UNIVERSIDADE DE SÃO PAULO
ESCOLA DE COMUNICAÇÕES E ARTES
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ALEXANDRE TEIXEIRA SALGADO

Contribuições da Terminologia no processo de conscientização em Segurança da Informação

Versão Corrigida
(versão original disponível na Biblioteca da ECA/USP)

São Paulo
2021

ALEXANDRE TEIXEIRA SALGADO

Contribuições da Terminologia no processo de conscientização em Segurança da Informação

Versão Corrigida (versão original disponível na Biblioteca da ECA/USP)

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Comunicações e Artes da Universidade de São Paulo para obtenção do título de Mestre em Ciências.

Área de Concentração: Cultura e Informação

Linha de pesquisa: Organização da Informação e do Conhecimento

Orientadora: Prof.ª. Dra. Vânia Mara Alves Lima

São Paulo

2021

Catalogação na publicação
Serviço de Biblioteca e Documentação
Escola de Comunicação e Artes da Universidade de São Paulo
Dados inserido pelo autor.

Salgado, Alexandre Teixeira
Contribuições da Terminologia no processo de conscientização em Segurança da Informação / Alexandre Teixeira Salgado; orientadora, Vânia Mara Alves Lima. - São Paulo, 2022.
96 p.: il.

Dissertação (Mestrado) - Programa de Pós-Graduação em Ciência da Informação / Escola de Comunicações e Artes / Universidade de São Paulo.
Bibliografia
Versão corrigida

1. Segurança da Informação. 2. Ciência da Informação. 3. Conscientização de Usuários. 4. Análise de Domínio. 5. Terminologia. I. Alves Lima, Vânia Mara. II. Título.

CDD 21.ed. - 20

Elaborado por Alessandra Vieira Canholi Maldonado - CRB-8/6194

FOLHA DE AVALIAÇÃO

Alexandre Teixeira Salgado

Contribuições da Terminologia no processo de conscientização em Segurança da Informação

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Comunicações e Artes da Universidade de São Paulo para obtenção do título de Mestre em Ciências.

Aprovado em: 10/12/2021

Banca Examinadora

Prof. Dr. _____
Instituição: _____
Julgamento: _____ Assinatura: _____

Prof. Dr. _____
Instituição: _____
Julgamento: _____ Assinatura: _____

Prof. Dr. _____
Instituição: _____
Julgamento: _____ Assinatura: _____

Prof. Dr. _____
Instituição: _____
Julgamento: _____ Assinatura: _____

AGRADECIMENTOS

À minha esposa Wanessa Salgado e à minha filha Valentina Salgado. Obrigado por todo o suporte e paciência, não apenas para a conclusão desta pesquisa, mas em tudo que envolve nossas vidas.

Ao amigo Prof. Dr. Leandro Fabricio Campelo, que foi fundamental durante o processo seletivo. Agradeço todas as conversas, dicas, empréstimo de livros e, principalmente por ter intercedido junto a ECA no processo seletivo nos momentos em estive impossibilitado.

Aos amigos do Banco BNP Paribas: Alessandro Roncatti, Daniel Yamaoka, Eduardo Tavares, Gregory Cardoso e Rafael Martin, por todo o apoio dado para a minha entrada no programa de pós-graduação e durante o seu transcorrer. Em muitos momentos, a vontade de jogar a tolha foi grande, mas vocês estavam à disposição para não deixar isso acontecer.

Ao Prof. Dr. Francisco Paleta e ao Prof. Dr. Rogerio Ramalho, que, durante as arguições no exame de qualificação, apresentaram críticas, sugestões e comentários que resultaram na reavaliação dos objetivos gerais e específicos da pesquisa e, consequentemente, contribuíram seu enriquecimento.

À Prof.ª. Dra. Vania Mara Alves Lima, que com sua orientação, puxões de orelha e empurrões que me ajudaram a finalizar esta pesquisa.

Aos diversos amigos que fiz na ECA, enquanto aluno especial e como aluno regular. As conversas e compartilhamento de informações foram essenciais para tornar a caminhada mais leve, já que passávamos pelas mesmas dificuldades.

Por último e não menos importante, agradeço a Deus, que concedeu a mim do uma segunda oportunidade para tentar fazer as coisas de maneira melhor nesse plano.

A obrigação de produzir aliena a paixão de criar.

Raoul Vaneigem

RESUMO

SALGADO, Alexandre Teixeira. **Contribuições da Terminologia no processo de conscientização em Segurança da Informação**. 2021. 104 f. Dissertação (Mestrado Acadêmico) – Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2021.

Ameaças e incidentes de segurança da informação têm tido grande destaque na mídia nos últimos tempos. O número de incidentes de segurança mostra que todos podem ser alvos de atacantes. Os ataques podem ser estruturados e direcionados às corporações dos mais diversos segmentos com o objetivo de roubar informações sensíveis e monetizar esse produto. Por outro lado, podem ser ataques simples, que visam obter acesso, por exemplo, ao aplicativo WhatsApp de pessoas físicas comuns com o intuito de executar golpes financeiros. Esta pesquisa tem como objetivo geral demonstrar como o uso da Terminologia no domínio Segurança da Informação pode contribuir na mitigação dos riscos oriundos do fator humano nos ataques à segurança da informação. Isso é feito através da pesquisa bibliográfica e documental, conduzindo o estudo para um âmbito exploratório, visando desenvolver conceitos e ideias. Para tanto, a pesquisa contextualiza os aspectos teóricos da análise de domínio e mostra a análise descritiva do domínio Segurança da Informação com base em um framework de segurança cibernética e em uma certificação profissional da área de segurança da informação, ambos globalmente conhecidos. Segue para o cerne da pesquisa, abordando a teoria envolvida nas diversas vertentes da Terminologia e que, consequentemente, apoiam a os estudos termológicos do domínio Segurança da Informação. Estes estudos terminológicos descrevem e comparam os significados técnicos de termos utilizados em Segurança da Informação, mas com significados diferentes em outras áreas de conhecimento. Por fim, o estudo apresenta um levantamento bibliométrico básico para abordar a produção cientifica em documentos em língua inglesa e suportar o tópico de tradução de textos especializados.

Palavras-chave: Segurança da Informação. Segurança Cibernética. Ciência da Informação. Engenharia Social. Conscientização de Usuários. Análise de Domínio. Terminologia.

ABSTRACT

SALGADO, Alexandre Teixeira. **Contributions of Terminology in the Information Security Awareness Process**. 2021. 104 f. Dissertação (Mestrado Acadêmico) – Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2021.

Information security threats and incidents have been prominent in the media lately. The number of security incidents shows that everyone can be targeted. Attacks can be structured having as target different-industries and large corporations to exfiltrate sensitive information and monetize this "product". In contrast, the attacks can be simple to gain access, for example, to the common people's WhatsApp application to carry out financial scams. The main objective of this research is to demonstrate how the use of Terminology in the Information Security domain can contribute to the mitigation of risks arising from the human factor in information security attacks. This is reached by executing bibliographical and documentary research. This leads the research to an exploratory scope to develop concepts and ideas. Therefore, the research contextualizes the theoretical aspects of domain analysis and shows the descriptive analysis of the Information Security domain based on a cybersecurity framework and on a professional certification in the information security area, both well-known globally. This leads to the core of the research, approaching all the theory involved in the different aspects of Terminology and support the terminological studies in the Information Security domain in consequence. These terminological studies describe and compare the technical meanings of terms used in Information Security, but with different concepts in other areas of knowledge. Finally, the study presents a basic bibliometric information gathering to address the scientific production of documents in English language and support the topic mentioning about translation of specialized texts.

Keywords: Information Security. Cybersecurity. Information Science. Social Engineering. User awareness. Domain Analysis. Terminology.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

CBK	-	*Common Body of Knowledge*
CERT.BR	-	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CI	-	Ciência da Informação.
CID	-	Confidencialidade, Integridade e Disponibilidade
CISSP	-	*Certified Information Systems Security Professional*
COBIT	-	*Control Objectives for Information and Related Technologies*
DBIR	-	*Data Breach Investigations Report*
ENISA	-	*European Union Agency for Cybersecurity*
GDPR	-	*General Data Protection Regulation*
ISC²	-	*International Information System Security Certification Consortium*
ISO	-	*International Organization for Standardization*
ITIL	-	*Information Technology Infrastructure Library*
LAN	-	*Local Area Network*
LGPD	-	Lei Geral de Proteção de Dados Pessoais
MAN	-	*Metropolitan Area Network*
NIST	-	*National Institute of Standards and Technology*
OSI	-	*Open System Interconnection*
SANS	-	*System Administration, Networking and Security*
SI	-	Segurança da Informação.
TCP/IP	-	*Transport Control Protocol / Internet Protocol*
TCT	-	Teoria Comunicativa da Terminologia
TGT	-	Teoria Geral da Terminologia
WAN	-	*Wide Area Network*

SUMÁRIO

1. INTRODUÇÃO

"Se você acredita que a tecnologia pode resolver seus problemas de segurança, então você não conhece os problemas e nem a tecnologia" (SCHNEIER, 2004)

Em maio de 2017, um ataque cibernético pelo *ransomware* Wannacry infectou mais de 200 mil sistemas em 150 países ao redor do mundo, causando estragos em indústrias, serviços públicos, operadoras de telefonia móvel e gerou perdas financeiras estimadas em 4 bilhões de dólares[1]. Pouco tempo depois, um novo ataque por *ransonware*, conhecido por NotPetya, voltou a desesperar equipes de Tecnologia da Informação e de Segurança da Informação ao redor do mundo. Um dos maiores prejuízos noticiados foi da multinacional de logística marítima MAERSK. O ataque fez a empresa dinamarquesa perder US$300 milhões em receita[2]. Desta então, estes números aumentaram e os ataques por *Ransomware* foi o mais comum entre as empresas brasileiras em 2021[3]. Ainda em 2021, uma subsidiária da empresa JBS nos Estados Unidos pagou um resgate de US $11 milhões para os atacantes[4].

Ransomware, segundo a definição do CERT.BR, é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso do usuário".[5] Ele se propaga através da exploração de vulnerabilidades técnicas em sistemas que não tenham recebido os devidos cuidados de segurança. A intenção desta pesquisa não é abordar as questões técnicas relacionadas à segurança da informação, mas os problemas de linguagem na transmissão de informações durante o processo de conscientização e da necessidade de se garantir a segurança da informação em uma instituição. Sob essa perspectiva, essa pesquisa se insere no âmbito da Ciência da Informação, pois vai tratar dos fluxos da informação, sua representação e apropriação em um sistema de informação. Relaciona-se também à Terminologia visto que terminologias dos domínios da segurança da informação contribuem nas etapas de representação e apropriação da informação.

Isto se justifica, porque o sucesso do ataque relatado só foi possível através da exploração de uma outra vulnerabilidade que não possui sistema, *software, hardware* ou

[1] https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses.
[2] https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.
[3] https://www.tecmundo.com.br/seguranca/223158-ransomware-ataque-comum-entre-empresas-brasileiras-2021.htm
[4] https://epocanegocios.globo.com/Tecnologia/noticia/2021/12/os-maiores-ataques-hackers-de-2021.html
[5] https://cartilha.cert.br/ransomware.

qualquer outra solução técnica para eliminá-la: o **fator humano**. E o método que permite explorar vulnerabilidades em pessoas é a **engenharia social**.

O ***National Institute of Standards and Technology*** (NIST), em seu documento **NIST SP 800-114**, define engenharia social como sendo:

> Um termo usado para os atacantes que tentam enganar as pessoas para revelar informações confidenciais ou executar determinadas ações, como baixar e executar arquivos que parecem ser benignos, mas são realmente maliciosos (tradução nossa).[6]

Assim, entende-se que a engenharia social estuda o conhecimento do comportamento humano e das suas características, com intuito de induzir um indivíduo a atuar conforme o desejo de quem a executa.

No caso do WannaCry e NotPetya, foram utilizadas técnicas de *phishing scam* induzindo usuários a clicar em um *link*, para baixar e abrir/executar um arquivo e, desta forma, instalar o código malicioso no computador.

Estatísticas mostradas pela feita pela Verizon, uma empresa americana do ramo de telecomunicações com mais de 200 milhões de clientes ao redor do mundo, no documento *Verizon Data Breach Investigations Report* (DBIR) lançado em 2017 tem alguns dados interessantes para ataques de engenharia social ocorridos em 2016[7] corroboram essa afirmação. A empresa estudou 42.068 incidentes de segurança que resultaram em 1.935 violações. No geral, 43% das violações documentadas envolveram ataques de engenharia social. Não surpreendentemente, 66% dos *malwares* vieram em anexos de e-mail mal-intencionados. Estes poderiam ter sido e-mails de ataques de *phishing scam* ou podem ter vindo de uma conta confiável que havia sido atacada anteriormente. De qualquer forma, a maioria das infecções por *malware* começou com um e-mail com conteúdo malicioso. A versão 2021 do mesmo relatório lançado pela Verizon mostrou que, por volta de 80% dos ataques de engenharia social relatados na pesquisa, ocorreram na forma de *phishing*[8].

É importante ressaltar que este tipo de ataque não é exclusivo do mundo corporativo. O ambiente doméstico também está sujeito a tais riscos. Apenas com o uso de ferramentas tecnológicas ou com a implantação de processos e políticas de segurança mais

[6] SP 800-114 Rev. 1, User's Guide to Telework and Bring Your Own Device Security | CSRC (nist.gov) - https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final
[7] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.
[8] https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

robustas não é suficiente para proteger a confidencialidade, integridade e disponibilidade das informações – há de se pensar no fator humano e suas vulnerabilidades. Uma máxima largamente mencionada no campo de segurança da informação diz que "o ser humano é o elo mais fraco desta corrente" (SCHNEIER, 2004). Neste caso, é necessário valorizar o treinamento para o bom entendimento e elaborar campanhas de conscientização para sensibilizar os usuários das vulnerabilidades inerentes do ser humano e das ameaças que exploram essas vulnerabilidades que o envolvem e que são viabilizadas por meio da atuação da engenharia social (MITNICK; SIMON, 2003, p. 195).

No ambiente corporativo, as principais ameaças à segurança da informação têm origem na própria organização. Os ataques feitos por funcionários já foram considerados alguns dos mais perigosos, visto que estas pessoas possuem conhecimento privilegiado da organização e familiaridade com a infraestrutura e processos internos. Estes funcionários, também denominados *insiders*, não, necessariamente, são pessoas descontentes com seu trabalho e ou mesmo espiões corporativos, que representam uma ameaçam à companhia - podem ser pessoas descuidadas (HARRIS; MAYMI, 2016) ou mal treinados, sem qualquer má intenção, que também pode trazer esse tipo de risco para a empresa.

Pode parecer contraditório, mas pessoas treinadas para reconhecer ameaças, deveriam estar cientes da importância da segurança da informação que manuseiam, mas essa contradição ocorre em virtude de uma estratégia falha, pois a implantação de programas de conscientização deve variar de empresa para empresa, levando em contato seu público-alvo e os riscos inerentes à sua companhia.

Uma mensagem será mais eficaz na medida em que estiver próximo da realidade das pessoas e das corporações de que elas fazem parte. Por isso, é importante que a linguagem utilizada na comunicação desta informação que será transmitida seja adaptada a cada público-alvo a que ela se destina, uma vez que todos têm responsabilidade no sucesso da estratégia de segurança da informação. A linguagem utilizada com um executivo sênior de uma grande corporação não pode ser a mesma para um profissional da área financeira, um professor, ou mesmo um adolescente. Todos têm necessidades e realidades diferentes. Além disso, uma estratégia de conscientização não é um "produto de prateleira", que pode ser comprado em uma loja, tampouco não existe "receita de bolo" para alcançar seu sucesso. Desta forma, podemos concluir que adaptação das campanhas para uma audiência específica é algo intrínseco à estratégia de qualquer tipo de programa de conscientização e não é exclusivo apenas à área de segurança da informação.

Uma das melhores maneiras de garantir que os funcionários da empresa não cometam erros onerosos em relação à segurança da informação é instituir iniciativas de conscientização de segurança que incluam, mas não se limitem, a sessões de treinamento em estilo de sala de aula, sites de conscientização de segurança, dicas úteis via e-mail ou pôsteres e outros. Esses métodos podem ajudar a garantir que os funcionários tenham uma sólida compreensão da política, dos procedimentos e das práticas recomendadas de segurança da empresa. Entretanto, deve ser adotada a estratégia correta, elaborada em uma linguagem adequada para que haja a melhor absorção da informação transmitida por parte dos usuários. Desta forma, a colaboração do campo da Terminologia, como parte da área da Ciência da Informação, é importante para entender os meios para alcançar a excelência dessa adequação.

Segundo Le Coadic, a Ciência da Informação é um campo de conhecimento transversal, onde existe a colaboração mútua entre diversas áreas tais como a psicologia, linguística, sociologia, matemática, estatística, tecnologia da informação e outras e complementa afirmando que:

> "A interdisciplinaridade traduz-se por uma colaboração entre diversas disciplinas, que leva a interações, isto é, uma certa reciprocidade, de forma que haja, em suma, enriquecimento mútuo. A forma mais simples de ligação é o isomorfismo, a analogia (LE COADIC, 1994).

A Ciência da Informação também pode ser vista como campo dedicado à investigação científica para tratar as questões da comunicação de conhecimentos e registros de conhecimentos em diversos contextos (SARACEVIC, 1995). Desta forma, é possível entender que os conceitos de ambos os autores se complementam, tendo em vista que a Ciência da Informação resolve problemas complexos e este tipo de abordagem demanda enfoques interdisciplinares e soluções multidisciplinares (SARACEVIC, 1996). Todas as disciplinas envolvidas concentram os estudos dos processos de informação que objetivam a redução de incertezas (WERSIG; NEVELLING, 1975).

Em alguns de seus trabalhos, SARACEVIC (1996) concentrou esforços em estudar a interdisciplinaridade entre a Ciência da Informação e a Ciência da Computação. Enquanto a Ciência da Computação, como um campo tecnológico, trata de algoritmos relacionados à informação, a Ciência da Informação se preocupa com a natureza da informação e seu uso por seres humanos. As duas preocupações não estão em competição, mostrando-se complementares.

A Segurança da Informação, conceitualmente, tem sustentação em Processos, Tecnologia e Pessoas. Ao tratar de questões tecnológicas, mostra sua interdisciplinaridade com a área de Ciência da Computação. Por lidar com pessoas, consequentemente, ela apresenta sua conexão com a Ciência da Informação, arcando com todas as consequências que as relações humanas trazem, tais como as questões de comunicação e a conscientização de usuários.

A Ciência da Informação tem por objetivo fornecer um corpo de conhecimento com o intuito de trazer procedimentos dedicados à retenção e a transmissão de conhecimento (BORKO, 1968). Com isso, além da interdisciplinaridade, é possível apresentar algumas similaridades com a Segurança da Informação – ambas possuem um corpo de conhecimento onde existe a atuação de diversas outras áreas de conhecimento.

Uma vez que este conhecimento é um produto da interpretação dentro de várias possibilidades e para não enfrentar mais um conhecimento absoluto, a Ciência da Informação requer uma teoria terminológica que permita admitir uma multiplicidade de estruturas conceituais urdidas nos espaços de atuação ou nas comunidades de distintos discursos. Deve poder, também, dar espaço às estruturas mais abertas de organização. Por fim, apropriação da Terminologia pela Ciência da Informação não tem apenas um objetivo instrumental. O exercício de construção do espaço interdisciplinar, ao não se resumir à identificação do que é útil ou não de um campo de conhecimento para outro, coloca em jogo uma série de conceitos que não se limitam ao campo observado. As associações que caracterizam o processo de construção da interdisciplinaridade – que de modo algum se constrói pela justaposição de conceitos, mas pela sua observação focada no objeto da área (LARA, 2005).

A teoria mostra que existe possibilidade destas áreas atuarem juntas para alcançar um objetivo e com resultados positivos. A hipótese desta pesquisa resvala na questão: A Terminologia pode, de fato, contribuir com a criação e manutenção de um processo eficiente e eficaz de conscientização de usuários de informação? Se sim, como alcançar esse resultado?

2. OBJETIVOS

2.1. Gerais

Esta pesquisa tem como objetivo geral demonstrar como o uso da Terminologia no domínio Segurança da Informação pode contribuir na mitigação dos riscos oriundos do fator humano nos ataques à segurança da informação.

2.2. Específicos

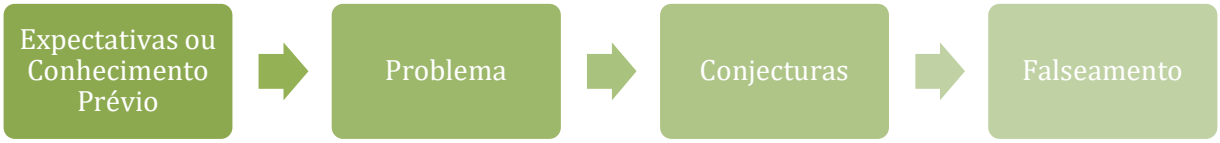
- Relacionar e mostrar interdisciplinaridade entre os campos da Ciência da Informação e da Segurança da Informação;
- Identificar os aspectos gerais do processo de Análise de Domínio, fazendo um recorte na análise do domínio Segurança da Informação e destacando o processo de conscientização de usuários em Segurança da Informação.
- Delinear os estudos terminológicos na área de Segurança da Informação, mostrando como a Terminologia pode contribuir no processo de conscientização em Segurança da Informação.
- Apresentar um glossário com termos e conceitos relevantes no processo de conscientização.

3. METODOLOGIA

Com o intuito de alcançar os objetivos gerais e específicos desta pesquisa, o método de investigação usado nessa pesquisa foi o hipotético-dedutivo.

O modelo hipotético-dedutivo de Popper (LAKATOS; MARCONI, 2003) mostra que se trata de um método que consiste em formulação de hipóteses e, consequentemente, o falseamento destas. O processo investigativo pode continuar ciclicamente para que as hipóteses sejam confirmadas ou corroboradas, segundo Popper.

Figura 1 - Método Hipotético-Dedutivo segundo Popper



Fonte: LAKATOS; MARCONI, 2003

Da perspectiva do procedimento técnico para a elaboração da pesquisa, adotei a pesquisa bibliográfica, pois foram utilizados materiais já produzidos sobre os temas a serem pesquisados para a coleta de dados, definição de conceitos e elaboração de conclusões. A pesquisa bibliográfica é procedimento técnico onde serão as literaturas relevantes já realizadas sobre o tema serão elencadas para que seja confirmada ou não determinada hipótese (SEVERINO, 2017). O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e certos erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações (LAKATOS; MARCONI, 2003). A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Esta vantagem se torna particularmente importante quando o problema de pesquisa requer dados muito dispersos pelo espaço (GIL, 2008). Isso faz sentido, justamente, quando é necessário fazer um estudo que une duas áreas de conhecimento, a Ciência da Informação e Segurança da Informação, onde o material que trata da união desses dois campos é escasso e os dados de pesquisa estão disseminados em fontes diversas. O desafio desta pesquisa, na verdade, não é somente a pesquisa bibliográfica em si, mas também o cruzamento desses dados de forma a corroborar os objetivos da pesquisa.

