afeta a Confidencialidade, Integridade ou Disponibilidade (CID) do Sistema de Informação de Segurança da Organização.

Identificador	[PN02]
A) Dados da publicação:	
Título:	Anomaly-based Insider Threat Detection using Deep Autoencoders
Autor (es):	Liu Liu, Olivier De Vel, Chao Chen, Jun Zhang e Yang Xiang.
Fonte de Publicação:	International Conference on Data Mining Workshops (ICDMW)
Ano de Publicação:	2018
Resumo:	Nos últimos anos, a ameaça interna mal-intencionada tornou-se uma das ameaças mais significativas de segurança cibernética a que uma organização pode estar sujeita.

B) Dados derivados do objetivo:	
Tipo de recomendação:	Ferramenta (Framework)
Recomendação de Segurança da Informação:	Um sistema de detecção que implemente a detecção de anomalias usando um conjunto de Autocodificadores Profundos.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Insider
Informações Adicionais:	Insiders não apenas se escondem atrás da segurança defensiva embutida mecanismos da rede, mas também poderia ter conhecimento detalhado sobre a rede.

Identificador	[PN03]
A) Dados da publicação:	
Título:	Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat
Autor (es):	Oliver Buckley, Jason R. C. Nurse, Philip A. Legg, Michael Goldsmith e Sadie Creese
Fonte de Publicação:	4th Workshop on Socio-Technical Aspects in Security and Trust
Ano de Publicação:	2014
Resumo:	A política de segurança da informação de uma empresa é um controle excepcionalmente importante, pois fornece aos funcionários de uma organização detalhes sobre o que se espera deles e o que eles podem esperar das equipes de segurança da organização, além de informar a cultura dentro dessa organização.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Modelo (Conjunto de questões)
Recomendação de Segurança da Informação:	Propomos uma especialização de um quadro para capturar pontos de dados pertinentes que podem então ser reduzidos a um conjunto de causas, vetores de ataque e impactos a uma organização.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Insider (Erro Humano, Politica não Seguidas, Email, Disposição Incorreta dos recursos, Perdido/danificado em trânsito, Engenharia Social, Vírus/Malware, dados indevidamente protegidos e dados copiados para dispositivos inseguros).
Informações Adicionais:	Pode-se argumentar que a motivação de um insider acidental é, na maioria dos casos, para cumprir seu papel e como tal, suas motivações são em sua maioria

	positivas e bem intencionado.

Identificador	[PN04]
A) Dados da publicação:	
Título:	Implementation of a Socially Engineered Worm to Increase Information Security Awareness
Autor (es):	Erlo Meister e Elmarie Biermann F'satie
Fonte de Publicação:	Third International Conference on Broadband Communications, Information Technology & Biomedical Applications
Ano de Publicação:	2008
Resumo:	Os usuários de computador são vistos como o elo mais fraco na cadeia de segurança do computador. Esses usuários são enganados para a execução de código malicioso por meio da utilização de táticas de engenharia social combinadas com, por exemplo, tecnologia de e-mail.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Prática
Recomendação de Segurança da Informação:	Implementação de um worm de engenharia social para aumentar a conscientização sobre segurança da informação
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Engenharia Social
Informações Adicionais:	-

Identificador	[PN05]
A) Dados da publicação:	
Título:	Social Engineering Attack Strategies and Defence Approaches
Autor (es):	Ibrahim Ghafir, Vaclav Prenosil, Ahmad Alhejailan e Mohammad Hammoudeh
Fonte de Publicação:	4th International Conference on Future Internet of Things and Cloud
Ano de Publicação:	2016
Resumo:	Este artigo examina o papel e o valor dos esforços de conscientização da segurança da informação na defesa contra ataques de engenharia social.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Prática
Recomendação de Segurança da Informação:	Categoriza as diferentes ameaças, engenharias sociais e táticas usadas na segmentação de funcionários e as

	abordagens para se defender contra tais ataques.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Engenharia Social
Informações Adicionais:	-

Identificador	[PN06]
A) Dados da publicação:	
Título:	A Framework to Mitigate Social Engineering through Social Media within the Enterprise
Autor (es):	Heidi Wilcox e Maumita Bhattacharya
Fonte de Publicação:	11th Conference on Industrial Electronics and Applications (ICIEA)
Ano de Publicação:	2016
Resumo:	A engenharia social por meio da mídia social é uma preocupação empresarial formidável devido à tendência dos engenheiros sociais de direcionar os funcionários por meio desses meios para atacar os ativos de informação que residem na organização.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Ferramenta (Framework)
Recomendação de Segurança da Informação:	A estrutura fornece um ponto de referência para a governança das mídias sociais para demonstrar um nível aceitável de segurança da informação nessas tecnologias e dentro da cultura de segurança dos usuários.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Engenharia Social
Informações Adicionais:	Os principais danos às organizações resultantes da engenharia social à mídia social incluem perda de reputação e / ou responsabilidade legal por meio do funcionário, vazamento inadvertido de informações, postagem de conteúdo impróprio ou introdução de malware / vírus nas redes da empresa.