A pesquisa bibliográfica conduz a pesquisa para um objetivo exploratório, visando desenvolver, esclarecer e modificar conceitos e ideias. Segundo GIL (2008), a pesquisa exploratória habitualmente envolve levantamento bibliográfico e documental. No tocante a área de Segurança da Informação e apoiando o caráter exploratório da pesquisa, também haverá a pesquisa documental, pois será necessário pesquisar e levantar informações oriundas de entidades privadas e públicas, incluindo a análise de materiais utilizados em campanhas de conscientização. Também serão utilizados relatórios de pesquisas e tabelas estatísticas para contextualizar os cenários de Segurança da Informação que serão abordados durante a pesquisa. Estes documentos, contendo informações já processadas são informações

de segunda mão (LAKATOS; MARCONI, 2003). O tratamento das informações coletadas será através da avaliação qualitativa, pois haverá a produção de conclusões a partir de observações extraídas diretamente do estudo do processo.

A **Introdução** desta pesquisa foi descrita utilizando diversos materiais, uma vez que houve a necessidade de relacionar diversos assuntos que fizeram parte dessa pesquisa. Com isso, utilizei os sites de notícias Cbsnews e CNBC para mostrar notícias sobre o ataque de *ransomware* ocorrido à época em que o projeto de pesquisa foi elaborado. O site do CERT.BR foi utilizado para mostrar o significado do termo *ransomware*. Utilizei também sites do NIST para suportar o significado de alguns termos e a pesquisa de mercado extraída do site da Verizon para mostrar o cenário ataques de engenharia social ocorridos em 2016. Para as questões relacionadas com segurança da informação e engenharia social, utilizei os livros dos autores Mitnick e Simon, além de Harris e Maymi para suporte nesses assuntos. Para introduzir a ciência da Informação nesta pesquisa, utilizei o suporte de Wersig e Nevelling, Saracevic e Borko. Por fim, Lara foi utilizada como uma autora introdutória da Terminologia nesta pesquisa.

Para fazer o relacionamento entre a **Ciência da Informação e a Segurança da Informação**, utilizei Le Coadic e Capurro para descrever o paralelo entre a Segurança da Informação e a Ciência da Informação da perspectiva epistemológica. Para delinear a interdisciplinaridade da Ciência da Informação utilizei Saracevic, Wersig e Nevelling e Borko para discorreram o assunto por diferentes prismas. A tese de doutorado de Marciano, por ser um dos poucos trabalhos aborda Segurança da Informação de forma social e que a conecta à Ciência da Informação, foi utilizada para dar breve apoio ao tópico que aborda o ciclo de vida da Informação.

Para o capítulo de **Análise de Domínio**, discorri sobre este assunto, separando-o em duas partes: a primeira, descrevendo os conceitos teóricos da análise de domínio, utilizando os materiais de Hjørland e suas onze abordagens da análise de domínio focadas em Ciência da Informação. Tennis foi utilizado para fazer um contraponto com uma abordagem baseada em seus dois eixos e quatro parâmetros, aplicáveis de forma genérica em qualquer domínio e Smiraglia foi utilizado descrever brevemente a análise de domínio e a produção e disseminação de conhecimento baseado na construção de um Sistema de Organização do Conhecimento; a segunda, foquei a análise no domínio Segurança da Informação. Primeiramente, para abordar os conceitos teóricos de Segurança da Informação utilizei os livros *(ISC)² CISSP Certified Information Systems Security Professional Official*

Study Guide, de Chapple, Stewart e Gibson, o *CISSP All-in-One Exam Guide,* de Harris e Maymi e o Gestão da segurança da informação: uma visão executiva, de Sêmola. Para incluir informações adicionais sobre assuntos mencionados nesse tópico, tais como: normas, padrões certificações profissionais, foram inseridos links de internet destas organizações e empresas fabricantes de soluções tecnológicas (PCI, ISSO, ISC2, ISACA, Comptia, Cisco, Microsoft e Checkpoint. Na sequência, para analisar o domínio Segurança da Informação, utilizei o *framework* de Segurança Cibernética da organização americana NIST e a certificação profissional CISSP da organização (ISC)². Para o primeiro domínio, utilizei os materiais que descrevem o framework no site do NIST e materiais e documentos de sites do governo americano para complementar as informações. Para o segundo, também utilizei os livros (*ISC)² CISSP Certified Information Systems Security Professional Official Study Guide*, de Chapple, Stewart e Gibson, o *CISSP All-in-One Exam Guide,* de Harris e Maymi. Entretanto para fazer o recorte específico sobre conscientização de usuários, utilizei o livro Gestão da segurança da informação: uma visão executiva, de Sêmola, utilizei o livro de Bessa para descrever aspectos pedagógicos básicos de no processo de conscientização e os livros de Gardner e Thomas e o material do NIST escrito por Nieles, Dempsey e Pillitteri para ajudar a descrever o processo de conscientização em segurança da informação. Também foram utilizados alguns links de internet como notas de rodapé para acesso de informações adicionais sobre o corpo de conhecimento da certificação CISSP no site do (ISC)² e informações sobre a alteração do exame no site da alteração da Netwrix.

Descrevi o capítulo sobre Terminologia, separando-o em três partes: Aspectos Teóricos, Aspectos relacionados à Segurança da Informação e A Terminologia na tradução de textos especializados. Para o primeiro tópico, procurei descrever a relação termo e conceito e utilizei os materiais dos seguintes autores para descrever alguns aspectos teóricos gerais que suportaram essa pesquisa:

- Barros - Aspectos gerais da Terminologia
- Cabre – Teoria Comunicativa da Terminologia
- Temmerman - Terminologia Sociocognitiva
- Faulstich - Socioterminologia
- Faber - Terminologia *Frame-based*

Para o segundo tópico, utilizei materiais de Schneier e Richet para descrever a diferença entre os termos hacker e cracker. Figura do site The Hack e notícia de site de informações

mencionando ataques cibernéticos com utilização do termo “hacker” também foram utilizados. Para dar suporte teórico aos aspectos voltados à segurança da informação, utilizei Barros e Sager. Para o comparar os significados técnicos do termo “vírus” para as áreas de segurança da informação, biologia e medicina, foram utilizados os sites, respectivamente, CERT.BR, Só Biologia e Medicinenet. Para o último tópico, voltado a tradução de textos especializados, novamente utilizei os materiais de Barros, Cabré e Sager como suporte teórico ao tópico. Para ter uma dimensão na quantidade de materiais referentes a segurança da informação e a escassez deste em língua portuguesa, utilizei o site Scopus com o intuito de obter um levantamento bibliométrica que mostram esses números e a necessidade de conhecer a língua inglesa, independentemente, da língua original de criação do material, uma vez que alguns termos não são traduzíveis. Figuras extraídas do site da ENISA (European Union Agency for Cybersecurity) foram utilizadas para mostrar as diferenças de uma tradução adequada e outra inadequada em língua portuguesa. Extraí também uma figura do site CERT.BR para trazer exemplos de termos em língua inglesa que não são traduzidos em língua portuguesa.

Por fim, apresento no **Apêndice**, como contribuição deste trabalho, um glossário amostra dos termos mais relevantes para a Segurança da Informação identificados nesta pesquisa em forma de um glossário, o qual, eventualmente, poderá ser ampliado no futuro. O site *Computer Security Resource Center*, pertencente ao NIST, foi utilizado como como referência para a definição dos termos.

4. A CIÊNCIA DA INFORMAÇÃO E A SEGURANÇA DA INFORMAÇÃO

Um ativo (do inglês *asset*), pode ser definido como qualquer coisa que possua valor dentro de uma organização, mas que pode extrapolar esse perímetro e dar contornos pessoais a este conceito. Documentos pessoais (registros e exames médicos, informações financeiras e extratos bancários e objetos com alto valor financeiro ou sentimental (joias, obras de arte) são exemplos de ativos em um contexto pessoal.

Voltando ao contexto corporativo, podemos incluir itens tangíveis e intangíveis. Como exemplo de itens tangíveis, podem ser classificados como sendo, por exemplo, os equipamentos, imóveis e sistemas e tudo aquilo que é possível precificar, de alguma maneira. Como itens intangíveis, temos, por exemplo, as pessoas, a reputação de uma organização e, nos tempos da Sociedade da Informação, obviamente, a informação (HARRIS; MAYMI, 2016).

Desta forma, empresas das mais variadas áreas de atuação, desde escolas e universidades até indústrias e empresas da área financeira, possuem a informação como um ativo que objetiva um aumento de produtividade, uma tomada de decisão estratégica, redução de custos, segredos de negócio ou um diferencial competitivo (SÊMOLA, 2003). Em linhas gerais, independentemente do segmento de atuação, a informação serve para balizar a gestão destas organizações.

Entretanto, na Sociedade da Informação e em um mundo altamente conectado, em 2019, onde em uma população de 7,67 bilhões de pessoas, 57% da população mundial está conectada à rede mundial de computadores e 45% são usuários ativos de redes sociais (WE ARE SOCIAL, 2019), Segurança da Informação não deveria ser uma preocupação apenas das organizações, mas de todas as pessoas físicas, como indivíduos. No Brasil, temos 70% de usuários de Internet e 66% de usuários ativos em redes sociais para uma população de 211 milhões de pessoas (ROCK CONTENT, 2019).

Abordar questões relacionadas a privacidade e segurança da informação ilustrando situações que usam tecnologias como exemplo é simples, uma vez que algumas pessoas tendem a acreditar que Segurança da Informação e Tecnologia da Informação são sinônimos e versam, exatamente, sobre os mesmos assuntos. Outras tendem a acreditar que Segurança da Informação e Tecnologia da Informação são assuntos diferentes, mas complementares. Para estas, sempre existe uma ferramenta tecnológica capaz de protegê-la de um problema de Segurança da Informação. Entretanto, a Tecnologia é apenas uma parte da tríade que suporta os princípios desta área de conhecimento, que também contempla

Processos e Pessoas. Com isso, os cuidados com a privacidade e a adoção de comportamentos seguros relacionados à Segurança da Informação servem não apenas para quem lida com computadores, Internet e outras ferramentas tecnológicas, mas com todos aqueles que, de alguma maneira, lidam com informação. Treinamento, educação e conscientização em assuntos relacionados à Segurança da Informação, de maneira ampla, são necessários a todos os indivíduos.

É importante ressaltar que a as questões relacionadas à privacidade, que antes eram, exclusivamente, atribuídas ao indivíduo e sem qualquer contrapartida por parte das entidades que detinham a posse dessas informações, agora andam a passos largos para um cuidado bidirecional – assim como os indivíduos devem salvaguardar suas informações pessoais, mas que, em algum momento da sua vida social, será necessário fornecê-las, as empresas também terão obrigações legais na adoção de contramedidas para proteger estas mesmas informações.

A Lei Geral de Proteção de Dados Pessoais, conhecida pela sigla LGPD, irá contribuir para a criação de um ordenamento, através de leis e princípios que tem por objetivo maior controle e a preservação de informações pessoais. Inspirada na legislação europeia *General Data Protection Regulation* (GDPR), este regulamento adotado pela União Europeia e aprovado em abril de 2016, indicando que indivíduos, empresas públicas e privadas e governo terão papéis e responsabilidades bem delimitadas nesse processo[9]. O cumprimento dessa lei implicará às empresas, instituições públicas e privadas a obrigatoriedade de deixar ainda mais evidenciada para os cidadãos brasileiros a forma de coleta, armazenamento e uso de seus dados pessoais, dentre outros aspectos. Desta forma, para a manutenção destes aspectos, é necessário a implantação de controles de proteção e isso torna evidente a ligação entre este regulamento e a Segurança da Informação.

Se, para o campo de atuação da Segurança da Informação, a informação é um bem de valor e, consequentemente, deve ser devidamente protegida, para a Ciência da Informação, a informação deve ser disseminada, comunicada. Esta diferente significação fica bastante evidente quando o ciclo de vida da informação em ambas as áreas de conhecimento é analisado.

Para Le Coadic (1994), a informação é um conhecimento inscrito (gravado) sob a forma escrita (impressa ou digital), oral ou audiovisual, que se comporta como elemento de sentido, onde um significado é transmitido a um ser consciente através de uma mensagem

[9] https://www.serpro.gov.br/lgpd/

com o objetivo de obter conhecimento. Esse processo de comunicação é definido como “o intermediário que permite a troca de informações entre as pessoas. É um ato, um processo, um mecanismo, e que a informação, é um produto, uma substância, uma matéria” (LE COADIC, 1994, p. 11).

O modelo social do ciclo da informação desenhado por Le Coadic (1994, p. 11) mostra que um processo de comunicação se encarrega de transmitir uma informação. Através do uso desta, ocorre a criação de um conhecimento. O papel da comunicação consiste em assegurar o intercâmbio de informações (LE COADIC 1994, p. 33) e o processo cíclico de uso desta informação irá gerar a criação de novos conhecimentos.

Figura 2 – Ciclo da Informação de Le Coadic

Fonte: LE COADIC (1994) adaptado pelo autor.

Em termos epistemológicos, CAPURRO (2003) confronta o conceito de informação com diversas áreas. A informação é a unidade básica para o desenvolvimento econômico, tendo em sua natureza digital a sua característica mais relevante.

Nas corporações o compartilhamento de informações passou a ser um termo de ordem para uma gestão moderna e com celeridade. A tecnologia passou a viabilizar essa rapidez interconectando computadores, digitalizando informações e automatizando processos. A informação passou a ser gerada, armazenada e utilizada em grandes volumes e disseminou-se em todos os seus departamentos. Estas novas condições elevaram o risco das empresas e as fizeram compreender a necessidade da adoção de controles que permitam abrandar os riscos ou trazê-los para níveis aceitáveis (SÊMOLA, 2003). Não obstante, essa

situação transcende os limites das corporações e situação semelhante passou a acontecer na vida dos indivíduos na Sociedade da Informação.

Independentemente se a informação precisa ser protegida ou divulgada, existem, para ambas as áreas, algumas unanimidades acerca de seu significado. A primeira, que está relacionado ao conhecimento. A segunda está relacionada à primeira - tornou-se uma mercadoria. Segundo MARX (1985), a mercadoria é algo que satisfaz a necessidade humana, seja ela produto de algo físico ou de sua imaginação. O corpo da referida mercadoria, faz dela um valor de uso, que se realiza no uso e no consumo. Isso fica mais evidente à medida que o capitalismo passa a fazer uso da grande massa de informações fornecidas pelos indivíduos através das plataformas. A concorrência criada pelo capitalismo faz com que seja necessário conseguir e manter clientes e a análise dessas informações para que esta se torne um produto ou serviço personalizado para cada indivíduo (SRNICEK, 2018).

O relacionamento da Ciência da Informação e Segurança da Informação assim como as suas diferenças e semelhanças do conceito de informação podem ser observados de várias formas. Uma destas formas, é o ciclo de vida da informação em seus ciclos de vida. A Segurança da Informação visa a proteção da informação em seu ciclo de vida durante as etapas de manuseio que a colocam em risco (SÊMOLA, 2003). Tanto CHAPPLE, STEWART, GIBSON (2018) como HARRIS, MAYMI (2016) apontam que a proteção da informação depende de um processo prévio de classificação desta, pois é necessário apresentar racionalidade aos controles (Processos, Pessoas e Tecnologias) que serão aplicados para proteger tal ativo.

Existem diversas formas de classificar e usar essas classificações, mas as denominações utilizadas por algumas corporações, por exemplo, são SECRETA, CONFIDENCIAL, INTERNA e PÚBLICA. No quadro abaixo, pode ser observado alguns exemplos de classificação, assim como exemplos de uso:

Tabela 1 – Exemplo de tipos de classificação e usos elaborado pelo autor

CLASSIFICAÇÃO	EXEMPLOS DE USO
SECRETA	As informações podem ser acessadas por **usuários específicos** da empresa.
CONFIDENCIAL	As informações podem ser acessadas por **áreas ou grupos específicos** da empresa.
INTERNA	As informações podem ser **acessadas por todos os usuários** da empresa.
PÚBLICA	As informações podem ser livremente **divulgadas dentro e fora** da empresa.

Fonte: elaborado pelo autor

Proteger informações pressupondo que todas são “Secretas” implica em um alto custo na implantação de controles suficientes para protegê-la. Por outro lado, classificá-las como “Públicas”, os controles aplicados estarão aquém ao necessário e, neste caso, informações sensíveis serão colocadas em risco. Independentemente da classificação adotada para determinada informação, está terá um ciclo de vida que, na perspectiva de Segurança da Informação, inicia na sua criação e termina em seu descarte. Vários modelos de ciclo de vida que podem ser adotados, porém, para o campo da Segurança da Informação, será abordado o modelo descrito por HARRIS, MAYMI (2016), que apresenta quatro níveis em seu fluxo:

Figura 3 – Ciclo de Vida da Informação em SI

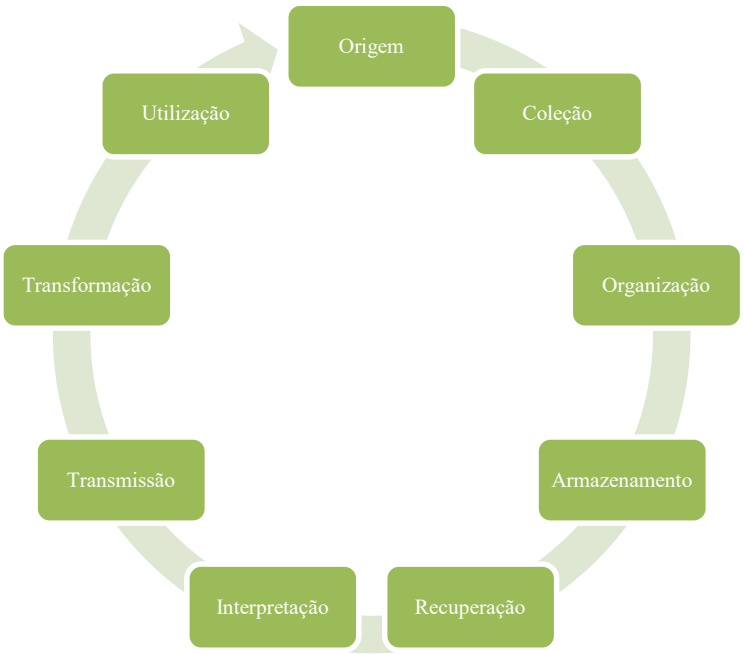
Fonte: HARRIS, MAYMI (2016).

A etapa de Aquisição é onde essa informação é formada, não importando a forma como ela é gerada. Pode ser uma informação escrita ou um registro digital, em um banco de

dados. Após a criação, na etapa de Uso, a informação passa a ser manuseada e é nesta fase que a Confidencialidade, Disponibilidade e Integridade passam a ser um desafio, uma vez que a informação somente é útil se existe o respeito a essa tríade. Logo após, na etapa de Arquivamento, a informação é guardada, ou seja, é armazenada em arquivos, quando a informação é física ou em discos e fitas de cópia de segurança, quando digital. É importante observar que as etapas de Uso e Arquivamento são cíclicas, pois a informação é usada e arquivada diversas vezes em seu ciclo de vida até seguir para o Descarte. Nesta etapa e informação não é mais útil e pode ser eliminada, mas, mês da mesma forma, critérios de segurança precisam ser adotados, seja para eliminar os documentos físicos em uma fragmentadora de papéis, por exemplo, ou a destruição de discos rígidos e fitas contendo cópias de segurança, quando em formato digital.

O ciclo de vida da informação sob a ótica da Ciência da Informação mostra a preocupação com sua disseminação e usabilidade. O modelo mencionado por Borko (1968) descreve como etapas de seu ciclo de vida a Origem, Coleta, Organização, Armazenagem, Recuperação, Interpretação, Transmissão, Transformação e Utilização. Este modelo mostra a interdisciplinaridade da Ciência da Informação, pois representa sistemas naturais e artificiais, assim como os dispositivos de processamento de informações.

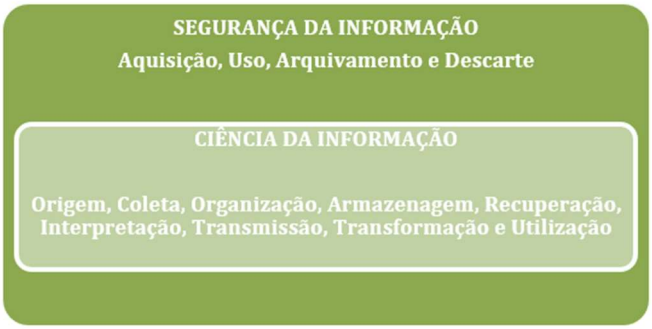
Figura 4 – Ciclo de Vida da Informação em Ciência da Informação



Fonte: BORKO (1968) adaptado pelo autor.

Entretanto, todas estas etapas estão sujeitas à riscos de segurança, que podem ocorrer em diversos deste ciclo de vida (MARCIANO, 2006). O ciclo de vida em Segurança da Informação deve criar uma camada de proteção de forma que o ciclo de vida proposto pela Ciência da Informação não sofra com possíveis ameaças.

Figura 5 - Modelo de integração do ciclo de vida de SI e CI



Fonte: elaborado pelo autor.

Por fim, é importante observar a Segurança da Informação como um domínio de conhecimento a ser analisado. HJØRLAND (2004) menciona a sua visão de uma humanização da Tecnologia da Informação e que a análise de domínio é uma abordagem que conecta a teoria e a prática. Isso pode ser estendido à Segurança da Informação, uma vez que esta é uma área oriunda da Tecnologia, porém também orientada às pessoas. Associar teoria é prática é crucial para mitigar riscos e evitar incidentes. Nesse aspecto, a conscientização dos usuários de informações. Entender a terminologia básica comumente utilizada e veiculada nas grandes mídias é um ponto inicial importante para conscientização e, com isso, tentar alcançar o estado da arte em Segurança da Informação. Os estudos terminológicos associados às questões de linguagem têm por obrigação trazer uma apropriação destes termos e, consequentemente, deste conhecimento de uma maneira natural para o público leigo.

5. ANÁLISE DO DOMÍNIO SEGURANÇA DA INFORMAÇÃO

5.1. Definição de Análise de Domínio

Primeiramente, é necessário definir o que um domínio. De maneira ampla e acadêmica, Hjørland e Albrechtsen definem domínios como comunidades de pensamento ou discurso, que comunidades, que fazem parte da divisão de trabalho da sociedade (1995, p. 400). Poderia ser uma área do conhecimento, o conjunto de literatura sobre um tópico ou mesmo um sistema de pessoas e práticas trabalhando com uma linguagem comum, (TENNIS, 2003, p. 191). Pode ser mais bem compreendido como uma unidade de análise para a construção de um Sistema de Organização do Conhecimento (SOC). Isto é, um domínio é um grupo com uma base ontológica que revela uma teleologia subjacente, um conjunto de hipóteses comuns, consenso epistemológico nas abordagens metodológicas, e semântica social, (SMIRAGLIA, 2012, p. 114).

Em 1995, Hjørland e Albrechtsen descreveram um paradigma analítico de domínio dentro da ciência da informação. De fato, usando a metáfora “vinho velho em garrafas novas” eles trouxeram juntos componentes da ciência da informação que já estavam em uso, mas não em conjunto, para demonstrar o poder da capacidade de identificar domínios explicitamente. O foco tornou-se a descrição do conhecimento - domínios, comunidades nas quais os indivíduos são vistos como membros participantes - sendo uma implicação de cumplicidade explícita na fixação dos limites do domínio. Um meio de tal participação pode ser como parte de uma comunidade discursiva. O objetivo do artigo de Hjørland e Albrechtsen não era definir esses termos; antes, sua intenção era demonstrar a utilidade da análise de domínio para o estudo de hipóteses em ciência da informação. Assim, resta-nos inferir uma relação hierárquica entre um domínio e uma comunidade do discurso. O insight apresentado é a aplicação da teoria da atividade à compreensão dos domínios, que mudaram as bases epistemológicas da ciência da informação da cognição simples para uma ontologia teleológica realista.

A descrição mais completa da análise de domínio vem de HJØRLAND (2002), que elabora a metodologia de uma abordagem analítica de domínio da ciência da informação por enumerando onze etapas que podem fornecer informações sobre um domínio. Estas abordagens, delineadas por Freitas e Albuquerque (2017) são:

- **Guias de literatura e portais de assuntos especializados**: onde organizam as listagens de fontes de informação de acordo com a função e tipologia dos recursos nos domínios de conhecimento. Podem demonstrar os pontos semelhantes e diferentes das obras, a inter-relação entre os temas, apoiar a gestão feita pelo usuário da literatura especializada além de evidenciar as descrições ideológicas das fontes informacionais e como estas se relacionam;

- **Elaboração de tesauros e classificações especializadas**: vocabulários utilizados especificamente para um domínio. Organizados através de relações semânticas, sinonímias, ou seja, utilizam a estrutura lógica e semântica para a organização das categorias e dos conceitos de um domínio.

- **Indexação e recuperação especializada**: aperfeiçoar a recuperação da informação através da organização dos conteúdos dos recursos informacionais melhorando assim a visibilidade das informações e os aspectos epistemológicos potenciais.

- **Estudos empíricos de usuários**: procuram estabelecer o comportamento de busca, estratégias cognitivas e preferências dos usuários a fim de organizar os domínios de acordo com os modelos mentais de contexto dos usuários de informação.

- **Estudos Bibliométricos**: a partir das métricas da produção do conhecimento a possibilidade de conhecer as conexões entre os documentos, entre os pesquisadores e os assuntos tratados, assim como perceber qual a abrangência geográfica destes elementos para que possam ser relacionados.

- **Estudos históricos**: possibilidade de estudos a partir das origens, epistemologia, fundamentações, formas de expressão e diferentes influências dos domínios do conhecimento.

- **Estudos de gênero e documentais**: consideram as estruturas e os elementos que as disciplinas ou as comunidades discursivas elaboram tipos de documentos de acordo com suas necessidades.

- **Estudos críticos e epistemológicos**: permite a organização dos documentos de acordo com o entendimento das diferenças entre os paradigmas, abordagens, técnicas e metodologias dos domínios.

- **Estudos terminológicos, de linguagem e de discurso**: possibilita compreender os problemas sobre a linguagem controlada e natural, as relações semânticas e os possíveis discursos para uma melhor recuperação das informações.

- **Estudos das estruturas e das comunidades científicas**: conhecimento dos indivíduos e instituições para distinguir as especificidades envolvidas concernentes ao domínio.

- **Análise de domínio em cognição profissional e inteligência artificial**: possibilita o estudo a partir de modelos mentais ou métodos para organizar o conhecimento na concepção de sistemas peritos.

No entanto, para Tennis (2003), as onze abordagens delineadas por Hjørland não permitem compartilhar as definições e os limites do que está sendo analisado. Servindo para a Ciência da Informação, parece mais importante definir o paradigma analítico de domínio do que o objeto de investigação. Tennis menciona a necessidade de outros dois dispositivos analíticos para ajudar a formalizar essa discussão. Estes dispositivos ou eixos delineiam o que está sendo estudado por um analista de domínio e trata-se de um sistema operacionalizado para a definição do domínio em estudo. Tennis delineou dois eixos e quatro parâmetros de análise baseados na pesquisa de Hjørland, porém aplicáveis para qualquer domínio. Os eixos e parâmetros mencionados abaixo podem ser usados para a operacionalização da definição de um domínio, ou seja, estabelecer parâmetros sobre o domínio:

Tabela 2 – Relação entre Eixos e Parâmetros.

Eixos	Parâmetros
Área de Modulação	Extensão
	Nome
Graus de Especialização	Foco
	Intersecção

Fonte: TENNIS (2003) adaptado pelo autor.

O eixo Áreas de Modulação define parâmetros nos nomes e na extensão do domínio. A extensão do domínio é seu escopo total e responde pelo alcance do domínio. Isso ocorre através da negociação dos termos e de suas definições usados pelos membros do domínio com aqueles usados por analistas de domínio. Em termos práticos, esse eixo reflete a pergunta: como é chamado o domínio (nome) e qual é o seu escopo (extensão)? Ambas as informações são necessárias para definir parâmetros sobre um domínio.

Desta forma, é necessário, neste eixo, dar um nome a extensão. Isso deve ser aparente para o analista de domínio e o leitor da análise de domínio. É um problema de classificação. As Áreas de Modulação, sendo uma declaração explícita do nome e extensão do domínio examinado, indica o que está incluído, o que não está incluído e como o domínio é chamado. Questões sobre a organização do domínio, em função de sua extensão e seu nome serão apresentadas no segundo eixo, Graus de Especialização.

Os Graus de Especialização qualificam e definem a intensão de um domínio. A intensão é a profundidade de um domínio a ser estudado (SMIRAGLIA, 2013) e pode não ser desejável e nem viável descrever um domínio inteiro. O domínio inteiro pode ter um nome e uma extensão que podem ser definidos, mas pode não se prestar facilmente à análise. Desta forma, o domínio deve ser qualificado para que sua extensão diminua e sua intensão, aumente. Conforme exemplificado por Tennis, estudar hinduísmo não é estudar toda a religião. O domínio qualificado é o hinduísmo. O hinduísmo tem um intensão maior, porém uma extensão menor em comparação com a religião. O hinduísmo, como parte da religião, é uma qualificação da religião. Significa mais especificamente, um tipo de religião. O hinduísmo também pode ser qualificado como História ou grupo político qualificado. No

entanto, nem todas as qualificações são facilmente aninhadas. Portanto, para estudar um domínio de maneira cumulativa, a análise de domínio deve definir o domínio e definir sua intenção. Um analista de domínio pode fazer isso descrevendo as Áreas de Modulação e os Graus de Especialização. Os Graus de Especialização são muito familiares para pesquisa em Organização do Conhecimento. Grande parte da pesquisa nesse campo lida com esses tipos de distinções. O primeiro grau de especialização é negativo, ou seja, nenhuma qualificação para o domínio. Um analista de domínio pode achar necessário analisar todo o domínio. Isso, então, deve ser estabelecido como intensão da análise de domínio. Além de todo o domínio, o analista de domínio pode qualificar um domínio com base no foco ou nas interseções.

Um foco, como Grau de Especialização, é um parâmetro usado para qualificar um domínio e, ao fazê-lo, aumenta sua intenção, diminuindo sua extensão. Um foco pode estar, por exemplo, no domínio das comunidades monásticas budistas. As comunidades monásticas budistas, como domínio, são muito diferentes do budismo em geral ou da religião em geral. É mais focado. Com uma Área de Modulação definida, um analista de domínio pode querer encontrar divisões usadas nesse domínio que permitirão qualificar sua análise de domínio. Por exemplo, no estudo acadêmico da religião, há estudiosos que são filósofos do pensamento cristão, ou historiadores da lei islâmica, ou antropólogos do hinduísmo. É concebível que um Foco possa ser restrito a uma pessoa.

O segundo grau de especialização é a interseção. Frequentemente, o que é percebido como um domínio estabelecido se sobrepõe a outro domínio. O resultado pode ser ou não um novo domínio, dependendo do contexto é um novo domínio para alguns, mas não para outros. Isso cria uma tensão entre as partes investidas, os propósitos e as operações do domínio. Essa interseção de domínios renomeia a si mesma, mas isso não ocorre com a mesma frequência e, por diversas vezes, esse cruzamento busca apoio institucional. Os Graus de Especialização oferecem uma maneira da análise de domínio qualificar um domínio. Foco e interseção aumentam a intenção de um domínio e, ao fazer isso, delineiam o que é estudado em uma análise de domínio.

5.2. O Domínio Segurança da Informação

A história da segurança da informação não começou com o avanço do telégrafo, das redes wireless, ou mesmo com advento da Internet. A maior prova de que segurança da informação não é apenas tecnologia é o fato de ela existir em um tempo em que a tecnologia

não era conhecida na forma que vemos hoje. A definição independe de qualquer estágio de desenvolvimento tecnológico, o que significa que pode ser aplicada tanto aos serviços de correio do início do mundo moderno quanto às redes de computadores de hoje.

A segurança dos sistemas de informação engloba toda a infraestrutura, organização, pessoas e componentes que atuam sobre a informação - seja coletando, processando, armazenando, transmitindo, exibindo e disseminando-a – mas sempre objetivando confidencialidade, integridade, disponibilidade dos ativos físicos (construções, equipamentos e pessoas) e ativos de informações (dados e sistemas de informação). Essa definição é independente de qualquer estágio de desenvolvimento tecnológico, o que significa que pode ser aplicada tanto aos serviços de correio do início do mundo moderno quanto às redes de computadores de hoje.

5.2.1. Conceitos Básicos

A área de Segurança da Informação visa mitigar ou reduzir os riscos causados por ameaças aos ativos de informação, estando eles em ambiente tecnológico ou não. No ambiente corporativo, um os objetivos de segurança devem ser estruturados de forma a garantir que os princípios de confidencialidade, integridade e disponibilidade – comumente conhecidos como a tríade CID – sejam suportados por controles projetados para evitar ameaças ou reduzir os riscos de perda, interrupção ou que os dados sejam corrompidos. De acordo com (CHAPPLE; STEWART; GIBSON, 2018; HARRIS; MAYMI, 2016), a tríade CID é definida da seguinte forma:

- **Confidencialidade** – Sujeitos são entidades ativas, que acessam objetos ou informações dentro destas entidades. Pode ser um usuário, um sistema ou um processo que acessa um objeto. O objeto é uma entidade passiva que contém a informação para alguma funcionalidade necessária para uso do sujeito. Pode ser um computador, arquivo, base de dados ou até um campo em uma tabela de uma base de dados. Desta forma, a confidencialidade determina que a informação deve ser acessada apenas pelos sujeitos que têm esse direito. Este conceito é suportado pelos princípios "*Need to know*" (Necessidade de saber) e "*Least Privilege*"

(Privilégio mínimo). Ambos os princípios são fundamentais na segurança da informação e limitam o acesso dos sujeitos apenas ao que é necessário para executar suas ações.

- **Integridade** - É o princípio que delimita que as informações devem ser protegidas contra alterações não autorizadas, sejam estas alterações intencionais ou acidentais. No mundo corporativo, informações armazenadas, em trânsito ou durante o processo de transações devem ser confiáveis e precisas para uma tomada de decisões de negócios. Controles técnicos ou administrativos devem ser implantados para garantir que as informações sejam modificadas através de um processo consistente.

- **Disponibilidade** – Trata-se do princípio que garante que as informações estejam disponíveis e acessíveis aos sujeitos sempre que necessário. As medidas de disponibilidade protegem o acesso oportuno e ininterrupto ao sistema e algumas das ameaças mais fundamentais à disponibilidade são de natureza não maliciosa e incluem falhas de hardware, tempo de inatividade não programado de software e problemas de largura de banda da rede. Ataques maliciosos incluem várias formas de sabotagem com a intenção de causar danos a uma organização, negando aos usuários o acesso ao sistema de informações.

A concepção da relação entre os objetivos de segurança e os conceitos da tríade CID pode ser observado através da figura abaixo:

Figura 6 – Relação entre os objetivos de segurança e a tríade CID.

Fonte: elaborado pelo autor baseado em CHAPPLE; STEWART; GIBSON (2018); HARRIS; MAYMI (2016)

Entretanto, os princípios mencionados nesta tríade são conceitos teóricos. Para alcançar os objetivos de segurança de fato, há a necessidade de materializar esses princípios, de colocá-los em prática. Para tanto, são necessários a implantação de controles, que visam reduzir os riscos a que os objetivos de segurança estão sujeitos. Esses controles são suportados através da integração de outra tríade – Tecnologia, Processos e Pessoas, descritas com maiores detalhes logo abaixo:

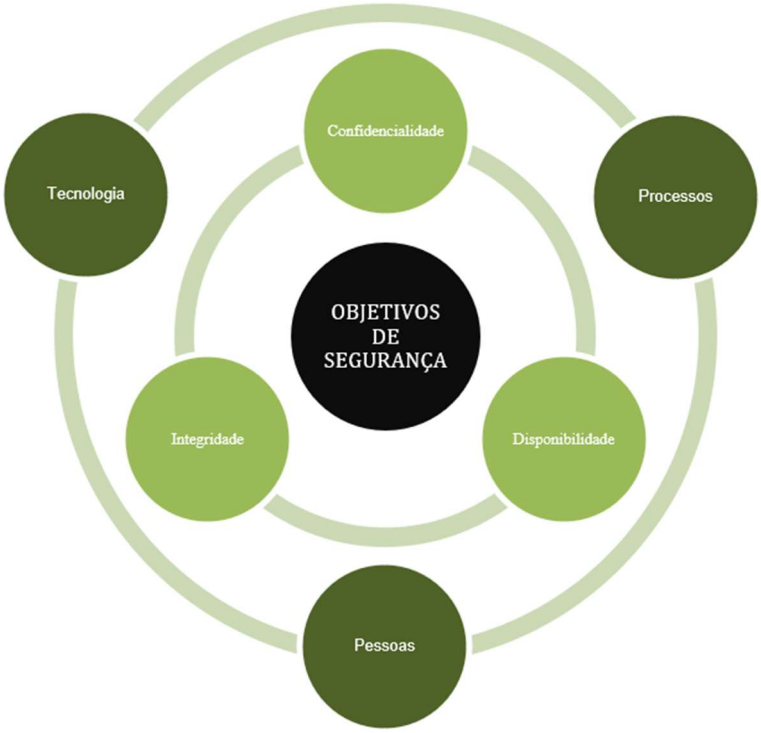
a. **Tecnologias** – São os controles ou ferramentas técnicas implementadas para prevenir ou reduzir o impacto dos riscos cibernéticos.

b. **Processos** – Os processos são cruciais para a implantação de uma estratégia de segurança da informação eficaz. Isso ocorre através da definição de atividades, funções e documentação usadas para mitigar os riscos nos ativos de informação. Os processos também precisam ser revisados continuamente, uma vez que as ameaças cibernéticas mudam rapidamente. É necessário que as documentações se adaptem a elas, refletindo as mudanças.

c. **Pessoas** – São todos os elementos humanos envolvidos no ciclo de vida da informação. Seja na produção, no uso ou, até mesmo, na proteção desta, este elemento pode apresentar alguns dos maiores riscos à segurança da informação.

Nesta tríade, as pessoas, conforme mencionado no tópico de introdução desta pesquisa, é o “elo mais fraco da corrente”. Quanto às tecnologias, é esperado um resultado das máquinas, pois elas executam o seu trabalho desde que devidamente configuradas para isso. Processos também são desenhados para direcionar a ação das pessoas ou das tecnologias. O problema está, justamente, no fator humano, que lida com a tecnologia e que deveria seguir as regras descritas nos processos. Este fator é o elemento que dá imprevisibilidade a todo processo de segurança (SÊMOLA, 2003). De nada adianta tecnologias devidamente implantadas e configuradas, assim como processos que enderecem perfeitamente as instruções para prevenir ou abrandar riscos se o elemento humano não entender a importância de seu papel e, consequentemente, de suas ações em todo esse contexto. Programas de treinamento, educação e conscientização devem ser levados adiante para criar uma forte cultura de segurança da informação de forma a contribuir com a minimização de ameaças. Abaixo, é possível observar como a tríade Tecnologia, Processos e Pessoas se relacionam no processo de segurança da informação com a tríade CID e, por consequência, com os objetivos de segurança:

Figura 7 – Relação da tríade Tecnologia, Processos e Pessoas no processo de SI.



Fonte: elaborado pelo autor baseado em CHAPPLE; STEWART; GIBSON (2018) ; HARRIS; MAYMI (2016)

Desta forma, reforçando o já mencionado, é possível observar que o campo de Segurança da Informação interage de forma natural com a Ciência da Informação.

A informação, para cumprir seu ciclo de vida sob a ótica da Ciência da Informação, precisa ser acessada por quem de direito (não, necessariamente, trata-se do princípio da Confidencialidade, neste caso, pois a informação pode ser pública. Entretanto, deve ser observado que a informação possui um respectivo público-alvo); ter seu conteúdo preciso e confiável (princípio da Integridade) e estar disponível sempre que for necessário ter acesso a ela (princípio da Disponibilidade).

A análise de domínio do campo de Segurança da Informação pode ser estudada por diversos *frameworks*. Um *framework*, dentro do contexto da área de Segurança da Informação, são processos usados para definir políticas e procedimentos na implantação e gerenciamento contínuo de controles de segurança da informação em um ambiente corporativo, podendo endereçar:

1. **Controles** – Desenvolvimento da estratégia e o fornecimento de controles básicos de segurança, avaliação do atual nível técnico de controles e priorização de sua implantação;
2. **Programas** – Avaliação do nível e criação de um programa de segurança abrangente, implantação da comunicação entre as equipes de segurança e a liderança das empresas.
3. **Riscos** – Definição das etapas do processo de avaliação e gerenciamento de riscos e estruturação do programa para gestão de risco.

A utilização de frameworks pode ser obrigatória em alguns tipos de mercados. O *Payment Card Industry Data Security Standard* ou *PCI DSS* [10], por exemplo, é um framework que rege a segurança do setor de cartões de pagamento aplicado às empresas que manuseiam processos de pagamento com cartões de crédito. Este *framework* possui um conjunto de requerimentos e procedimentos que tem como objetivo a proteção das informações pessoais dos titulares de cartão e, consequentemente, reduzir o risco de roubo de dados de cartão ou fraudes cometidas por este meio de pagamento.

[10] https://www.pcisecuritystandards.org/

A família de normas ISO 27000 também fornece recomendações das melhores práticas sobre a gestão de riscos da informação por meio de controles de segurança da informação conhecido e a análise de domínio também pode ser feita à luz deste *framework*. A *International Organization for Standardization* (ISO) é uma organização internacional não governamental independente, associada a 165 organismos de normalização nacionais, dentre elas a Associação Brasileira de Normas Técnicas (ABNT). Segundo a entidade:

> "A ISO / IEC 27001 é amplamente conhecida, fornecendo requisitos para um sistema de gerenciamento de segurança da informação (ISMS), embora haja mais de uma dúzia de padrões na família ISO / IEC 27000. Seu uso permite que organizações de qualquer tipo gerenciem a segurança de ativos, como informações financeiras, propriedade intelectual, detalhes de funcionários ou informações confiadas por terceiros."[11]

Trata-se de uma família de normas bastante extensa e que endereça diversos assuntos, abordando desde diretrizes de avaliação de controles de Segurança da Informação (ISO/IEC TS 27008:2019) e governança de Segurança da informação, segurança cibernética e proteção da privacidade (ISO/IEC 27014:2020) até questões relacionadas à protocolos e estrutura de dados de controle de segurança de aplicativos (ISO/IEC 27034-5:2017), princípios de gerenciamento de incidentes (ISO/IEC 27035-1:2016) e diretrizes para a prontidão da Tecnologia da Informação e Comunicação para a Continuidade dos Negócios (ISO/IEC 27031:2011).[12]

É interessante fazer um recorte especial nos documentos ISO/IEC 24760-1:2019 (*IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*[13]) e ISO/IEC 20889:2018 (*Privacy enhancing data de-identification terminology and classification of techniques*[14]). Ambos abordam a terminologia e os conceitos, respectivamente, para o *framework* específico de gerenciamento de identidade e para a terminologia de "desidentificação" de dados para a privacidade e classificação de técnicas. O primeiro atende à necessidade de implantar uma forma eficiente e eficaz de sistemas que tomem decisões baseadas em identidade e faz a especificação de conceitos fundamentais e estruturas operacionais de gerenciamento de identidade, que servem para

[11] https://www.iso.org/isoiec-27001-information-security.html
[12] https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0
[13] https://www.iso.org/standard/77582.html
[14] https://www.iso.org/standard/69373.html

caracterizar indivíduos, organizações ou componentes de tecnologia da informação que operam em nome de indivíduos ou organizações com o objetivo de realizar o gerenciamento de sistemas de informação para que os sistemas de informação possam atender às obrigações comerciais, contratuais, regulatórias e legais. Já o segundo documento fornece uma visão geral dos principais conceitos relacionados à "desidentificação" de dados – processo de remoção da associação entre um conjunto de atributos ou característica de identificação e o principal de dados (entidade, como uma pessoa, uma organização, um dispositivo ou um software aplicativo) - e estabelece uma terminologia padrão e uma descrição da operação e propriedades de uma variedade de técnicas e métodos de "desidentificação"

A análise do domínio de segurança da informação também pode ser estudada sob a perspectiva das bases de conhecimento das diversas certificações profissionais internacionais disponíveis. As certificações em Segurança da Informação visam comprovar as habilidades desta área de conhecimento. As certificações podem ser classificadas neutras (*vendor-neutral*), que são aquelas que não estão diretamente associadas a fornecedores ou fabricantes de soluções tecnológicas. Estas certificações, administradas por entidades, associações ou organizações e afins, tendem a desenvolver uma base de conhecimentos e habilidades amplamente aplicáveis. Na tabela abaixo estão elencados alguns exemplos de certificações neutras e suas respectivas entidades:

Tabela 3 – Exemplos de certificações neutras elaborado pelo autor.