Identificador	[PN07]
A) Dados da publicação:	
Título:	AHP-based Security Decision Making: How Intention and Intrinsic Motivation Affect Policy Compliance
Autor (es):	Ahmed Alzahrani e Christopher Johnson

Fonte de Publicação:	(IJACSA) International Journal of Advanced Computer Science and Applications
Ano de Publicação:	2019
Resumo:	O processo de hierarquia analítica é uma ferramenta de múltiplos critérios usada em aplicativos relacionados à tomada de decisão.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Modelo
Recomendação de Segurança da Informação:	Processo de hierarquia analítica é usado como orientação na tomada de decisão da política de segurança da informação, identificando os fatores de influência e seus pesos para a conformidade da política de segurança da informação.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Cyber-attack, uso de e-mail e internet, resposta a incidentes e conformidade com políticas.
Informações Adicionais:	O método AHP para orientar a tomada de decisões políticas foi utilizado para determinar os fatores e os seus pesos para garantir a conformidade com os ISPs.

Identificador	[PN08]
A) Dados da publicação:	
Título:	An Evaluation of the Proposed Framework for Access Control in the Cloud and BYOD Environment
Autor (es):	Khalid Almarhabi, Kamal Jambi, Fathy Eassa E Omar Batarfi
Fonte de Publicação:	(IJACSA) International Journal of Advanced Computer Science and Applications
Ano de Publicação:	2018
Resumo:	À medida que a tendência de trazer seu próprio dispositivo (BYOD) para o trabalho cresce, também aumentam os riscos à segurança da rede. Essa tendência de crescimento rápido traz enormes benefícios para funcionários e empregadores.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Ferramenta (Framework)
Recomendação de Segurança da Informação:	Uma estrutura que reduz as restrições do sistema, ao mesmo tempo em que aplica políticas de controle de acesso para ambientes BYOD e de nuvem, utilizando uma plataforma independente.

Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Malware, spyware e outros downloads maliciosos.
Informações Adicionais:	-

Identificador	[PN09]
A) Dados da publicação:	
Título:	An Information Security Awareness Program to Address Common Security Concerns in IT Unit
Autor (es):	Shadi Al Awawdeh e Abdallah Tubaishat
Fonte de Publicação:	11th International Conference on Information Technology: New Generations
Ano de Publicação:	2014
Resumo:	Conscientização é de longe a técnica de maior sucesso que não custa muito quando em comparação com treinamento e educação e pode reduzir o gasto total com segurança.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Sistema
Recomendação de Segurança da Informação:	Um sistema de segurança da informação programa de conscientização (ISAP)
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Ativos Organizacionais
Informações Adicionais:	Na maioria das organizações, grandes ou pequenas, protegendo o ambiente contra crimes cibernéticos é geralmente o papel da unidade de tecnologia da informação.

Identificador	[PN10]
A) Dados da publicação:	
Título:	An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector
Autor (es):	Melissa K. Chinyemba e Jackson Phiri
Fonte de Publicação:	Journal of Computer Science
Ano de Publicação:	2018
Resumo:	Ataques internos são violações de segurança representadas por uma parte interessada organizacional existente ou anterior com direitos de acesso irrestrito aos recursos que, com ou sem intenção, comprometem a confidencialidade, integridade e disponibilidade dos dados organizacionais.

B) Dados derivados do objetivo:	
Tipo de recomendação:	Modelo
Recomendação de Segurança da Informação:	Um modelo expediente de mitigação interna com ênfase na conscientização do usuário e controle de acesso, considerando que é difícil modelar o comportamento humano.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Insider (Sabotagem, Fraude)
Informações Adicionais:	

Identificador	[PN11]
A) Dados da publicação:	
Título:	Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions
Autor (es):	Hussain Aldawood e Geoffrey Skinner
Fonte de Publicação:	Digital Object Identifier
Ano de Publicação:	2020
Resumo:	A engenharia social é uma das maiores ameaças que as organizações enfrentam hoje, à medida que mais e mais organizações estão adotando a digitalização.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Medida
Recomendação de Segurança da Informação:	Medidas contra os desafios de segurança da informação enfrentados pelas organizações
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Engenharia Social
Informações Adicionais:	Ataques cibernéticos podem ter como alvo a parte técnica de um sistema, mas outros tipos de ataques são projetados para atingir o elemento humano e dependem das vulnerabilidades do pessoal. Esses ataques são considerados incidentes de engenharia social.