CERTIFICAÇÃO	ENTIDADE
Certified Information Systems Security Professional (CISSP)[15]	*International Information Systems Security Certification Consortium* (ISC)²
Certified Information Security Manager (CISM)[16]	*Information Systems Audit and Control Association* (ISACA)
Security+[17]	*Computing Technology Industry Association* (*CompTIA*)

Fonte: elaborado pelo autor.

Em contrapartida, existem as certificações não neutras, desenvolvidas por fabricantes de plataformas e soluções tecnológicas baseadas em *software* ou *hardware*. Estas se concentram em demonstrar o conhecimento em uma ferramenta técnica específica. A

[15] https://www.isc2.org/Certifications/CISSP
[16] https://www.isaca.org/credentialing/cism
[17] https://www.comptia.org/pt/certificacoes/security

tabela abaixo elenca alguns exemplos destas certificações, que tem como objetivo testar os conhecimentos e habilidades de implantação, suporte, operação e administração das soluções criadas por seus fabricantes:

Tabela 4 - Exemplos de certificações de fabricantes elaborado pelo autor.

CERTIFICAÇÃO	FABRICANTE
Cisco Certified Network Associate (CCNA)[18]	Cisco
Microsoft Certified Professional (MCP)[19]	Microsoft
Check Point Certified Expert (CCSE)[20]	Check Point

Fonte: elaborado pelo autor.

Por conta da grande quantidade de *frameworks* e certificações profissionais disponíveis no mercado, é necessário delimitar o escopo da análise deste domínio de conhecimento. Desta forma, a análise de domínio, da perspectiva dos *frameworks*, será baseada no *framework* desenvolvido pelo *National Institute of Standards and Technology* (NIST), que um dos mais conhecidos e utilizados para a adoção de padrões de segurança cibernética nos mais diversos mercados. Da perspectiva das certificações profissionais, o estudo será feito com base na certificação CISSP, que é uma das certificações mais conhecidas e cobiçadas pelos profissionais de segurança da informação, mantida pela organização (ISC)².

5.2.2. *National Institute of Standards and Technology* (NIST)

O NIST ou *National Institute of Standards and Technology* foi fundado em 1901 e faz parte do Departamento de Comércio dos Estados Unidos[21]. O NIST reconheceu que a segurança nacional e econômica dos Estados Unidos depende da confiabilidade de todas as infraestruturas consideradas críticas. Desta forma, o governo emitiu a Ordem Executiva n°

[18] https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html
[19] https://www.microsoft.com/pt-br/learning/microsoft-certifications-for-students.aspx
[20] https://training-certifications.checkpoint.com/#/

[21] https://www.nist.gov/about-nist

13636, chamada *Improving Critical Infrastructure Cybersecurity*, em fevereiro de 2013[22]. A referida ordem instruía o NIST a trabalhar com as partes interessadas para desenvolver um programa com base em padrões, diretrizes e práticas existentes - para reduzir os riscos cibernéticos em infraestruturas críticas. O *Cybersecurity Enhancement Act* de 2014[23] reforçou a já referida Ordem Executiva. A abordagem priorizada, flexível, repetível e econômica da Estrutura ajuda os proprietários e operadores de infraestrutura crítica a gerenciar os riscos relacionados à segurança cibernética.

Neste *framework*, o termo *Cybersecurity* ou Segurança Cibernética é amplamente usado e com a seguinte definição:

> *Prevenção de danos, proteção e restauração de computadores, sistemas de comunicações eletrônicas, serviços de comunicações eletrônicas, comunicação com fio e comunicação eletrônica, incluindo as informações neles contidas, para garantir sua disponibilidade, integridade, autenticação, confidencialidade e não-repúdio.* (tradução nossa).

Apesar de o termo Segurança Cibernética estar com uma definição enviesada para segurança tecnológica, o NIST possui definições diferentes em seu glossário, algumas mais genéricas e outras mais específicas[24]. Entretanto, é possível observar a diferença entre os termos Segurança Cibernética e Segurança da Informação, mostrada abaixo e que possui uma definição mais ampla:

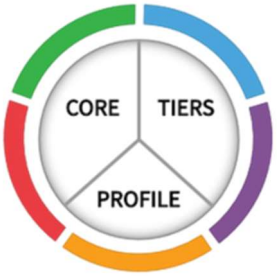
> A proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer confidencialidade, integridade e disponibilidade. (tradução nossa).

O *Framework* de Segurança Cibernética (*Cybersecurity Framework*) foi criado como uma forma de orientação para que as organizações gerenciem e reduzam seu risco de segurança cibernética. Foi projetado também para promover as comunicações de gerenciamento de risco e segurança cibernética entre as partes interessadas organizacionais

[22] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[23] https://www.govinfo.gov/content/pkg/COMPS-12455/pdf/COMPS-12455.pdf
[24] https://csrc.nist.gov/glossary/term/cybersecurity

internas e externas[25]. A estrutura de segurança cibernética consiste em três componentes principais:

Figura 8 – Principais componentes do NIST Cybersecurity Framework.



Fonte: site do NIST Cybersecurity Framework.

- **Núcleo *(Core)*** – Fornece um conjunto de atividades e resultados de segurança cibernética desejados, usando uma linguagem comum de fácil compreensão e orientando as organizações no gerenciamento e redução de seus riscos de segurança de uma forma que complementa os processos existentes de gerenciamento de riscos e segurança de uma organização. O componente *Core* é dividido em três partes - Funções, Categorias e Subcategorias. As **Funções** (*Functions*), por sua vez, endereçam cinco tópicos de alto nível - Identificar, Proteger, Detectar, Responder e Recuperar. Cada uma dessas funções é desmembrada em 23 **Categorias**, conforme mostrado na figura abaixo.

  Figura 9 – Lista de categorias por funções.

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

  Fonte: site do NIST Cybersecurity Framework.

[25] https://www.nist.gov/cyberframework/new-framework

As **Funções** são o nível mais alto de abstração incluído no Framework e atuam como a base de organização dos outros elementos. São divididas em cinco níveis[26]:

- **Identificar** (*Identify*) – Auxiliam no desenvolvimento do entendimento organizacional para o gerenciamento de riscos de segurança cibernética para sistemas, pessoas, ativos, dados e recursos e a compreender o contexto de negócios, os recursos que suportam funções críticas e os riscos relacionados à segurança cibernética permite que uma organização concentre e priorize seus esforços, de acordo com sua estratégia de gerenciamento de risco e necessidades de negócios.
- **Proteger** (*Protect*) – Descreve as contramedidas adequadas para garantir a entrega de serviços de infraestrutura crítica e suporta a capacidade de limitar ou conter o impacto de um possível evento de segurança cibernética.
- **Detectar** (*Detect*) – Define as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética e permite a descoberta oportuna de eventos de segurança cibernética.
- **Responder** (*Respond*) – Inclui atividades apropriadas para agir em relação a um incidente de segurança detectado e suporta a capacidade de conter o impacto de um potencial incidente de segurança cibernética.
- **Recuperar** (*Recover*) – Identifica atividades apropriadas para manter planos de resiliência e para restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética. Oferece suporte à recuperação para que as operações voltem ao normal e, com isso, reduzir o impacto de um incidente de segurança cibernética.

As **Categorias** (*Categories*) são tópicos relacionados à segurança cibernética foram desenhadas para cobrir todos os objetivos de segurança cibernética de uma organização, abrangendo com amplitude tópicos cibernéticos, físicos e pessoais, mas sempre objetivando os resultados de negócios.

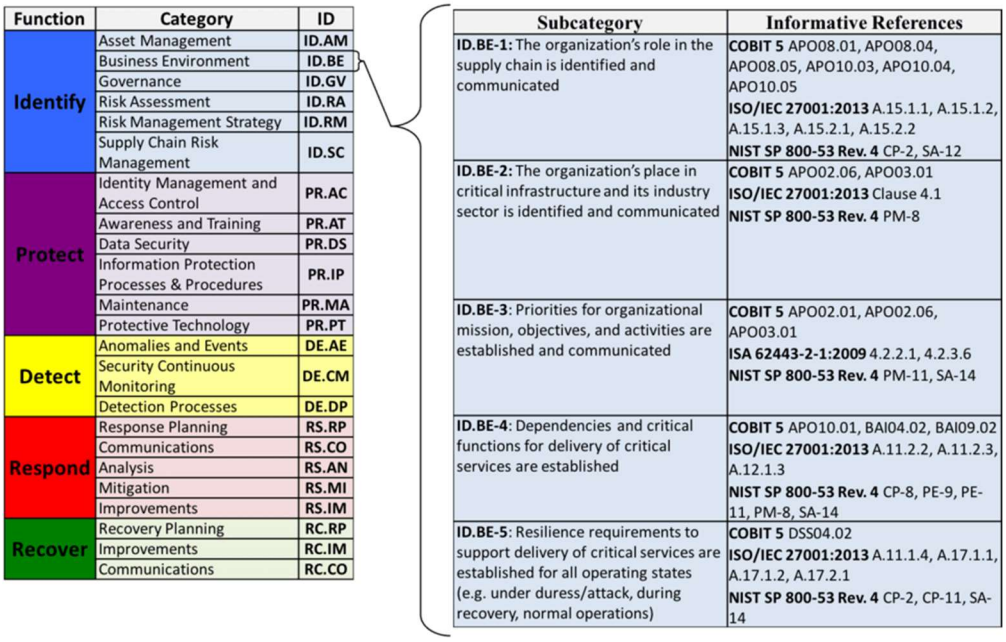
Por conseguinte, as **Subcategorias** são o nível mais profundo de abstração do componente *Core*. Consta de 108 subcategorias, que são declarações baseadas em resultados que fornecem considerações para a criação ou melhoria de um programa

[26] https://www.nist.gov/cyberframework/online-learning/five-functions

de segurança cibernética. É importante ressaltar que este *framework* não determina como uma organização deve atingir esses resultados, pois permite que as implantações dos controles baseados em risco possam ser personalizadas de acordo com as necessidades da organização.

Por fim, existem as **Referências Informativas** (*Informative References*), que fazem parte do componente Core e visam fornecer referências técnicas detalhadas para a implantação dos controles. Em termos práticos, trata-se de padrões, diretrizes e práticas comuns entre os setores de infraestrutura crítica que ilustram um método para alcançar os resultados associados a cada subcategoria, conforme mostrado na figura abaixo. As referências são apenas ilustrativas e podem ser excedidas para alcançar os resultados desejados, conforme exemplificado na figura 10.

Figura 10 – Desmembramento das Categorias em Subcategorias e referencias informativos.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Fonte: site do NIST *Cybersecurity Framework*.

- **Níveis de Implantação *(Implementation Tiers)*** – Esse componente auxilia as organizações, fornecendo um contexto sobre como lidar com o gerenciamento de riscos de segurança e orientam em como considerar o nível de rigor apropriado em seu programa de segurança. Pode atuar como uma ferramenta de comunicação para discutir o apetite pelo risco, prioridade e orçamento para a implantação. Os níveis descrevem um grau crescente de rigor e sofisticação nas práticas de gerenciamento

de risco de segurança cibernética e auxiliam a determinar até que ponto o gerenciamento de riscos de segurança cibernética é informado pelas necessidades de negócios e é integrado às práticas gerais de gerenciamento de riscos de uma organização, sendo divididos em quatro:

- **Nível 1** – Parcial
- **Nível 2** – Risco Informado
- **Nível 3** – Repetível
- **Nível 4** – Adaptativo

As considerações de gerenciamento de riscos incluem muitos aspectos da segurança cibernética, incluindo o grau em que as questões de privacidade e liberdades civis são integradas ao gerenciamento de uma organização. O processo de seleção de nível considera as práticas atuais de gerenciamento de riscos de uma organização, ambiente de ameaças, requisitos legais e regulatórios, práticas de compartilhamento de informações, missão e objetivos de negócios, requisitos de segurança cibernética da cadeia de suprimentos e restrições organizacionais. As organizações devem determinar o nível desejado, garantindo que o nível selecionado atenda às metas da organização seja viável para a sua implantação e que reduza o risco de segurança cibernética para os ativos críticos e recursos para níveis aceitáveis. Embora as organizações identificadas como Nível 1 (Parcial) sejam incentivadas a considerar a mudança para o Nível 2 ou superior, os níveis não representam níveis de maturidade. As camadas destinam-se a apoiar a tomada de decisão organizacional sobre como gerenciar o risco de segurança cibernética, bem como elencar as áreas de maior prioridade para receber recursos adicionais. A progressão para níveis mais altos é incentivada quando uma análise de custo-benefício indica uma redução viável e econômica do risco de segurança cibernética. A implantação bem-sucedida deste *framework* é baseada nos resultados obtidos na descrição do Perfil da organização e não através do que os níveis determinam. Obviamente, a designação de um determinado nível afeta os Perfis do *framework*. A recomendação dos níveis pelos executivos da organização, definirá como o risco de segurança cibernética será gerenciado dentro da organização e deve influenciar a priorização dentro de um perfil alvo. Abaixo, está uma tabela contendo as definições detalhadas para cada nível:

Tabela 5- Definições por nível de risco extraído do site do NIST[27].

	Nível 1: Parcial	Nível 2: Risco Informado	Nível 3: Repetível	Nível 4: Adaptativo
Gerenciamento de Risco	A gestão de risco de segurança cibernética não está formalizada e as práticas são feitas sob demanda ou de maneira reativa. A priorização dos riscos pode não ser endereçada nos objetivos de riscos da organização.	As práticas de gerenciamento de risco são aprovadas, mas não, necessariamente, implantadas de maneira regular pela organização. A priorização das atividades de segurança cibernética é informada diretamente pelos objetivos de risco da organização	As práticas de gestão de risco de segurança cibernética da são formalmente aprovadas e expressas em sua política. As práticas são atualizadas regularmente com base nas mudanças dos objetivos de negócios e nas mudanças no cenário de ameaças e tecnologia	Práticas baseadas em atividades anteriores e atuais, melhoria contínua, rápida adaptação aos cenários de ameaças e tecnologia e respostas de maneira efetiva.
Risco Integrado	A gestão de risco de segurança cibernética é limitada e o processo é aplicado de maneira irregular. A organização pode não ter processos que permitam que as informações de segurança cibernética sejam compartilhadas dentro da organização.	Possui conhecimento sobre risco de segurança cibernética, mas uma abordagem ampla não foi estabelecida. As informações são compartilhadas de maneira informal. Segurança cibernética é abordado nos objetivos da organização, mas não em todos os níveis da organização.	Possui uma abordagem para gerenciar os riscos de segurança cibernética. Documentos relacionados ao processo de gestão de riscos são definidos, implantados e revisados. Métodos consistentes e equipes habilitadas estão disponíveis para responder de forma eficaz às mudanças no risco. Há monitoração consistente dos riscos. Existe comunicação entre executivos de forma a garantir que a segurança cibernética esteja em todas as linhas de negócio.	Relação entre risco de segurança cibernética e organizacional é compreendido, considerado e incorporado na cultura da empresa ainda que a missão e os objetivos da empresa mudem ao longo do tempo.
Participação Externa	A organização não entende sua função no ecossistema mais amplo com respeito a	Entende seu papel no ecossistema maior quanto a sua	Entende seu papel, dependências e dependentes no	Entende que faz parte de um ecossistema maior e contribui

[27] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

	suas dependências ou dependentes. A organização não colabora, não recebe e nem compartilha informações com outras entidades.	dependência ou seus dependentes no processo (não a ambos). Colabora e recebe algumas informações de outras entidades e gera algumas de suas próprias informações, mas não compartilha. Está ciente dos riscos de segurança cibernética na cadeia de suprimentos associados aos produtos e serviços que fornece e usa, mas não age de forma consistente ou formal sobre esses riscos.	ecossistema mais amplo e pode contribuir para o entendimento mais amplo da comunidade sobre os riscos, trocando informações regularmente com outras entidades e complementando as informações geradas internamente. Está ciente dos riscos de segurança cibernética associada à cadeia de fornecimento de produtos e serviços. Atua formalmente sobre esses riscos, incluindo mecanismos de proteção.	compartilhando informações relacionadas aos riscos de segurança cibernética com entidades internas e externas de maneira proativa. Usa mecanismos de proteção formais e informais para desenvolver e manter relacionamentos fortes da cadeia de abastecimento

Fonte: site do NIST[28].

- **Perfis (*Profiles*)** – Trata-se do alinhamento das Funções, Categorias e Subcategorias com os requisitos de negócios, tolerância ao risco e recursos da organização em relação aos resultados desejados do componente *Core*. Este componente é usado principalmente para identificar e priorizar oportunidades para melhorar a segurança cibernética em uma organização[29]. Um perfil permite que as organizações estabeleçam um roteiro para reduzir o risco de segurança cibernética de forma que esteja bem alinhado com a organização e o setor objetivos, consideram os requisitos legais e regulatórios, as melhores práticas do setor e reflete as prioridades de gestão de risco. Devido à complexidade de muitas organizações, vários perfis de risco podem ser adotados, alinhados aos componentes específicos e reconhecendo necessidades individuais. Os perfis podem ser adotados para descrever não somente o atual estado das atividades específicas de segurança cibernética - os resultados da segurança cibernética que estão sendo alcançados, mas também um estado de gerenciamento de risco de segurança cibernética desejado no futuro. Uma característica inerente a este

[28] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[29] https://www.nist.gov/cyberframework/new-framework

componente é o fato de os perfis não oferecer suporte aos requisitos ou missão de negócios, tampouco prescreve modelos, que permitam flexibilidade na implantação. Entretanto, suportam o processo de comunicação dos riscos dentro da organização e entre organizações. O plano de ação para preencher as lacunas de uma determinada categoria ou subcategoria, impulsionado pelas necessidades de negócios da organização e nos processos de gestão de risco, pode contribuir na elaboração de um roteiro e na priorização das ações de mitigação destas lacunas no gerenciamento de risco de segurança cibernética. Esta abordagem baseada em risco permite que uma organização avalie os recursos humanos, financeiros e outros que sejam necessários para atingir as metas de segurança cibernética de maneira econômica e priorizada.

É importante ressaltar que o NIST *framework* serve como um modelo internacional de cooperação internacional no fortalecimento da segurança cibernética e ajuda as organizações de diversos setores a lidar com as questões de segurança cibernética em sua infraestrutura crítica. Há diversas formas de usar e personalizar as práticas descritas no *framework* e, com isso, desenvolver a força de trabalho e as atividades de evolução do gerenciamento de risco de segurança cibernética para infraestrutura crítica e, desta forma, priorizar os investimentos. Não há regras para o uso do *framework* e a decisão sobre como implantá-lo é por conta da organização.

Os requisitos e necessidades de segurança cibernética mudam ao longo do tempo e o mercado fornece informações que retroalimentam suas implantações. Isso faz com que o *framework* seja um processo vivo e que necessita de atualização constante. Uma vez implantado o *framework* em uma organização, um processo cíclico de melhoria contínua tal qual enunciado através do ciclo de Deming ou PDCA (*Plan, Do, Check* e *Act*)[30], executado de forma a atualizar e melhorar a implantação do *framework*. A utilização voluntária e eficaz das melhores práticas deste framework e o compartilhamento destas informações são os próximos passos para melhorar a segurança cibernética da infraestrutura crítica e, consequentemente, aumentando a postura de segurança cibernética da infraestrutura crítica da nação e da economia e da sociedade em geral.

[30] https://us-cert.cisa.gov/bsi/articles/best-practices/deployment-and-operations/plan-do-check-act

5.2.3. Certified Information Systems Security Professional (CISSP)

O (ISC)², um acrônimo para *International Information System Security Certification Consortium*, é uma associação internacional sem fins lucrativos e especializada em treinamento e certificações para profissionais de segurança da informação. De todas as certificações oferecidas por esta instituição, a mais conhecida é a CISSP (*Certified Information Systems Security Professional*). Essa certificação um possui um CBK, acrônimo para *Common Body of Knowledge* ou Corpo de Conhecimento Comum, que é uma coleção de tópicos relevantes no campo de Segurança da Informação, estabelecendo uma estrutura comum de termos e princípios deste campo e que permite discussões pertinentes através da padronização do entendimento, taxonomia e léxico. Para o (ISC)²:

> "Um Corpo de Conhecimento Comum refere-se a uma síntese desenvolvida para delimitar o que um profissional competente em seu respectivo campo de atuação deva saber, incluindo as habilidades, técnicas e práticas que são rotineiramente empregadas. O CBK composto pelo ISC² é uma coleção de tópicos relevantes para profissionais de segurança cibernética em todo o mundo. Estabelece uma estrutura comum de termos e princípios de segurança da informação que permite que profissionais de segurança cibernética e TI / TIC em todo o mundo discutam, debatam e resolvam questões relacionadas à profissão com um entendimento, taxonomia e léxico comuns. (ISC)² foi estabelecido, em parte, para agregar, padronizar e manter CBK para profissionais de segurança em todo o mundo. Os domínios das credenciais do (ISC)² são extraídos de vários tópicos do CBK do (ISC)², que são usados para avaliar o nível de domínio de um candidato nos aspectos mais críticos da segurança da informação." [31] (tradução e adaptação nossa).

O (ISC)² define e organiza os domínios CISSP com base em sua pesquisa de mercado de como funciona a segurança da informação no mercado. Os tópicos que compõem o currículo desta certificação são denominados domínios. Desde 15/04/2018[32], estes domínios passaram a ser elencados da seguinte forma:

- Gerenciamento de Riscos e Segurança
- Segurança de Ativos

[31] (ISC)² CBK | Common Body of Knowledge - https://www.isc2.org/Certifications/CBK
[32] CISSP Exam Changes Effective April 2018 - https://blog.netwrix.com/2018/07/17/cissp-exam-changes-effective-april-2018-what-you-need-to-know/

- Arquitetura e Engenharia de Segurança
- Segurança de Redes e Comunicação
- Gestão de Identidade e Acesso
- Avaliação e Testes em Segurança
- Segurança em Operações
- Segurança no Desenvolvimento de Software

O (ISC)² possui literaturas oficiais preparatórias para as suas certificações. No caso da certificação CISSP, a entidade possui um guia oficial onde é possível:

- Independentemente do processo de certificação, obter um direcionamento sobre os assuntos que precisam ser estudados para se tornar um profissional de segurança da informação;
- Ter uma fonte de informação confiável sobre os tópicos que serão abordados nos oito domínios cobertos pelo exame;
- Conseguir informações sobre o processo de obtenção da certificação CISSP.

Entretanto, este capítulo não tem o objetivo de elencar as etapas que um possível candidato tenha que galgar ou explicar os pré-requisitos necessários para ter êxito no processo de certificação, mas abordar os tópicos relevantes que cobrem, não somente a certificação, mas o domínio Segurança da Informação, na ótica da Ciência da Informação, conforme delineado pelo (ISC)² e descrito por CHAPPLE; STEWART; GIBSON, (2018) e HARRIS; MAYMI (2016). É importante observar que o próprio termo “domínio” pode ser utilizado para designar a área de Segurança da Informação de forma ampla e como um todo, sob a perspectiva da Ciência da Informação e material para a análise de domínio, mas também delimita um tópico do corpo de conhecimento comum do (ISC)². Doravante, de forma a evitar a sobreposição de conceitos, a área de Segurança da Informação será tratada como “domínio” de conhecimento a ser estudado e os” domínios”, que fazem parte do corpo de conhecimento do (ISC)², serão designados como “subdomínios”, a saber:

- **Subdomínio 1 - Gerenciamento de Riscos e Segurança**

O domínio “Gerenciamento de Segurança e Risco” aborda os conceitos, princípios, frameworks, políticas e padrões usados para estabelecer critérios para a proteção de ativos de informação e para avaliar a eficácia dessa proteção. Inclui questões de governança, comportamento organizacional e conscientização em segurança. O gerenciamento de segurança de informação estabelece a base de um programa de segurança abrangente e proativo para garantir a proteção dos ativos de informações de uma organização e, para isso, é necessário compreender a conexão entre Tecnologia da Informação e os objetivos de negócio, visto que, atualmente, os ambientes de sistemas são altamente interconectados e interdependentes.

Os departamentos de segurança da informação, por sua vez, devem comunicar os riscos, que podem ser aceitos pela organização frente aos controles de segurança implantados e atuar continuamente para aprimorar estes controles dentro de um parâmetro aceitável de custo-benefício, para minimizar cada vez mais os riscos para os ativos de informação. Estes controles necessários para proteger adequadamente a confidencialidade, integridade e disponibilidade dos ativos de informação podem ser de ordem administrativa, técnica e física e são manifestados por meio de políticas, procedimentos, padrões, baselines e diretrizes.

As práticas de gestão de segurança da informação podem incluir ferramentas para avaliação e análise de riscos, classificação de informações e conscientização em segurança. Os ativos de informações são classificados e, por meio da avaliação de risco, as ameaças e vulnerabilidades relacionadas a esses ativos são categorizadas e as contramedidas adequadas para mitigar o risco de comprometimento da informação podem ser identificadas e priorizadas e, desta forma, minimizar a perda de ativos de informações devido a eventos indesejáveis por meio da identificação, medição e controle, abrangendo a revisão geral de segurança, análise de risco, seleção e avaliação de salvaguardas, análise de custo-benefício, decisão de gerenciamento e identificação e implantação de salvaguardas, junto com a revisão contínua de eficácia.

A gestão de risco fornece um mecanismo para a organização garantir que a gestão executiva conheça os riscos atuais e que decisões informadas possam ser tomadas para usar um dos princípios de gestão de risco - prevenção de risco, transferência de risco, mitigação de risco ou aceitação de risco - todos descritos adiante em mais detalhes. O gerenciamento de segurança está preocupado com os requisitos

regulatórios, de clientes, funcionários e parceiros de negócios para gerenciar dados conforme fluem entre os vários processos de negócio para oferecer suporte ao processamento e uso comercial das informações. A confidencialidade, integridade e disponibilidade das informações devem ser mantidas durante todo o processo.

O Plano de Continuidade de Negócios (do inglês *Business Continuity Planning* ou BCP) e o Plano de Recuperação de Desastres (do inglês *Disaster Recovery Planning* ou DRP) abordam a preparação, os processos e as práticas necessárias para garantir a preservação da organização em face de grandes interrupções das operações normais da organização. O BCP e o DRP envolvem a identificação, seleção, implantação, testes e atualização de processos e ações específicas necessárias para proteger os processos críticos da organização contra os efeitos de grandes interrupções dos sistemas e da rede de dados e para garantir a restauração oportuna das operações da organização caso ocorra interrupções significativas nos processos de negócio. O processo de construção de um programa de continuidade de negócios discute a evolução de questões regulatórias que influenciam ou que exijam que as organizações criem programas que garantam a continuidade de seus processos de negócio. Discute a inter-relação entre segurança da informação e continuidade de negócios com outras áreas de gestão de risco como segurança física, gestão de fornecedores, auditoria interna, gestão de riscos financeiros, gestão de riscos operacionais e conformidade com questões regulatórias.

Para este subdomínio, uma vez que ele trata de assuntos estratégicos segurança da informação, é importante ressaltar as questões relacionadas à educação, treinamento, conscientização e as formas de proteção do fator humano, visto que pessoas é algo crucial dentro deste processo.

As políticas de segurança definem a estratégia de uma empresa no que tange os objetivos de segurança da informação. A conscientização tem um papel importante para estabelecer e homogeneizar a compreensão da importância e como essas regras devem ser cumpridas dentro da organização (CHAPPLE; STEWART; GIBSON, 2018; HARRIS; MAYMI, 2016; SÊMOLA, 2003).

Uma vez que estas políticas de segurança da informação estejam adequadamente implantadas e que, de fato, reflitam as necessidades de negócios baseadas nos riscos identificados, é necessário criar um processo cíclico para manter os usuários informados sobre os procedimentos que devem ser seguidas e suas

respectivas responsabilidades em todo esse processo e estabelecer formas para monitorar este processo.

Estudos já mencionados na introdução têm mostrado que a grande maioria dos ataques tem tirado proveito das vulnerabilidades do fator humano. Isso revela que grande parte dos atacantes não tem mais interesse em atacar as ferramentas técnicas implantadas pelas empresas, pois estes controles técnicos estão cada vez mais sofisticados. As companhias, por sua vez, têm aumentado os investimentos em soluções técnicas para manter seu perímetro protegido e isso torna os ataques às soluções técnicas algo não muito atrativo, pois é necessário gastar tempo para obter informações das vulnerabilidades e, consequentemente, conhecimento técnico suficiente para explorá-las. Desta forma, os invasores agora estão se voltando para ataques direcionados, focados em engenharia social (GARDNER, THOMAS; 2014).

Conforme já mencionado, o fator humano é considerado o elo mais fraco da segurança da informação. As pessoas querem ser úteis, querem fazer um bom trabalho ou executar um bom atendimento ao cliente para seus colegas de trabalho, clientes e fornecedores e, com isso, suscetíveis aos ataques de engenharia social. SCHNEIER (2004) elencou seis aspectos dos problemas gerados pelo fator humano:

- **Como as pessoas entendem os riscos** – Pessoas não sabem analisar riscos e não tomam decisões inteligentes ao lidar com isso.
- **Como as pessoas lidam com algo que ocorre raramente** – Pessoas tendem a ignorar situações que ocorrem raramente. Quando realmente é necessário tomar uma ação, não sabem o que fazer.
- **O problema e o perigo das pessoas confiarem nas tecnologias** – Pessoas tendem a acreditar que soluções tecnológicas podem mantê-las seguras, independentemente de suas ações.
- **Não fazer perguntas para a tomada de decisões inteligentes** – Pessoas tendem a tomar decisões sem levantar todos os fatores relacionados.
- **O perigo das ameaças internas** – Recursos humanos que trabalham nas companhias podem ser descuidados, negligentes e mal-intencionados.
- **Engenharia Social** – Pessoas costumam ser prestativas e fáceis de enganar.

Dos aspectos relacionados aos problemas do fator humano, deve ser dada uma atenção especial deve ser tomada ao que menciona as ameaças internas. Uma ameaça interna é um risco à segurança que está dentro da organização visada. Trata-se de funcionários, colaboradores e usuários internos confiáveis que têm acesso a dados e sistemas sensíveis. Podem ser também consultores, ex-funcionários, parceiros de negócios ou, até mesmo, membros do conselho de administração da companhia. As ameaças internas podem ser classificadas da seguinte forma:

- **Descuidado** – Aquele que, por descuido ou acidente, acaba gerando uma brecha ou causando um incidente de segurança.
- **Negligente** – Aquele que, intencionalmente, ignora a política e as regras, mas não age de forma maliciosa.
- **Malicioso** – Aquele que, intencionalmente, age querendo causar danos e prejuízos.

Uma pesquisa conduzida em 2019 pela empresa de tecnologia Fortinet indica que 68% das organizações confirmaram que os ataques causados por ameaças internas se tornaram mais frequentes. O documento também mostra que 38% e 21% das empresas entrevistadas indicam que os usuários descuidados são vulneráveis aos ataques de *Phishing* e *Spear Phishing* (ataques direcionados), respectivamente (FORTINET, 2019). Isso indica que mais da metade das empresas entrevistadas consideram seus usuários suscetíveis a ataques de engenharia social.

A única defesa conhecida para ataques de engenharia social é um programa de conscientização de segurança eficaz. Conforme mencionado por GARDNER e THOMAS (2014) e HARRIS e MAYMI (2016) um programa adequado deve ser ou ter:

- **Cíclico** – As mensagens importantes devem ser repetidas e em diversos formatos.
- **Direcionado a todos os usuários** – As mensagens devem ser alcançar todos os usuários com mensagens simples e com linguagem acessível a todos os públicos.
- **Sob medida** – As mensagens devem ser personalizadas para grupos específicos quando necessário.
- **Suporte da alta gestão** – Os executivos da companhia devem alocar recursos e reforçar o engajamento de todos no programa.

De acordo com Ferreira (1999, apud BESSA, 2011, p. 14), aprendizado é definido como:

> "Ato ou efeito de aprender; tomar conhecimento de; reter na memória mediante o estudo, a observação, a observação ou a experiência; tornar-se apto ou capaz de alguma coisa em consequência de estudo".

De forma adicional ao processo de aprendizagem, é necessário também elencar alguns elementos que possuem contribuição fundamental neste processo, tais como: a memória, a atenção, o interesse e a inteligência. Adicionalmente as capacidades intelectuais e as habilidades cognitivas, o processo de aprendizagem envolve também relações sociais que a pessoa estabelece ao longo da vida e os conhecimentos prévios. Diversas teorias pedagógicas foram desenvolvidas para explicar o processo de aprendizagem, porém não serão abordadas, visto que fogem do escopo desta pesquisa (BESSA, 2011).

Nas corporações ou onde quer que um programa de conscientização em segurança da informação precisa ser aplicado, ocorre da mesma semelhante. Devem ser consideradas as ações que serão tomadas devem ser cíclicas e o público-alvo das ações de conscientização.

Programas de conscientização devem ser criados, em linhas gerais, para três tipos de públicos-alvo:

- Funcionários Executivos;
- Funcionários relacionados a atividades técnicas ou especificas;
- Funcionários em geral.

Um programa de conscientização e treinamento é fundamental na medida em que é o veículo de disseminação das informações de que os usuários, inclusive os gestores, precisam para realizar seu trabalho. No caso de um programa de segurança de TI, é o veículo a ser usado para comunicar os requisitos de segurança em toda a empresa. Um programa eficaz de conscientização e treinamento de segurança de TI explica as regras de comportamento adequadas para o uso dos sistemas e informações de TI. O programa comunica as políticas e procedimentos de segurança de TI que

precisam ser seguidos. Isso deve preceder e estabelecer a base para quaisquer sanções impostas devido ao descumprimento. Os usuários primeiro devem ser informados sobre as expectativas. A responsabilidade deve ser derivada de uma força de trabalho totalmente informada, bem treinada e consciente. A tabela abaixo mostra a distinção entre os 3 níveis:

Tabela 6 – Diferença entre conscientização, treinamento e educação

	CONSCIENTIZAÇÃO	TREINAMENTO	EDUCAÇÃO
Característica	O que	Como	Por que
Nível	Informação	Conhecimento	Discernimento
Objetivo de aprendizagem	Reconhecimento e retenção	Habilidade	Entendimento
Exemplo de métodos de ensino	**Mídia** Vídeos, boletins informativos, pôsteres, *Computer-Based Tests* (CBT), simulações de engenharia social	**Instrução Prática** Apresentações e demonstrações, Estudos de casos, Exercícios práticos	**Instrução Teórica** Seminários e discussões, Estudos e leitura, Pesquisa
Medida de teste	Questões de múltipla escolha ou de "Verdadeiro ou Falso"	Aplicação da aprendizagem através de reconhecimento e resolução de problemas	Monografias, dissertações e teses
Tempo de impacto	Curto prazo	Médio prazo	Longo prazo

Fonte: documento NIST SP800-50[33] adaptado pelo autor.

A alta direção de uma companhia é responsável em última instancia pela proteção dos ativos da organização. Além disso, possuem os recursos e a autoridade necessária para assegurar que as regras e políticas de segurança sejam devidamente implantadas e seguidas. Com isso, um programa de segurança da informação deve usar a abordagem Top-Down, o que significa que o suporte e a direção do programa devem vir de cima para baixo, ou seja, deve partir da alta direção da companhia para todos os níveis hierárquicos que estão abaixo. A abordagem Top-Down deixa claro que as todas as pessoas são responsáveis pela proteção dos ativos protegidos pelo programa de segurança (HARRIS; MAYMI, 2016).

[33] https://csrc.nist.gov/publications/detail/sp/800-50/final

O programa de conscientização, como parte de um programa de segurança da informação, deve usar a mesma estratégia. Todos os programas de conscientização precisam ser patrocinados para serem bem-sucedidos. No entanto, engajar os funcionários nem sempre é algo simples a ser executado. Para muitas organizações, isso exigirá uma mudança de cultura. Será mais fácil obter a aprovação de um novo paradigma se a alta gestão da companhia compreender as ameaças e seus riscos (GARDNER; THOMAS, 2014). Portanto, a alta gerência, como qualquer outra área da empresa, precisa ser instruída para que se aproprie desta mudança cultural para que o engajamento seja cascateado para todos os recursos humanos de todas as áreas da empresa.

- **Subdomínio 2 - Segurança de Ativos**

Conforme já mencionado, um ativo é, por definição, qualquer coisa que possua valor. Em uma organização, isso inclui pessoas, parceiros de negócio, equipamentos, instalações físicas, sua reputação e, obviamente, suas informações, que se movem pelos sistemas de informação, agregando valor aos processos e, às vezes, aguardando o momento de ser utilizado. Este subdomínio tem por objetivo delimitar os conceitos usados, exclusivamente, na proteção de ativos de informação, na monitoração e na implantação de controles usados para impor vários níveis de confidencialidade, integridade e disponibilidade. O ciclo de vida da informação, conforme também já mencionado, também é parte integrante deste subdomínio e, com isso, o seu uso, a sua manutenção e a sua destruição preparam o terreno para uma discussão dos vários processos que lidam com a informação, suas ameaças inerentes e seus controles para mitigar seus riscos.

Com a arquitetura e o desenho de segurança da informação, este subdomínio visa cobrir a prática para a aplicação de um método abrangente e rigoroso para descrever uma estrutura de modo que essas práticas e processos se alinhem com a direção estratégica e os objetivos principais da organização. A segurança das operações se preocupa, principalmente, com a proteção e controle dos ativos de processamento de informações em ambientes centralizados e distribuídos. Já a governança de segurança de informação e gerenciamento de riscos aborda as estruturas e políticas, conceitos, princípios, estruturas e padrões usados para estabelecer critérios para a

proteção de ativos de informação, também para avaliar a eficácia dessa proteção. Inclui questões de governança, comportamento organizacional e consciência de segurança. O gerenciamento de segurança de informações estabelece a base de um programa de segurança abrangente e proativo para garantir a proteção das informações de uma organização ativa. O ambiente atual de sistemas altamente interconectados e interdependentes necessita do requisito de compreender a ligação entre a tecnologia da informação e o cumprimento dos objetivos de negócios. O gerenciamento de segurança da informação comunica os riscos aceitos pela organização devido aos controles de segurança atualmente implantados e trabalha continuamente para aprimorar os controles de maneira econômica para minimizar o risco para os ativos de informação da empresa. O gerenciamento de segurança abrange os controles administrativos, técnicos e físicos necessários para proteger adequadamente a confidencialidade, integridade e disponibilidade dos ativos de informação. Os controles são manifestados por meio de uma base de políticas, procedimentos, padrões, linhas de base e diretrizes.

- **Subdomínio 3 - Arquitetura e Engenharia de Segurança**

Este subdomínio descreve os conceitos, princípios, estruturas e padrões usados para projetar, implantar, monitorar e proteger sistemas operacionais, equipamentos, redes, aplicativos e os controles usados para impor vários níveis de confidencialidade, integridade e disponibilidade. A arquitetura de segurança da informação se atém a aplicar um método abrangente e rigoroso para descrever uma estrutura atual ou futura para os processos e sistemas de segurança da informação de forma que essas práticas se alinhem com os objetivos da organização. Fornece a estrutura e a base para permitir uma comunicação segura, que proteja os ativos de informação e garantir confidencialidade, integridade e disponibilidade destes. Identifica os serviços básicos necessários para fornecer segurança para sistemas atuais e futuros em modela também as regras de comportamento como as tecnologias necessárias para proteger ativos de forma segura e eficaz. Normalmente, estes modelos são construídos usando metodologias padronizadas baseadas em frameworks de mercado e padrões internacionais. Os principais tópicos abordados por esse subdomínio são:

- Arquitetura do sistema, computação confiável e mecanismos de segurança;
- Modelos de software de segurança da informação;
- Critérios de avaliação e classificações, processos de certificação (*Certification*) e credenciamento (*Accreditation*) de sistemas e segurança de sistemas distribuídos;
- Componentes de criptografia e seus relacionamentos, criptografias simétrica e assimétrica e esteganografia;
- Tópicos relacionados a segurança física de infraestruturas, considerações do projeto do local e da instalação, riscos de segurança física, ameaças e contramedidas, problemas de energia elétrica e suas contramedidas e prevenção, detecção e supressão de incêndios.

Este subdomínio também tem por objetivo auxiliar:

- Na coordenação adequada de investimento em tecnologias e práticas de segurança;
- No planejamento de investimentos e orçamentos operacionais em longo prazo;
- Na interoperabilidade com outros componentes e na arquitetura de sistemas corporativos;
- Na coerência de serviços de segurança tornando-os adaptáveis e escaláveis;
- Na aplicação consistente de práticas e soluções de segurança, incluindo conformidade com as regulamentações;
- A fornecer os meios para garantir que a implantação dos controles de segurança seja correta e verificável.

- **Subdomínio 4 - Segurança de Redes e Comunicação**

O subdomínio Segurança de Redes e Comunicação abrange as estruturas, métodos de transmissão, formatos de transporte e medidas de segurança usadas para fornecer confidencialidade, integridade e disponibilidade para transmissões em redes e meios de comunicação públicos e privados. Redes de computadores usam diversos mecanismos, dispositivos, softwares e protocolos que estão inter-relacionados e

integrados e é um dos tópicos mais complexos no campo da computação, principalmente por conta das tecnologias envolvidas e que estão sempre evoluindo.

A segurança de rede é frequentemente descrita como a pedra fundamental da área de Segurança em Tecnologia da Informação. Tendo em vista que a maioria dos profissionais de segurança da informação no Brasil é oriunda das diversas áreas de Tecnologia da informação é natural, e natural que este seja um subdomínio familiar para estes profissionais. Este subdomínio aborda sob a perspectiva de segurança da informação os seguintes tópicos:

- Modelos OSI e TCP / IP
- Tipos de protocolo e questões de segurança
- Tecnologias LAN, WAN, MAN, intranet e extranet
- Tipos de cabo e tipos de transmissão de dados
- Dispositivos e serviços de rede
- Gerenciamento de segurança de comunicações
- Dispositivos e tecnologias de telecomunicações
- Tecnologias de conectividade remota
- Tecnologias sem fio
- Criptografia de rede
- Ameaças e ataques
- Roteamento definido por software
- Redes de distribuição de conteúdo
- Protocolos multicamadas
- Tecnologias de rede convergentes

Diferentes tecnologias adotadas para os diversos tipos de redes e como elas funcionam juntas para fornecer um ambiente no qual os usuários podem comunicar, compartilhar recursos e ser produtivo são abordados nesse subdomínio e podem ser observados termos específicos relacionados à equipamentos de rede, equipamentos para controle de acesso a redes, mídias de transição de dados, tecnologias de acesso remoto, protocolos de comunicação de dados e redes virtualizadas são frequentemente

mencionados. As diversas formas de ataques às redes e seus métodos de prevenção e mitigação são abordados.

É neste subdomínio que surge o termo **Engenharia Social** como sendo um dos vetores de ataque para sistemas de e-mail em sua forma mais conhecida – o ataque de *phishing*. Os ataques de *phishing* usam e-mail ou sites maliciosos para solicitar informações pessoais aparentando ser uma organização confiável. Uma variação é *spear phishing*, que é um ataque direcionado a públicos ou pessoas específicas.

- **Subdomínio 5 - Gestão de Identidade e de Acessos**

O subdomínio Gerenciamento de Identidade e de Acessos delimita alguns conceitos importantes, que formam a base para a compreensão da forma de funcionamento do gerenciamento de acessos.

Os significados dos termos “sujeito” e “objeto” são delimitados neste subdomínio, assim como o fluxo de informações (acesso) entre eles. Um sujeito é a entidade ativa que solicita acesso a um objeto ou aos dados dentro de um objeto. Um sujeito pode ser um usuário, programa ou processo que acessa um objeto para realizar uma tarefa. Quando um programa acessa um arquivo, o programa é o sujeito e o arquivo é o objeto. Um objeto é entidade passiva que contém informações ou funcionalidades necessárias. Um objeto pode ser um computador, banco de dados, arquivo, programa de computador, diretório ou campo contido em uma tabela dentro de um banco de dados. Em termos práticos, controle de acesso é a coleção de mecanismos, processos ou técnicas que funcionam juntos para proteger os ativos de uma organização contra ameaças e mitigar vulnerabilidades, reduzindo a exposição a atividades não autorizadas e fornecendo acesso a informações e sistemas apenas para pessoas, processos ou sistemas autorizados e protegendo a disponibilidade, integridade e confidencialidade dos ativos de informação.