Identificador	[PN12]
A) Dados da publicação:	
Título:	Contagion in cyber security attacks
Autor (es):	Adrian Baldwin, Iffat Gheyas, Christos Ioannidis, David Pym e Julian Williams
Fonte de Publicação:	Journal of the Operational Research Society

Ano de Publicação:	2016
Resumo:	A segurança dos sistemas é essencial para a operação eficiente de todas as organizações. Na verdade, a maioria das grandes empresas emprega um 'Chief Information Security Officer' designado para coordenar os aspectos operacionais das informações da organização segurança.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Sistema
Recomendação de Segurança da Informação:	Um sistema de equação vetorial de ameaças para 10 importantes serviços de IP, usando dados SANS padrão da indústria sobre ameaças a vários componentes das informações de uma empresa sistema durante o período de janeiro de 2003 a fevereiro de 2011.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Ataques a SSH e Secure Web Server
Informações Adicionais:	-

Identificador	[PN13]
A) Dados da publicação:	
Título:	Demographic Factors in Cyber Security: An Empirical Study
Autor (es):	Shweta Mittal e P. Vigneswara Ilavarasan
Fonte de Publicação:	IFIP International Federation for Information Processing
Ano de Publicação:	2019
Resumo:	Apesar da segurança dos sistemas de informação de alta qualidade, as organizações são vulneráveis a ataques cibernéticos devido a falhas no comportamento humano.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Recomendação
Recomendação de Segurança da Informação:	Sugestões para programas de treinamento de conscientização de segurança da informação para lidar com as inadequações
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Ativo (Fator Humano)
Informações Adicionais:	-

Identificador	[PN14]
A) Dados da publicação:	

Título:	Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks
Autor (es):	Bora Kim, Do-Yeon Lee e Beomsoo Kim.
Fonte de Publicação:	Behaviour e Information Technology
Ano de Publicação:	2019
Resumo:	Não há dúvida de que as ameaças à segurança organizacional estão surgindo atualmente, interna e externamente. Em um esforço para prevenir ameaças internas - violações de funcionários da política de segurança da informação (ISP) - programas de treinamento de segurança e políticas de sanção são implementados em grande parte nas organizações.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Medida
Recomendação de Segurança da Informação:	Medidas de dissuasão eficazes e políticas para segurança da informação organizacional
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Phishing.
Informações Adicionais:	No contexto organizacional, phishing é arriscado porque pode desativar a defesa organizacional Sistemas de TI, atacando os usuários desses sistemas. Portanto, programas para educar os funcionários a evitar phishing golpes são extremamente importantes para proteger valiosas informações organizacionais.

Identificador	[PN15]
A) Dados da publicação:	
Título:	Developing an Information Security Policy: A Case Study Approach
Autor (es):	Fayez Hussain Alqahtani
Fonte de Publicação:	4th Information Systems International Conference
Ano de Publicação:	2017
Resumo:	As informações e dados organizacionais devem ser protegidos de ataques ativos e passivos e protegidos contra acesso ilegal, interrupção indesejada, alteração não autorizada ou aniquilação.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Abordagem
Recomendação de Segurança da Informação:	Explorou a implementação de ISPs em uma grande organização para avaliar a

	adequação da política e determinar o usuário conscientização e cumprimento de tais políticas.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Gerenciamento de senhas, uso de e-mail, internet e sites de redes sociais, computação móvel e tratamento de informações
Informações Adicionais:	-

Identificador	[PN16]
A) Dados da publicação:	
Título:	Identification of Information Security Threats Using Data Mining Approach in Campus Network
Autor (es):	Norkhushaini Awang, Ganthan Narayana Samya, Noor Hafizah Hassana, Nurazean Maaropa, Pritheega Magalingama e Norshaliza Kamaruddina
Fonte de Publicação:	Journal of Physics: Conference Series
Ano de Publicação:	2020
Resumo:	A implementação de uma avaliação de risco abrangente em uma organização é crucial para proteger os ativos valiosos da organização e minimizar as ameaças à segurança da informação.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Controle
Recomendação de Segurança da Informação:	Orientar o administrador da rede, á desenvolver um plano de resposta para incidentes apropriados com base, nas ameaças identificadas do risco, atividade de avaliação.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Phishing, ransomware, e malware; WI-FI; Propagação de vírus através das redes sociais; Dispositivos móveis e Dispositivos Embutidos
Informações Adicionais:	A avaliação de risco é parte de um processo de gestão de risco projetado para fornecer níveis adequados de segurança para sistemas de informação.

Identificador	[PN17]
A) Dados da publicação:	
Título:	Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues
Autor (es):	Hussain Aldawood e Geoffrey Skinner
Fonte de Publicação:	Future internet
Ano de Publicação:	2019

Resumo:	A ideia e a percepção de uma boa proteção de segurança cibernética permanecem na vanguarda da estratégia e do investimento em tecnologia da informação e comunicação de muitas organizações.
B) Dados derivados do objetivo:	
Tipo de recomendação:	Recomendação
Recomendação de Segurança da Informação:	Recomenda estratégias para enfrentar os desafios do ponto visão dos tomadores de decisão de segurança nas organizações.
Ameaças, vulnerabilidades e/ou comportamentos de risco no contexto de Segurança da Informação:	Engenharia Social
Informações Adicionais:	A eficiência dos sistemas de informação organizacional no combate às ameaças da engenharia social necessita da combinação de medidas técnicas avançadas, juntamente com esforços gerenciais para aumentar conscientização do pessoal.