Neste subdomínio, é definido o significado do termo “controle de acesso”, que são os recursos de segurança que controlam como os usuários e sistemas se comunicam e interagem com outros sistemas e recursos. Eles protegem os sistemas e recursos de acesso não autorizado e podem ser componentes que participam da

determinação do nível de autorização após a conclusão bem-sucedida de um procedimento de autenticação.

O ataque de engenharia social do tipo *phishing* surge aqui como uma forma de ataque de roubo de identidade, mencionando como os atacantes podem criar e-mails falsos, porém convincentes, solicitando às vítimas em potencial para que cliquem em um link para atualizar suas informações de conta bancária, por exemplo. As vítimas incautas, ao clicar nesses links, tem acesso a um formulário solicitando números de contas bancárias, números de previdência social, credenciais e outros tipos de dados pessoais importantes que podem ser usados em crimes de roubo de identidade. O ataque pode ser perpetrado também através de sites falsos semelhantes aos sites legítimos e com nomes de domínio de internet muito parecidos com o endereço do site legítimo (o site www.amazon.com pode se tornar www.amza**0**n.com ou www.itau.com.br pode ser tornar www.**1**tau.com.br), atraindo as vítimas por meio de mensagens de e-mail e outros sites para obter o mesmo tipo de informação.

- **Subdomínio 5 - Avaliação e Testes em Segurança**

Este subdomínio endereça a importância de avaliações periódicas dos controles de segurança implantadas como forma medir a eficácia destes controles. O subdomínio, dividido em quatro seções, ressalta que os controles devem ser continuamente avaliados e melhorados para que a postura de segurança não se torne ineficaz e obsoleta ao longo do:

- **Estratégias de auditoria** – Trata-se do planejamento de uma auditoria dos objetivos da auditoria de segurança, visto que não é possível testar todos os controles e é necessário concentrar esforços naquilo que é relevante e preocupante. Uma auditoria pode ser conduzida por requisitos regulatórios ou de conformidade, por uma mudança significativa na arquitetura dos sistemas de informação ou por conta de novas ameaças que a organização enfrenta.

- **Auditoria de controles técnicos** – Um controle técnico é um controle de segurança implantado através do uso de uma ferramenta tecnológica ou um ativo de Tecnologia da Informação e, geralmente, trata-se de algum tipo de software

configurado de uma maneira particular. Este tópico menciona a auditoria destes controles técnicos e os testes de sua capacidade de mitigar os riscos identificados processo de gerenciamento de risco. A ligação entre os controles e os riscos que eles desejam mitigar é importante para entender o contexto no qual estes controles específicos foram implantados. Desta forma, entendendo o que um controle técnico se destina a realizar, podem ser selecionados os meios adequados de testar a sua eficácia.

- **Auditoria de controles administrativos** – Um controle administrativo é, tipicamente, implantado por meio de políticas ou procedimentos. Neste tópico, são endereçadas as formas de avaliação de controles administrativos, que podem ser elencados em:
  - **Gerenciamento de contas** – Contas de usuários com maior privilégio são diferentes das contas de usuários comuns, que requerem menos privilégios. Contas privilegiadas possuem amplos poderes em um determinado sistema. Embora esses privilégios possam ser necessários, eles podem ser usados indevidamente por atacantes. Manter o controle e a supervisão contínua dessas entidades privilegiadas é necessário para garantir o uso legítimo destas. Contas de usuários comuns também precisam ser controladas por meio de boas práticas de gerenciamento de contas.
  - **Verificação de cópias de segurança** (*backups*) – As organizações modernas lidam com grandes quantidades de dados estes que devem ser protegidos por uma variedade de razões, incluindo recuperação de desastres. Independentemente da estratégia de backup de dados adotada, é necessário testá-lo periodicamente para garantir a sua disponibilidade, principalmente, ao enfrentar um evento ou desastre que exige restauração de alguns ou todos os dados armazenados nos backups. Desta forma, evita-se descobrir que a cópia de segurança possuía dados ausentes, corrompidos ou desatualizados. Esta seção visa discutir as abordagens que devem ser adotadas com o intuito de avaliar a disponibilidade destes dados quando necessários
  - **Recuperação de desastres e continuidade de negócios** – O plano de continuidade de negócios (BCP) - que deve incorporar um plano de recuperação de desastres (DRP) - precisa ser testado e exercitado

regularmente porque os ambientes mudam continuamente. Todas as vezes que ocorre um exercício e BCP, pontos de melhorias são descobertas, proporcionando resultados melhores ao longo do tempo. A responsabilidade de estabelecer exercícios periódicos e a manutenção do plano deve ser atribuída a uma pessoa ou pessoas específicas que terão responsabilidades nas iniciativas relacionadas ao plano de continuidade de negócios dentro da organização. A manutenção do BCP deve estar incorporada no processo de gerenciamento de mudanças, pois, com isso, quaisquer mudanças no ambiente serão refletidas no plano de continuidade. Os testes e exercícios visam também apontar problemas relacionados mão somente aos processos de negócio, mas também aos problemas relacionados à equipe de planejamento e gerenciamento do processo e que podem não ter sido, previamente, contemplados. No final, os exercícios devem demonstrar se a empresa pode se recuperar, realmente, de um desastre.

- **Treinamento e conscientização em segurança** – É importante para a organização avaliar o desempenho das ações de segurança com a finalidade melhoria contínua das iniciativas. Também é importante para a organização garantir que os usuários conheçam suas responsabilidades no que tange segurança da informação e que concordem em se submeter ao programa, políticas, procedimentos, planos e iniciativas de segurança da organização através da assinatura de um termo ou através de algum outro método que comprove a aceitação desse compromisso. Quanto a processo de medição, podem ser utilizados exercícios simulados de engenharia social, questionários, *quizzes* e outros.
- **Indicadores de desempenho e de risco** – Os indicadores de desempenho (do inglês, *Key Performance Indicator* ou *KPI*) são ponteiros que mostram o progresso relacionado a um determinado objetivo. Estes indicadores fornecem uma direção para a melhoria estratégica e operacional, criam uma base analítica para a tomada de decisões e ajudam a focar a atenção no que é mais importante. Para a gestão através do uso de indicadores, é necessária a definição de metas, do nível de desempenho desejado e o rastreabilidade do progresso em relação a essa meta. Paralelamente ao *KPI*, existe o Indicador de Risco (do inglês, *Key Risk Indicator* ou *KRI*), que é uma métrica para

avaliação da probabilidade de um evento e suas consequências extrapolarem o apetite de risco da organização. O papel principal de um *KRI* é rastrear as tendências ao longo de um período, que são então convertidas em sinais de alerta antecipado. Por meio da associação de *KRI*s aos riscos contidos em um registro de risco, os dados coletados em um *KRI*s auxiliam no processo de tomada de decisão para a equipe de risco, fornecendo incentivos e mensuráveis reais para basear suas decisões de gerenciamento de risco.

- **Avaliação da postura de segurança** – Esta é a etapa é que melhor distingue o um bom profissional de segurança da informação de outros, pois além de entender a função de segurança dos sistemas de informação dentro do contexto mais amplo do negócio, é também capaz de comunicá-la a públicos técnicos e não técnicos. É necessário traduzir as principais conclusões e recomendações em uma linguagem que seja acessível e significativo para a liderança sênior de sua organização, pois é deles que virão o apoio, autoridade e os recursos necessários que permitirá que a implantação dos ajustes necessários. A elaboração de relatórios técnicos deve ser muito mais do que apenas mostrar os resultados extraídos de uma ferramenta, mas deve ser aplicada uma metodologia padrão ao contexto específico do sistema avaliado. Em outras palavras, o relatório deve provar que a auditoria foi feita de maneira personalizada medida e, acima de tudo, o relatório deve mencionar os riscos à organização. Normalmente, estes relatórios incluem um pequeno resumo executivo de não mais do que uma ou duas páginas, o que destaca o que os líderes seniores precisam saber a partir do relatório. Entretanto, é necessário tomar a atenção da alta liderança para efetuar a mudança desejada. Diferentemente dos relatórios técnicos, os relatórios executivos explicam os resultados da auditoria em termos de exposição ao risco. Segurança da Informação é quase sempre percebido como um centro de custo para a empresa e uma maneira adequada de mostrar o Retorno de Investimento (ROI) para um departamento que, basicamente, não gera lucros é quantificar o risco em termos monetários. Embora a análise gerencial já exista há muito tempo, o uso moderno do termo talvez seja mais bem fundamentado em padrões de qualidade (como a série ISO 9000) e estes definem um ciclo PDCA (*Plan, Do, Check* e *Act*) de melhoria contínua.

Neste subdomínio, o termo Engenharia Social também é mencionado, porém é abordado como uma forma de teste para avaliar o quão os usuários são suscetíveis a esta forma de ataque ou o nível de conhecimento para detectar este tipo de ataque. Conceitualmente, exercícios simulados de engenharia social não deixam ataques, uma vez que estes exercícios utilizam as técnicas aplicadas pelos atacantes, porém a diferença está no viés benigno da ação. Tendo em vista que os usuários podem não confessar de maneira espontânea que foram vítimas de um ataque de engenharia social e nem sempre os controles técnicos irão detectar, de alguma maneira, é importante que sejam conduzidos exercícios de engenharia social tendo os usuários como alvos deste "ataque". Desta forma, quando os usuários, por exemplo, clicam em um link em um e-mail como parte do exercício, estes são avisados de que fizeram algo errado e podem ser redirecionados para uma página web com conteúdo educacional evitar tais erros no futuro, em situações reais de ataque. Paralelamente, é possível verificar quais usuários são mais suscetíveis e com que frequência esses ataques poderiam ser bem-sucedidos.

- **Subdomínio 7 - Segurança em Operações**

Este subdomínio diz respeito a tudo o que ocorre para manter redes, computadores sistemas, aplicativos e ambientes em funcionamento de forma segura e protegida. O subdomínio explica como garantir que pessoas, aplicativos, servidores e equipamentos tenham apenas os acessos e privilégios aos recursos. Podemos dividir este subdomínio em dois tópicos:

- **Segurança de operações** - A segurança das operações preocupa-se principalmente com a proteção e o controle dos ativos de processamento de informações em ambientes centralizados e distribuídos.
- **Operações de segurança** - As operações de segurança estão principalmente preocupadas com as tarefas diárias necessárias para manter os serviços de segurança operando de forma confiável e eficiente. A segurança das operações é uma qualidade de outros serviços e um conjunto de serviços por direito próprio.

Neste subdomínio são abordados os conceitos de Plano de Continuidade de Negócios (do inglês *Business Continuity Planning* ou BCP) e Plano de Recuperação de Desastres (do inglês *Disaster Recovery Planning* ou DRP), que abordam a preparação, os processos e as práticas necessárias para garantir a preservação da organização em face de grandes interrupções nas operações normais da. BCP e DRP envolvem a identificação, seleção, implantação, teste e atualização de processos e ações específicas necessárias para proteger os processos críticos da organização dos efeitos de grandes interrupções do sistema e da rede e para garantir a restauração oportuna das operações da organização se ocorrer interrupções significativas. Também são endereçadas as questões de resposta aos incidentes de segurança da informação, que envolvem a detecção, contenção, erradicação e recuperação que são necessárias para garantir a continuidade dos negócios.

Também é abordado o conceito de incidente de segurança, que é todo o evento que afete a confidencialidade, integridade e disponibilidade dos ativos (SÊMOLA, 2003). Nieles, Dempsey, Pillitteri (2017) complementam que este evento pode ocorrer em um sistema de informação, nas informações que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação da segurança políticas, procedimentos de segurança ou políticas de uso aceitável. No caso de políticas e procedimentos de segurança, em um primeiro momento, vem à mente as regras corporativas para uso seguro de recursos de tecnologia, mas podemos transcender estas regras para outros cenários além do mundo empresarial, incluindo o mundo doméstico. Sistemas de controle parental, que controlam o acesso aos aplicativos ou ao acesso simples à internet através de navegadores, e regras impostas pelos responsáveis por crianças no uso de recursos de tecnologia, uma vez violados, não deixam de ser incidentes de segurança, por exemplo. Já no mundo corporativo, um incidente de segurança pode acarretar impactos de ordem financeira, regulatória e, mesmo em sua reputação Como consequência, afetar negativamente a empresa.

- **Subdomínio 8 - Segurança no Desenvolvimento de Software**

Embora a segurança da informação tradicionalmente enfatize os controles de acesso no nível do sistema, é necessário também focar esforços na segurança de sistemas e aplicativos e que estes também sejam incluídos na arquitetura de segurança

corporativa. Critérios de Segurança devem ser adotados em todo o ciclo de vida do desenvolvimento de sistemas, desde a sua concepção até a sua descontinuação. Isso se deve ao fato de muitos incidentes de segurança da informação envolver vulnerabilidades em sistemas e aplicativos.

Neste subdomínio é onde o termo malware e todos os seus termos derivados, (vírus, trojans ou cavalos de Tróia, *worms* ou vermes etc.) são mencionados. É apresentado o grande risco de segurança enfrentado por todas as empresas que se conectam a redes externas e permitem que dados externos sejam inseridos em sistemas internos de alguma forma, sejam eles desenvolvidos ou não internamente e a importância da manutenção e configuração de aplicativos para evitar esses riscos.

Menciona-se também a dificuldade de encontrar profissionais desenvolvedores de sistemas com habilidades de segurança da informação. Esse cenário tem se mostrado diferente, pois existe uma visão com maior foco segurança da informa. Modelos e metodologias de desenvolvimento já estão se apoiando em melhores práticas de desenvolvimento e encontramos cada vez mais desenvolvedores que estão preocupados com o processo de desenvolvimento seguro. Empresas que antes não entendiam isso como um a prioridade, agora entendem a necessidade de desenvolver essas habilidades em sua equipe[34].

É importante observar na análise deste domínio que muitos assuntos relacionados à segurança da informação são transversais (engenharia social, arquitetura de segurança, plano de continuidade de negócios etc.). Isto não é diferente para a conscientização dos usuários de informações nos assuntos que tangem segurança da informação. Desta forma, entender o processo de conscientização e seus públicos-alvo é crucial para o sucesso do programa.

[34] DevSecOps: crescendo cada vez mais e dominando o mercado – Conviso AppSec - https://blog.convisoappsec.com/secdevops-crescendo-cada-vez-mais-e-dominando-o-mercado. Acesso em 01/05/2021.

6. ASPECTOS TEÓRICOS DA TERMINOLOGIA

A ciência avança e a divulgação de suas pesquisas produz uma documentação variada, em diferentes línguas. A transmissão do saber faz-se por meio de textos que possuem características peculiares, em nível semiótico, pragmático, sintático, semântico e, sobretudo, lexical, uma vez que é principalmente por meio de uma terminologia própria que esse tipo de texto veicula os conhecimentos especializados (BARROS, 2006).

A Terminologia, enquanto campo que estuda representação do conhecimento especializado e o vocabulário das áreas técnicas e científicas, desempenha um papel fundamental nesse processo. Entretanto, vários elementos intervêm nos estudos terminológicos – diversidade temática, objetivos, contexto de trabalho, de metodologia, de visão de objeto de estudo – fazendo com que a disciplina cientifica seja vista por diferentes prismas. Conforme exemplificado usando o termo "vírus" em tópicos anteriores, percebemos que distintas abordagens podem conduzir a diferentes definições de um mesmo objeto (BARROS, 2004). Desta forma, Barros delimita que a Terminologia pode ser analisada de acordo com suas:

- Funções da Terminologia;
- Finalidades e Métodos;
- Escolas e Perspectiva do Objeto

Quantos às funções da Terminologia, seja qual for o contexto, deve representar esse conhecimento, assim como a sua transmissão e o grau de especialização deste conhecimento pode variar de acordo com a densidade terminológica. (CABRE, 1999). Os termos que determinam essa densidade constituem seu objeto de análise e produção este conjunto de termos é um elemento precioso para comunicação particular ou profissional para diferentes públicos. Desta forma, Barros (2004), a terminologia, na qualidade de conjunto de unidades linguísticas, pode ser considerada sob três perspectivas, que enveredam para três dimensões e estas para três funções como disciplina científica, conforme descrito abaixo:

Tabela 7 – Funções da Terminologia

PERSPECTIVA	DIMENSÃO	FUNÇÃO
• Quem com ela trabalha • Quem usa para se expressar • Quem a dirige	• Metalinguística • Comunicativa • Político-indenitária	• Conceitual ou cognitiva • Comunicacional • Simbólica ou identitária
• Análise e descrição terminológica; • Sistematização dos termos para compreensão e comunicação do saber.	• Relacionado à comunicação, informação e transferência de conhecimentos, através de discurso científico e técnico; • Nesta etapa, os termos são investidos de valor e sua validade, economia, precisão e eficiência são testadas.	• Relaciona a Terminologia a uma identidade nacional, regional ou de um grupo; • É evidenciado através de intervenções oficiais por meio de resgate da identidade nacional ou, por lado, da asfixia de idiomas ou dialetos.

Fonte: BARROS (2004) e elaborado pelo autor

Os estudos terminológicos desenvolvidos em diversos países permitem a identificação de três tendências na Terminologia Mundial, segundo AUGER (entre 1978 e 1989, apud BARROS; 2004, P.46):

Tabela 8 – Finalidades e Métodos da Terminologia

TENDÊNCIA	CORRENTE	EXPLICAÇÃO
Orientada para o sistema linguístico	Linguístico-terminológica	Considera subconjunto léxico como objeto de estudo focado na descrição, organização sistemática e normalização de termos e conceitos.
Orientada para a tradução	Traducionista	Tem o objetivo de dar aos tradutores instrumentos de trabalho e produções dotadas de maior grau de precisão.
Orientada para o planejamento	Planejadora	Servem ao planejamento linguístico, fornecendo dados importantes para a elaboração de instrumentos de modificação da forma e do estatuto de uma língua.

Fonte: BARROS (2004) e elaborado pelo autor

Para FELBER (1984, apud BARROS; 2004, P.47), na perspectiva do objeto Terminologia pode ser classificada de acordo com o enfoque dado a seu objeto de estudo pelas diferentes correntes cientificas, a saber:

- **Linguística** – Ocupa-se das línguas de especialidades e de suas respectivas terminologias, que devem ser analisadas por modelos linguísticos, pois, embora possuam especificidades de ordem sintáticas, léxico-semânticas, estilísticas e outras, fazem parte da língua geral.
- **Filosófica** – Foca a atenção no estudo dos conceitos e em sua classificação em categorias filosóficas, elaborando teorias de classificação e aproximando-se da abordagem orientada aos domínios.
- **Abordagem orientada aos domínios** – Trata o conceito e suas relações com outros conceitos. Atua de maneira autônoma, distinta da linguística, seguindo um percurso onomasiológico, indo do conceito à sua designação.

Wuster considera a terminologia como estando localizada na interseção da linguística, lógica, ontologia, ciência da informação, ciência da computação e disciplinas individuais. Esta interdisciplinaridade da terminologia é determinada pelas características da terminologia unidades, que são simultaneamente unidades de linguagem (linguística), cognitivos elementos (lógica e ontologia, ou seja, parte da ciência cognitiva) e veículos de comunicação (teoria da comunicação). Os termos aparecem em comunicações especializadas (ciência da informação) e os computadores são geralmente empregados na atividade terminográfica (Ciência da Computação).

O lado cognitivo da Terminologia é representado pela ordenação do pensamento e da conceituação. A transferência de conhecimento constitui seu lado comunicativo. Terminologia é a característica mais importante da comunicação especializada porque as línguas especiais se diferenciam da língua geral e das várias línguas especiais umas das outras. Os especialistas usam terminologia não apenas para fazer ordenar o pensamento, mas também para transferir conhecimento especializado em uma ou mais línguas e estruturar as informações contidas em textos especializados.

Em uma perspectiva cognitivista, surge uma nova concepção de termo. Rita Temmerman rejeita a ideia de conceito e de significado e propõe que se fale em unidade de compreensão ou de entendimento (*unit of understanding*) em sua teoria da Terminologia

Sociocognitiva. Nessa linha, a delimitação do conteúdo toma como base o texto no qual o termo está inserido (TEMMERMAN, 2000). Desse modo, o conceito não é universal nem imutável, mas a expressão de um conjunto de elementos de natureza linguística que se consubstanciam em um texto que possui não apenas uma dimensão linguística, mas também pragmática, discursiva e comunicativa. A abordagem Sociocognitiva pode se beneficiar dos achados de semântica cognitiva que elabora todo o potencial da interação entre o mundo, a linguagem e a mente humana; e pela percepção de que os elementos do triângulo semântico funcionam em um ambiente social (TEMMERMAN, 1997).

Passou-se também a estudar a unidade terminológica também do ponto de vista sociolinguístico, o que proporcionou o surgimento da Socioterminologia. De acordo com essa disciplina científica, as variantes lexicais e conceptuais devem constituir objeto de estudo da terminologia e devem ser analisadas em contexto. Faulstich (1995) delimita a Socioterminologia como sendo uma disciplina que se ocupa da identificação e da categorização das variantes linguísticas dos termos em diferentes tipos de situação de uso da língua. É preciso levar em conta critérios básicos de variação terminológica no meio social, bem como critérios etnográficos, porque as comunicações entre membros da comunidade em estudo podem gerar termos diferentes para um mesmo conceito ou mais de um conceito para o mesmo termo. As reflexões sobre a variação lexical e a identidade científica da Socioterminologia são feitas, no âmbito deste Núcleo Temático, no artigo de Faulstisch intitulado “A Socioterminologia na comunicação científica e técnica”. Nele a autora ressalta que a Socioterminologia "é um ramo da terminologia que se propõe a refinar o conhecimento dos discursos especializados, científicos e técnicos, a auxiliar na planificação linguística e a oferecer recursos sobre as circunstâncias da elaboração desses discursos ao explorar as ligações entre a terminologia e a sociedade" (FAULSTICH, 2006).

Por fim, a Terminologia Frame-based, de Pamela Faber (2009), é uma abordagem cognitiva da Terminologia, que vincula diretamente a representação do conhecimento especializado à linguística cognitiva e semântica, que compartilha muitas das mesmas premissas entre a Teoria Comunicativa da Terminologia de Cabré e também da Teoria Sociocognitiva de Temmerman.

7. ANÁLISE TERMINOLÓGICA DO DOMÍNIO SEGURANÇA DA INFORMAÇÃO

A Terminologia, especialmente como um campo interdisciplinar, é interessante por conta das relações internas e externas que mantém com as áreas de conhecimento que a entornam. Com isso, a Terminologia se molda a outros campos de conhecimento, dos quais toma emprestado um conjunto específico de conceitos. Entretanto, uma determinada área de conhecimento não define seu campo de estudo com uma adição linear de conceitos de diferentes origens, mas extraindo de cada assunto um certo número correto de conceitos e elementos e desenvolvendo a partir desses conceitos um objeto e um campo próprio. Somente após isso, pode-se dizer que a área de conhecimento adquiriu um status de novo área (CABRE, 1999).

7.1. Relacionamento com Segurança da Informação

Como exemplo de termo do domínio Segurança da Informação temos o termo *Hacker*. Este termo tem diversas definições, mas as mídias de comunicação apropriaram-se do termo, mas deturparam seu conceito (SCHNEIER, 2004; RICHET, 2015). É comum associá-lo a um indivíduo criminoso que comete delitos digitais, rouba dados e derruba sistemas. O trecho abaixo, extraído da notícia veiculada no portal G1 em 21/07/2020 sobre a acusação de roubo de dados relacionados a vacina contra o Covid-19 por criminosos chineses feita pelo governo dos Estados Unidos, evidencia esta definição equivocada:

> "O Departamento de Justiça norte-americano denunciou nesta terça-feira (21) **dois hackers chineses suspeitos de roubar informações** sobre projetos de vacinas contra a Covid-19. Eles também são acusados de **violar a propriedade intelectual** de empresas nos Estados Unidos e em outros países (EUA, 2020)."[35]

[35] EUA acusam hackers chineses de roubar dados sobre vacina contra a Covid-19. G1, 21 julho 2020. Disponível em: https://g1.globo.com/mundo/noticia/2020/07/21/eua-acusam-dois-hackers-chineses-de-roubar-dados-sobre-projetos-de-vacina-contra-covid-19.ghtml. Acesso em: 13 ago 2020.

As ações criminosas mencionadas no trecho da notícia e atribuídas, erroneamente, a um *hacker*, na verdade, é o conceito de *cracker*. Desta forma, é importante delimitar a diferença de conceito entre estes dois termos:

- *Hackers* – Indivíduos que procuram ter uma compreensão profunda do funcionamento interno de sistemas, computadores e redes de computadores em especial. Dedicam-se a entender o funcionamento destes dispositivos, extrapolando os limites do funcionamento normal destes sistemas, conforme previstos por quem os projetou.
- *Crackers* – Indivíduos que usam suas habilidades relacionadas à segurança de computador para, ilegalmente, infiltrar sistemas seguros com a intenção de prejudicar o seu funcionamento ou com outra intenção criminosa. Este termo também é usado para diferenciá-los do original e não criminoso hacker (RICHET, 2013).

Entretanto, muito embora o conceito tenha sido deturpado de seu sentido original, conforme mencionado por Schneier, o termo "*hacker*" já foi apropriado como sendo o indivíduo que comete crimes em detrimento ao indivíduo que estuda tecnologias de maneira profunda e até mesmo empresas especialistas em segurança da informação já se referem ao termo desta forma. Como exemplo, logo abaixo, podemos ver um trecho de uma notícia da The Hack, que é uma revista digital especializada na área de Segurança da Informação.

Figura 11 – Notícia utilizando o termo "Hacker" no sentido de criminoso digital.

Fonte: site The Hack [36]

[36] https://thehack.com.br/hackers-chineses-teriam-invadido-servidores-da-vale/

A Terminologia aborda a relação entre o termo e o conceito dentro de um determinado domínio. Segundo Barros (2004), a Terminologia tem como campo de atuação o estudo das línguas de especialidades, que são subsistemas linguísticos que compreendem o conjunto dos meios linguísticos próprios de um campo da experiência, de conhecimento ou de atuação. Trata-se de um subsistema baseado na língua geral, porém com discurso técnico especializado. Barros descreve que embora cada universo de discurso especializado tenha particularidades sintáticas, pragmáticas, semióticas e terminológicas especificas, não deixam de ser regidas por uma língua geral. Desta forma, não se trata de uma língua de especialidade, mas uma linguagem de especialidade conforme apresentado na figura abaixo que ilustra a língua geral posicionada como ponto central que norteia as linguagens de especialidade que a cercam.

Figura 12 – Relação entre a língua geral e as linguagens de especialidade.

Fonte: elaborado pelo autor

Já o objeto de estudo da Terminologia é o termo que, segundo a ISO 1087-1990[37], que se define como a designação, por meio de uma unidade linguística, de um conceito em uma linguagem de especialidade. Trata-se de uma palavra, uma unidade lexical, com um conceito específico dentro de um domínio de conhecimento específico (BARROS, 2004). Um exemplo disso é o termo “vírus”, que possui definições diferentes em diversos domínios do conhecimento como exemplificado no quadro a seguir:

[37] ISO - ISO 1087:1990 - Terminology — Vocabulary - https://www.iso.org/standard/5591.html

Tabela 9 – Comparação do termo “vírus” entre diversos domínios de conhecimento.

DEFINIÇÃO DO TERMO “VÍRUS”		
SEGURANÇA DA INFORMAÇÃO	BIOLOGIA	MEDICINA
Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.[38]	Partícula basicamente proteica que pode infectar organismos vivos. Vírus são parasitas obrigatórios do interior celular e isso significa que eles somente se reproduzem pela invasão e possessão do controle da maquinaria de autorreprodução celular. O termo vírus geralmente refere-se às partículas que infectam eucariontes (organismos cujas células têm carioteca), enquanto o termo bacteriófago ou fago é utilizado para descrever aqueles que infectam procariontes (domínios bactéria e archaea).[39]	Microrganismo menor do que uma bactéria que não pode crescer ou se reproduzir separado de uma célula viva. Um vírus invade células vivas e usa sua maquinaria química para se manter vivo e se replicar. Pode se reproduzir com fidelidade ou com erros (mutações); essa capacidade de mutação é responsável pela capacidade de alguns vírus se alterarem ligeiramente em cada pessoa infectada, dificultando o tratamento. Os vírus causam muitas infecções humanas comuns e são responsáveis por uma série de doenças raras.[40]

Fonte: elaborado pelo autor

Embora as definições deste termo sejam diversas nos diferentes domínios exemplificados, é possível identificar um radical ou porção comum na referida definição, que permite que o termo possa ser intercambiado entre os domínios de conhecimento, desde que devidamente ajustado para que possua discurso próprio, ou seja, que tenha características em níveis léxico-semântico, semântico-sintático, narrativo e discursivo no texto técnico, científico ou especializado (BARROS, 2004). Abaixo, utilizando o exemplo do quadro anterior, são mostrados trechos que indicam a similaridades na definição dos termos em suas respectivas áreas de conhecimento:

[38] https://cartilha.cert.br/glossario/#v
[39] https://www.sobiologia.com.br/conteudos/Seresvivos/Ciencias/biovirus.php
[40] https://www.medicinenet.com/script/main/art.asp?articlekey=5997

Tabela 10 – Semelhanças do termo "vírus" em diversos domínios de conhecimento

SEMELHANÇAS DO TERMO "VÍRUS"		
SEGURANÇA DA INFORMAÇÃO	BIOLOGIA	MEDICINA
...normalmente malicioso...	... infectar organismos vivos...	Os vírus causam muitas infecções humanas...
... inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos...	... se reproduzem pela invasão e possessão do controle da maquinaria de autorreprodução celular.	Um vírus invade células vivas e usa sua maquinaria química para **se manter vivo** e se replicar
O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.	...somente se reproduzem pela invasão e possessão do controle da maquinaria de autorreprodução celular.	Um vírus invade células vivas e usa sua maquinaria química para se manter vivo e **se replicar**.

Fonte: elaborado pelo autor baseado nas informações da Tabela 9

Visto que os textos técnicos, científicos e especializados possuem um objetivo de comunicação, ou seja, de transmitir uma informação, é importante salientar que a função referencial predominante e as unidades lexicais, com conteúdo especificam de cada domínio de conhecimento, é sua principal característica.

Desta forma, aprender o conhecimento transmitido pelas unidades terminológicas especializadas pode ser comparado a aprender uma segunda língua. É importante frisar que a primeira língua ou língua geral serve a muitas necessidades de comunicação e expressão cotidianas e se aprende através de imitação. As unidades terminológicas aprendidas são segunda língua, porém trata-se de uma metalinguagem, pois esta é transmitia e ensinada através da primeira. O ensino do significado de um termo específico do campo de Segurança da Informação é feito da mesma maneira para um termo de Medicina, Biologia, Tecnologia da Informação ou de uma palavra em alemão ou sueco (SAGER, 1993).

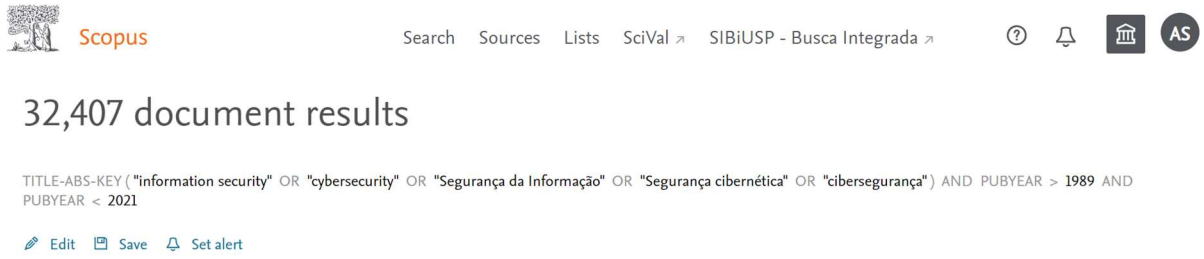
Entretanto é importante admitir que cada pessoa tem um domínio próprio de seu idioma e que esse domínio é caracterizado por sua educação, nível cultural, sua procedência geográfica etc. Esse domínio não uniforme da língua leva a várias formas de aprender e que implicam, consequentemente em níveis variados de compreensão. Essas várias formas de compreensão são, nitidamente, observadas no trabalho de tradutores e intérpretes. Estes profissionais compreendem textos especializados sem, no entanto, serem especialistas em determinado campo e conseguem expressá-los em outro idioma. Os tradutores atuam como pontes entre a linguagem e áreas de especialidades, pois conhecem a linguagem do campo, mas não como especialistas. Desta forma, deve ser admitido que existem diversos níveis de

saber, conectando a Terminologia com a Psicolinguística e a Ciência Cognitiva (SAGER, 1993). A tradução de textos especializados, principalmente nos campos da Segurança da Informação e Tecnologia da Informação possuem particularidades que serão estudadas adiante.

7.2. Produção cientifica em Segurança da Informação e a relação com idiomas

Apenas para comprovar de forma bibliométrica a escassa produção científica da área de Segurança da Informação em língua portuguesa, foi feita uma busca básica no site da base de dados bibliográfica Scopus por títulos de artigos, resumos e palavras-chaves que continham o termo "*Information Security*", "*Cybersecurity*", "Segurança da Informação", "Segurança Cibernética" e "Cibersegurança" entre os anos de 1990 e 2019.

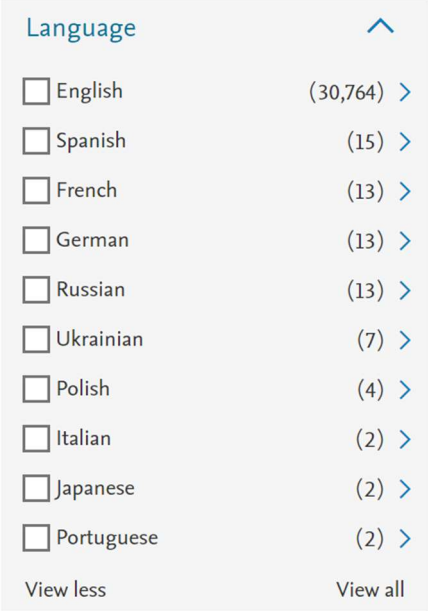
Figura 13 – Resultados da pesquisa feita no site www.scopus.com



Os resultados mostraram que foram encontrados 32.407 documentos de diversas línguas, sendo que 95% destes documentos estão no idioma inglês[41].

[41] Scopus - Document search results - https://www.scopus.com/results/results.uri?sort=plf-f&src=s&sid=62f69af05aea040b313a493c925312de&sot=a&sdt=a&sl=170&s=TITLE-ABS-KEY%28%22information+security%22+OR+%22cybersecurity%22+or+%22Seguran%c3%a7a+da+Informa%c3%a7%c3%a3o%22+OR+%22Seguran%c3%a7a+cibern%c3%a9tica%22+OR+%22ciberseguran%c3%a7a%22%29+AND+PUBYEAR+%3e+1989+AND+PUBYEAR+%3c+2021&origin=searchadvanced&editSaveSearch=&txGid=456c92476789584459278639385823 8e

Figura 14 – Levantamento bibliométrico através do site www.scopus.com



Desta forma, é necessário que o profissional desta área domine a leitura, no mínimo técnica, de materiais com origem no idioma inglês. Entretanto, é importante que existam literaturas básicas para os usuários não técnicos que, por alguma razão, queiram se aprofundar nos temas relacionados a esta área e que precisam que os materiais estejam em língua portuguesa por não dominar outro idioma.

Por conta disso, é importante que o tradutor tenha conhecimento dos termos técnicos que devem e aqueles que não devem ser traduzidos nestes materiais para que não haja prejuízo da compreensão da mensagem e, consequentemente, uma falha na apropriação daquela informação.

7.3. A Terminologia na tradução de textos especializados

A aplicação da Terminologia é ampla, podendo ser utilizada no ensino de idiomas, no ensino de disciplinas técnicas e científicas, nas Ciências Sociais, no planejamento linguístico e outras. O intuito desta pesquisa não é abordar as diversas aplicações da Terminologia, porém existe uma aplicação que merece uma atenção especial, que é a tradução de textos técnicos, científicos e especializados.

SAGER (1993) afirmou ou que existem várias formas de aprender que implicam em vários níveis de compreensão e que a evidência mais clara destes níveis de compreensão

são os tradutores e intérpretes. Estes profissionais não são especialistas, mas compreendem textos especializados relacionados a diversos campos de conhecimento ao ponto de expressá-los em outro idioma, mas não são habilitados a atuar nestas áreas especializadas. Particularmente, em Tecnologia da Informação e Segurança da Informação, não conhecer, minimamente, os termos destas áreas pode acarretar prejuízos de compreensão na tradução de termos técnicos, principalmente, quando se trata de interlocutores com especialização de nível médio ou alto nestas áreas. Muitos dos termos utilizados nestas áreas estão em inglês e devem continuar dessa forma em língua portuguesa, pois os profissionais destas áreas já estão habituados com esta terminologia. Traduzir termos como *firewalls, switches, backdoors, broadcast* dentre outros pode não gerar um problema que, porventura, venha a comprometer o entendimento por parte de interlocutores profissionais das áreas de Segurança da Informação e Tecnologia da Informação, mas soa estranho, visto que não são termos usuais. Em provas de certificação profissional oferecidas por entidades e empresas tais como, por exemplo, Microsoft e Cisco, não é incomum que os exames sejam feitos em língua inglesa pelos pretendentes. A razão disso é para que não haja perda de tempo em compreender as questões contendo traduções literais de termos técnicos. Desta forma, é necessário diferenciar as diferentes formas de saber de quem irá obter o conhecimento. Existem linguagens usadas pelos especialistas para se comunicar com outros especialistas e linguagens para se comunicar com interlocutores menos especializados ou não especializados. O discurso científico deve ser ajustado para os mais diversos públicos (CABRÉ, 1993).

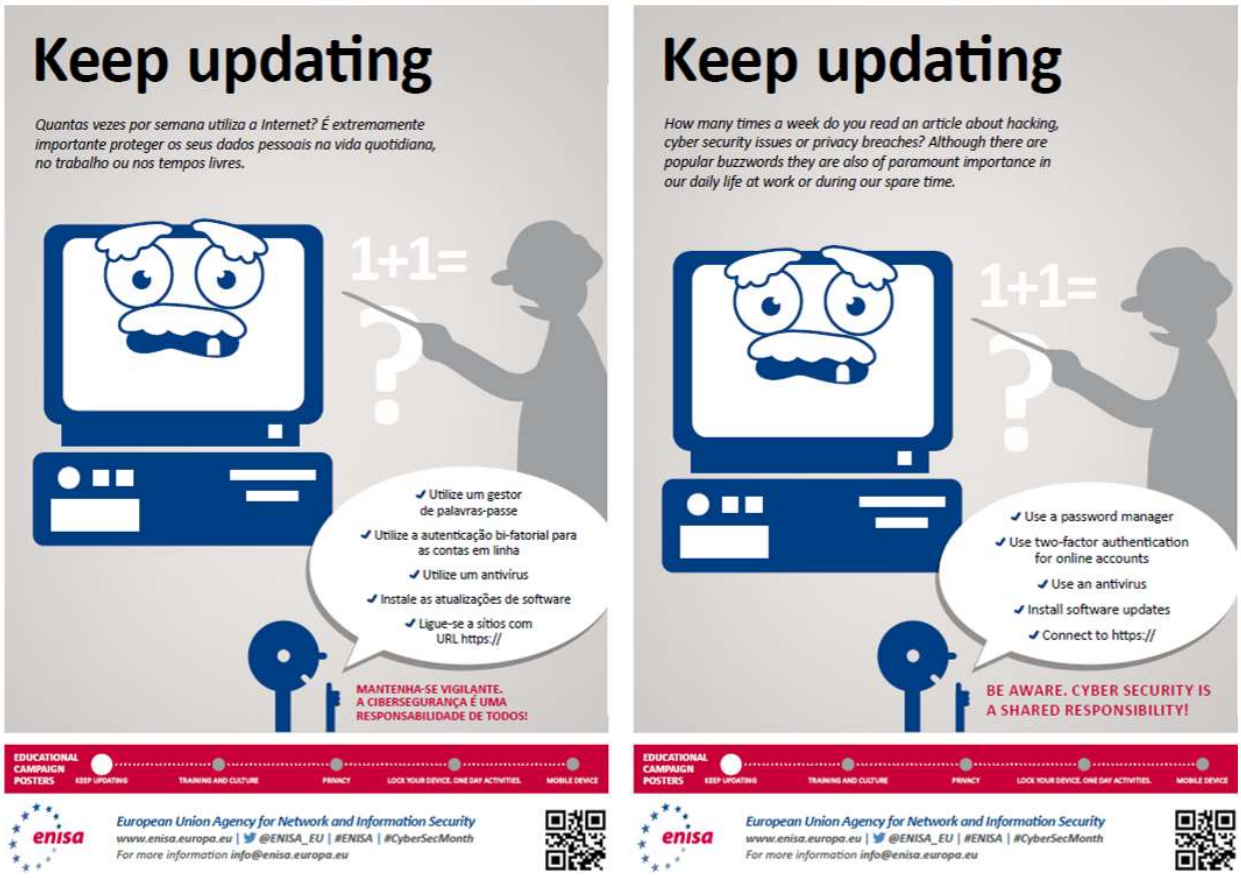
BARROS (2004) menciona que o processo de tradução implica na compreensão do texto na língua de partida e o conhecimento das unidades terminológicas especializadas, visto que é por meio de sua terminologia que este tipo de texto transmite o conhecimento de determinada área de conhecimento. Entretanto, um trabalho de tradução de qualidade não deve apenas refletir o mesmo conteúdo que o texto de partida, mas expressar-se nos mesmos moldes de um nativo da língua de chegada.

A tradução de termos nos campos de Segurança da Informação e Tecnologia da Informação merece um recorte especial, pois, nestas áreas, a tradução de textos técnicos possui algumas particularidades. O profissional que atua na tradução de textos destes campos precisa compreender que alguns termos já são largamente conhecidos e aceitos, não havendo a necessidade de tradução para a língua portuguesa, principalmente, quando traduzidos do idioma inglês. Para usuários de ativos de informação em geral, isso ocorre por conta da força de imposição da cultura americana no Brasil através das várias formas disponíveis de mídia

que é possível ter acesso. Contudo, para profissionais destas áreas, isso ocorre devido a produção de materiais acadêmicos e literaturas profissionais, que, em sua maioria, são produzidos em língua inglesa.

As figuras abaixo foram extraídas do site da ENISA (*European Union Agency for Cybersecurity*). Trata-se de dois pôsteres, em língua inglesa (lado direito) e portuguesa (lado esquerdo), usados em uma campanha de educação e conscientização sobre proteção de dados pessoais.

Figura 15 - Exemplos de pôsteres de conscientização.



Fonte: site da ENISA. [42]

A figura em inglês possui os termos corretos e que são comumente utilizados neste idioma. A figura em português possui os termos equivalentes traduzidos. Para um melhor estudo dos termos, foram extraídos das figuras alguns termos em inglês e o seu respectivo equivalente em português. A tabela abaixo mostra os termos extraídos da figura e os termos corretos equivalentes utilizados em língua portuguesa:

[42] https://www.enisa.europa.eu/topics/cybersecurity-education

Tabela 11 - Análise comparativa de termos em inglês da figura 15.

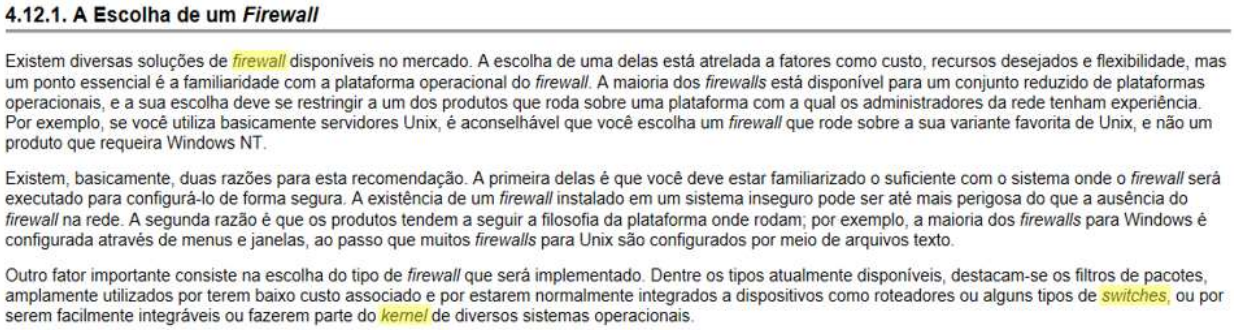
ANÁLISE DOS TERMOS DA FIGURA		
Termo em inglês	**Termo em português**	**Termo correto equivalente em português brasileiro**
Password Manager	Gestor de palavra-passe	Gerenciador de senhas
Two-Factor Authentication	Autenticação bifatorial	Autenticação em dois fatores
Online accounts	Contas em linha	Contas online

Fonte: elaborado pelo autor.

Percebe-se que os termos em inglês possuem equivalentes adequados em língua portuguesa, embora seja possível, com algum esforço, a compreensão da mensagem transmitida na figura em língua portuguesa. Todavia, os termos utilizados não sejam coloquiais e soarão estranhos para nativos em língua portuguesa.

Por outro lado, existem alguns termos que não possuem termos equivalentes em língua portuguesa que possam ser utilizados. O trecho abaixo, extraído do site do CERT.BR, trata-se de um documento que menciona as Práticas de Segurança para Administradores de Redes Internet. Este texto descreve uma seleção de boas práticas em segurança da informação no processo de configuração, administração e operação de redes conectadas à Internet e são direcionados aos profissionais de Segurança da Informação que lidam com controles e soluções técnicas de segurança. Da mesma maneira, alguns termos foram destacados com o intuito de ter um estudo mais aprofundado.

Figura 16- Trecho sobre Práticas de Segurança para Administradores de Redes Internet.



4.12.1. A Escolha de um *Firewall*

Existem diversas soluções de *firewall* disponíveis no mercado. A escolha de uma delas está atrelada a fatores como custo, recursos desejados e flexibilidade, mas um ponto essencial é a familiaridade com a plataforma operacional do *firewall*. A maioria dos *firewalls* está disponível para um conjunto reduzido de plataformas operacionais, e a sua escolha deve se restringir a um dos produtos que roda sobre uma plataforma com a qual os administradores da rede tenham experiência. Por exemplo, se você utiliza basicamente servidores Unix, é aconselhável que você escolha um *firewall* que rode sobre a sua variante favorita de Unix, e não um produto que requeira Windows NT.

Existem, basicamente, duas razões para esta recomendação. A primeira delas é que você deve estar familiarizado o suficiente com o sistema onde o *firewall* será executado para configurá-lo de forma segura. A existência de um *firewall* instalado em um sistema inseguro pode ser até mais perigosa do que a ausência do *firewall* na rede. A segunda razão é que os produtos tendem a seguir a filosofia da plataforma onde rodam; por exemplo, a maioria dos *firewalls* para Windows é configurada através de menus e janelas, ao passo que muitos *firewalls* para Unix são configurados por meio de arquivos texto.

Outro fator importante consiste na escolha do tipo de *firewall* que será implementado. Dentre os tipos atualmente disponíveis, destacam-se os filtros de pacotes, amplamente utilizados por terem baixo custo associado e por estarem normalmente integrados a dispositivos como roteadores ou alguns tipos de *switches*, ou por serem facilmente integráveis ou fazerem parte do *kernel* de diversos sistemas operacionais.

Fonte: site do CERT.BR[43]

[43] https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsubsec4.12.1

O quadro abaixo mostra a análise comparativa dos termos em inglês, a tradução literal dos termos:

Tabela 12 - Análise comparativa de termos em inglês da figura 16.

ANÁLISE DOS TERMOS DA FIGURA			
Termo em inglês	Tradução literal	Termo a ser utilizado em português	Definição
Firewall	Parede de Fogo	*Firewall*	*Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.*[44]
Switch	Comutador	*Switch*	*Um switch é um dispositivo de rede que conecta dispositivos utilizando endereços MAC anexados a cada uma de suas portas para que os dados sejam transmitidos diretamente aos destinatários dos dados.*[45]
Kernel	Núcleo	*Kernel / Núcleo*	*Núcleo do um sistema operacional de computador, que fornece serviços básicos para todas as outras partes do sistema operacional.*[46]

Fonte: elaborado pelo autor.

Isso mostra que a tradução literal de alguns termos não é benvinda nos textos técnicos destas áreas de conhecimento e, conforme mencionado por Barros (2004), o conhecimento dos termos é imprescindível para a confecção de traduções de boa qualidade. Um profissional da área, ao se deparar com materiais técnicos que, porventura, possuam uma tradução de baixa qualidade (feita por um tradutor com pouco ou nenhum conhecimento dos termos relacionados à Segurança da Informação ou ainda por métodos automatizados), por dedução, possivelmente, conseguirá compreender a mensagem. Entretanto, um indivíduo que não tenha o conhecimento prévio dos termos corretos que compõe o léxico da linguagem referente ao campo da Segurança da Informação, terá a compreensão da mensagem e, consequentemente, a absorção da informação, totalmente comprometida.

Apresento no apêndice desta pesquisa um glossário contendo termos relevantes para Segurança da Informação, que devem ser apropriados pelos usuários de informação e, com isso, diminuir a superfície e a possibilidade de ataques à segurança da informação.

[44] https://cartilha.cert.br/glossario
[45] [8] https://www.sans.org/security-resources/glossary-of-terms/

CONSIDERAÇÕES FINAIS

Esta pesquisa, em seu capítulo introdutório, mostrou que 2017 foi um ano dos maciços de *ransomware* e algumas empresas tiveram prejuízos na casa de US$ 300 milhões. Dispositivos de Internet das Coisas também foram atacados com o intuito de serem conectados em *botnets* para atuar em ações ilícitas. Em 2018, ocorreram ataques em cadeias de fornecimento e a utilização de Inteligência Artificial para ataques sofisticados de *spear phishing*[47].

Nos dias atuais, a situação não está diferente. A pandemia de Covid 19 triplicou o número de ataques cibernéticos a empresas privadas no mundo todo. Por conta da adoção generalizada e sem planejamento do regime de trabalho em home office, o crescimento expressivo do uso de comércio eletrônico e das transações bancárias pela internet, associado às vulnerabilidades de sistemas digitais de algumas empresas, contribuíram para o aumento de crimes digitais no Brasil e em outros países[48]. Entretanto, as vulnerabilidades de sistemas é apenas uma parte desta equação que pode ser somada às vulnerabilidades do fator humano. Vale ressaltar que o fator humano também pode ser um vetor de abertura de brechas em sistemas – seja pela negligência, ao executar ações que permitam exploração de vulnerabilidades (clicar em links de Internet e arquivos vindos de e-mails de origem desconhecida, por exemplo); seja pela omissão, ao deixar de executar ações de segurança (ao não aplicar *patches* e correções de segurança ou não trocar a senha padrão de seu roteador Wi-Fi, por exemplo).

Em ambos os casos, é importante valorizar o fator humano e colocá-lo em primeiro lugar nos objetivos estratégicos de segurança da informação. Educação, treinamento e conscientização de usuários é necessário para que as pessoas sejam hábeis ao lidar com as ameaças de segurança da informação e manusear os ativos de maneira segura dentro das organizações, mas também em duas vidas pessoais.

O estudo mostrou que a Segurança da Informação, em seu aspecto social, está relacionado com a Ciência da Informação. Ressaltou as diferenças e semelhanças em como a informação é manuseada, usando como exemplo a análise do ciclo de vida da informação em ambas as áreas de conhecimento.

---

[47] O cenário de ameaças cibernéticas para 2018 é complexo e assustador | CIO - https://cio.com.br/tendencias/o-cenario-de-ameacas-ciberneticas-para-2018-e-complexo-e-assustador/

[48] Ataques cibernéticos a empresas aumentam 300% na pandemia - ISTOÉ Independente (istoe.com.br) - https://istoe.com.br/ataques-ciberneticos-a-empresas-aumentam-300-na-pandemia/

A análise do domínio Segurança da Informação foi feita sob duas perspectivas: na primeira, o *framework* de cyber segurança do NIST apresentou as questões relacionadas à segurança da informação de infraestruturas críticas em forma de controles enviesado à tecnologia; na segunda, na certificação profissional CISSP do (ISC)², a segurança da informação foi mostrada de uma maneira ampla. A tríade "processos, pessoas e tecnologia" foi desmembrada em oito domínios de conhecimento (abordados nessa pesquisa como "subdomínios" da Segurança da Informação). Termos e conceitos importantes do domínio Segurança da Informação, que devem ser conhecidos por quem manuseia informações, surgem nessa análise, tais como: engenharia social, *phishing*, *malwares*, *ransomware* etc. Vale ressaltar que a análise deste domínio pode ser feita de outras formas, por exemplo: a partir de outros *frameworks,* de outras certificações profissionais com outras especificidades; de um subdomínio isolado, a partir das políticas de segurança da informação etc.

Nos estudos terminológicos do domínio Segurança da Informação, este domínio foi apresentado como uma Linguagem de Especialidade, um subsistema linguístico particular de um campo da experiência. A pesquisa mostrou aspectos da Terminologia na tradução de textos especializados. O levantamento bibliométrico efetuado mostrou que a produção cientifica de materiais relacionados à Segurança da Informação em língua inglesa é de 95%. Desta forma, o estudo mostrou que o conhecimento da língua inglesa, ainda que básico, é necessário para ter acesso a materiais de qualidade sobre o assunto – para os profissionais das áreas de Tecnologia da Informação e Segurança da Informação. Para usuários de informações em geral, este conhecimento é necessário no processo de conscientização em Segurança da Informação, principalmente, porque muitos termos necessários nesse processo para absorção deste. conhecimento não possuem tradução em língua portuguesa.

Os aspectos teóricos mostraram que a Teoria Comunicativa indicou que a Terminologia deve representar o conhecimento e sua transmissão deste. Entretanto, a Terminologia Sociocognitiva e sua unidade de entendimento mostrou que, além da dimensão linguística, é também necessário considerar aspectos discursivos e comunicativos. A Socioterminologia leva em conta diferentes tipos de situação de uso da língua e sua variação terminológica considerando o meio social. Desta forma, pesquisa mostrou que a Terminologia pode, de fato, contribuir no processo de conscientização em Segurança da Informação, porém aspectos sociais, cognitivos e comunicativos por parte de quem recebe esta informação devem ser considerados para que seja eficaz.

Por fim, como uma contribuição para esta pesquisa, o apêndice contém um glossário com alguns termos relacionados à Segurança da Informação e baseada no *Computer Security Resource Center*, do NIST, que podem ajudar na apropriação destes conceitos e conscientizar os usuários de seu importante papel neste processo.

REFERÊNCIAS

BARROS, L. A. **Curso básico de terminologia**. São Paulo: Edusp, 2004. p. 25-96.

BARROS, L. A. **Aspectos epistemológicos e perspectivas científicas da terminologia**. **Cienc. Cult.**, São Paulo, v. 58, n. 2, p. 22-26, junho 2006 Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252006000200011&lng=en&nrm=iso>. Acesso em 13/08/2020.

BESSA, V. H. **Teorias da Aprendizagem**. Curitiba: IESDE, 2011, 2ed.

BORKO, Harold. Information science: What is it? **American Documentation**, v. 19, n. 1, p. 3–5, 1968. Disponível em: <https://doi.org/10.1002/asi.5090190103>. Acesso em 13/09/2020.

CABRÉ, M. T. **La terminología: representación y comunicación**. Barcelona: Institut Universitari de Linguística Aplicada, Universitat Pompeu Fabra, 1999.

CAPURRO, R. **Epistemologia e Ciência da Informação**. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 5, Belo Horizonte, 2003. Anais... Belo Horizonte: UFMG, 2003. Disponível em: <www.capurro.de/enancib_p.htm>. Acesso em: 29/04/2020.

CHAPPLE, M; STEWART, J; GIBSON, D. **(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide**, Eighth Edition. Indianapolis: Sybex, 2016.

FABER, P. **The cognitive shift in terminology and specialized translation**. MonTI. Monografías de Traducción e Interpretación 1: 107-134, 2009

FAULSTICH, E. **Socioterminologia: mais que um método de pesquisa, uma disciplina**. Ciência da Informação, [S. l.], v. 24, n. 3, 1995. Disponível em: <http://revista.ibict.br/ciinf/article/view/566>. Acesso em: 1 Nov. 2021.

FAULSTICH, E. **A socioterminologia na comunicação científica e técnica**. Cienc. Cult., São Paulo, v. 58, n. 2, p. 27-31, 2006. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252006000200012&lng=en&nrm=iso>. Acesso em: 01 Nov. 2021.

FORTINET. **Insider Threat Report**, 2019. Disponível em: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf. Acesso em: 12 mai. 2020.

FREITAS, L. M.; ALBUQUERQUE, A. C. As abordagens da análise de domínio como aporte metodológico para a classificação arquivística. **Encontro Nacional de Pesquisa em**

Ciência da Informação, n. XVIII ENANCIB, 2017. Disponível em: http://hdl.handle.net/20.500.11959/brapci/105090. Acesso em: 31 out. 2021.

GARDNER, B; THOMAS, V. **Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition**, 2014. Disponível em: <https://www.researchgate.net/publication/291092430>. Acesso em 10/03/2021.

GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2006.

HARRIS, S; MAYMI, F. **CISSP All-in-One Exam Guide**. Seventh Edition. New York: McGraw-Hill Education, 2016.

HJØRLAND, B**. Domain Analysis: A Socio-Cognitive Orientation for Information Science Research**. Bul. Am. Soc. Info. Sci. Tech., 30: 17-21. 2004. Disponível em: https://doi.org/10.1002/bult.312. Acessado em 10/10/2021.

HJØRLAND, B. Domain analysis in information science: Eleven approaches - Traditional as well as innovative. **Journal of Documentation**, v. 58, n. 4, p. 422–462, 2002.

HJØRLAND, B; ALBRECHTSEN, H. Toward a new horizon in Information Science. **Journal of the American Society for Information Science**, p. 26, 1995.

LARA, M. **Uma teoria terminológica para um conceito contemporâneo de informação documentária**. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 6., 2005, Florianópolis. Anais... Florianópolis: UFSC, 2005. Disponível em: http://repositorios.questoesemrede.uff.br/repositorios/bitstream/handle/123456789/362/GT2_Lara.pdf?sequence=1. Acessado em 26/09/2021.

LE COADIC, Y.-F. **A ciência da informação**. 2. ed. Brasília: Briquet de Lemos/Livros, 1996.

MARCIANO, L. P. Segurança da Informação - uma abordagem social. **Cid/Face - Unb**, p. 212, 2006. Disponível em: <http://repositorio.unb.br/handle/10482/1943>. Acesso em 20/04/2020.

MARX, K. **O Capital**. Crítica da economia política. Vol. I, livro Primeiro, O processo de produção do Capital. Tomo I. cap. 1, item 1 e 2. p. 45-53;

MITNICK, K. D.; SIMON, W. L.; **A Arte de Enganar**. Editora Pearson, 2003.

NIELES, M; DEMPSEY, K; PILLITTERI, V. Yan. NIST SP800-12 Revision 1 : An introduction to information security. **NIST special publication**, n. 800–12 (draft) revision

1, 2017. Disponível em: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. Acesso em 09/02/2020.

NIST. **Cybersecurity Framework: An Introduction to the Components of the Framework**. 2021. Disponível em: https://www.nist.gov/cyberframework/online-learning/components-framework. Acesso em: 27 jun. 2021.

RICHET, J. From Young Hackers to Crackers. **International Journal of Technology and Human Interaction**. 9. 53-62, 2013.

ROCK CONTENT. **Quais são as redes sociais mais usadas no Brasil em 2019?** 2019. Disponível em: https://rockcontent.com/br/blog/redes-sociais-mais-usadas-no-brasil/. Acesso em: 26 jun. 2020.

SAGER, J.C. Prólogo: la terminología, ponte entre varios mundos. In: CABRÉ, M.T. **La terminología: teoría, metodología, aplicaciones**. Barcelona: Ed. Antártida; Empúries, 1993. p.11-17.

SCHNEIER, B. **Secrets and Lies: Digital Security in a Networked World**. Indianapolis: Wiley, 2004.

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

SRNICEK, N. **Capitalismo de Plataforma**. Buenos Aires: Caja Negra, p. 39-86, 2016.

SMIRAGLIA, R. P. The epistemological dimension of knowledge organization. **IRIS - Revista de Informação, Memória e Tecnologia**, v. 2, n. 1, p. 2-11, 2013. Disponível em: http://hdl.handle.net/20.500.11959/brapci/93381. Acesso em: 29 jan. 2022.

SMIRAGLIA, R. P. Epistemology of domain analysis. **Cultural frames of knowledge**, p. 111–124, 2012.

SARACEVIC, T. A natureza interdisciplinar da ciência da informação. **Ciência da Informação**, v. 24, n. 1, 11, 1995.

SARACEVIC, T. **Information Science: origin, evolution and relations**. [s.l.: s.n.], 1996.

SEVERINO, A. J. **Metodologia do Trabalho Científico**. 24. ed. São Paulo, Cortez, 2007.

TEMMERMAN, R. Questioning the univocity ideal. The difference between socio-cognitive Terminology and traditional Terminology. Hermes, Journal of Linguistics, 18: 51-90, 1997.

TEMMERMAN, R. (2000). ***Towards New Ways of Terminology Description: The Sociocognitive-Approach***. John Benjamins Publishing Company. https://doi.org/10.1075/tlrp.3, 2000.

TENNIS, J.T. **Two Axes of Domain Analysis**. Knowledge Organization, v. 30, n.3/4, p.191-195, 2003.

WE ARE SOCIAL. **Digital, Social Media, Mobile et E-Commerce,** 2019. Disponível em: https://wearesocial.com/blog/2019/01/global-digital-report-2019/. Acesso em: 26 jun. 2020.

APÊNDICE – GLOSSÁRIO

A lista de termos abaixo foi elaborada nos termos considerados relevantes no que tange conscientização de usuários em Segurança da Informação. A maioria dos termos foram utilizados na pesquisa, porém outros, que considerei relevantes, foram incluídos como forma de enriquecer a lista.

A definição dos termos foi baseada no *Computer Security Resource Center*, do NIST, mas com tradução nossa.

Os termos que possuem correspondência em língua portuguesa foram mencionados em língua portuguesa e com o respectivo termo em língua inglesa entre parênteses. Entretanto, nos casos em que os termos não possuem correspondente em língua portuguesa e são conhecidos apenas pelos nomes em língua inglesa, não há referência entre parênteses.

Ameaça (*Threat*)	Qualquer circunstância ou evento com potencial para explorar com êxito uma vulnerabilidade e impactar a adversamente a Confidencialidade, Integridade e/o Disponibilidade de algum tipo de ativo.
Assinatura digital (*Digital Signature*)	O resultado do uso de criptografia para autenticação de origem das informações; integridade de dados e o não repúdio da origem das informações.
Ataque (*Attack*)	Qualquer tipo de atividade maliciosa com o intuito de coletar, interromper, negar, degradar ou destruir ativos.
Ativo (*Asset*)	Qualquer dado, dispositivo, objeto ou componente que possua valor.
Autenticação em dois fatores (*Two-Factor Authentication*)	Autenticação usando dois ou mais fatores, que podem incluir: algo que você sabe (por exemplo, senha / número de identificação pessoal – PIN); algo que você possui (por exemplo, dispositivo de identificação criptográfica ou token); algo que você é (por exemplo, biometria).
Backdoor	É uma forma não documentada de obter acesso a um sistema de computador. Também é recurso utilizado por diversos malwares para garantir acesso remoto a um sistema, roteador, firewall ou uma rede de computadores.
Biometria (*Biometric*)	Características físicas ou traços pessoais de comportamento mensuráveis usados para identificar ou autenticar um indivíduo. Exemplos de biometria são as imagens faciais, impressões digitais e amostras de caligrafia.
Botnet	Rede de computadores que infectados por softwares maliciosos, podendo ser controlados remotamente, obrigando-os a enviar spam, espalhar *malwares* ou executar ataques de negação de serviços distribuído sem o conhecimento ou o consentimento dos seus donos.

Cavalo de Troia (*Trojan horse*)	Um programa de computador que parece ter uma função útil, mas também tem uma função oculta e potencialmente maliciosa, burlando mecanismos de segurança.
Classificação da dados (*Data Classification*)	A classificação de dados (ativos) é identificação dos tipos de dados que estão sendo processados e armazenados em um sistema de informação pertencente a uma organização ou operado por ela.[49]
Confidencialidade (*Confidentiality*)	Conceito que determina que a informação deve ser acessada apenas pelos sujeitos que tem esse direito.
Conscientização (*Awareness*)	Processo de aprendizagem que visa mudar atitudes individuais e organizacionais para perceber a importância da segurança e as consequências adversas quando não eficiente.
Cópia de segurança (*Backup*)	Cópia de arquivos e programas com o intuito de facilitar a recuperação, quando necessário.
Cracker	É um indivíduo que invade sistemas, burla processos ou violou intencionalmente sistemas de segurança, normalmente por intenções maliciosas ou para auferir lucro. O termo é considerado antiquado sendo, originalmente, proposto como sendo um antônimo ao termo hacker. Entretanto, essa distinção nunca ganhou força.
Criptografia (*Cryptography*)	A disciplina e a ciência de usar matemática para proteger informações e criar confiança, incorporando princípios, meios e métodos para a transformação de dados a fim de ocultar seu conteúdo semântico, prevenir seu uso não autorizado ou prevenir sua modificação.
Negação de serviço (*Denial of servic*e - DoS)	Ataque que visa tornar um sistema (serviço) indisponível (negado).
Disponibilidade (*Availability*)	Conceito que indica que as informações devem estar disponíveis para serem acessadas sempre que necessário.
Engenharia Social (*Social Engineering*)	Qualquer ato que influencie uma pessoa a realizar uma ação que pode ou não ser do seu melhor interesse.[50]
Firewall	Aplicativo ou dispositivo de conexão entre redes que restringe o tráfego de comunicação de dados entre duas redes conectadas.
Firmware	Programas de computador e dados armazenados em hardware de forma que os programas e dados não possam ser gravados dinamicamente ou modificados durante a execução dos programas.

[49] https://d1.awsstatic.com/whitepapers/compliance/PT_Whitepapers/AWS_Data_Classification.pdf
[50] The Official Social Engineering Hub - Security Through Education (social-engineer.org) - https://www.social-engineer.org/#:~:text=Security%20Through%20Education,-Learn%20how%20to&text=We%20define%20social%20engineering%20as,The%20Science%20of%20Human%20Hacking.

Framework	É uma série de processos documentados usados para definir políticas e procedimentos em torno da implementação e gerenciamento contínuo de controles de segurança da informação em um ambiente corporativo.[51]
Gerenciador de senhas (*Password Manager*)	Aplicativo de software desenvolvido para armazenar e gerenciar credenciais.
Hacker	Indivíduos que se dedicam a entender o funcionamento destes dispositivos, extrapolando os limites do funcionamento normal destes sistemas, conforme previstos por quem os projetou. Como desuso do termo cracker, passou a designar os criminosos cibernéticos.
Hardening	Um processo que visa eliminar meios de ataque corrigindo vulnerabilidades, aplicando patches ou correções de sistemas e através da desativação de serviços não essenciais ou não utilizados em sistemas.
Incidente (*Incident*)	Ocorrência que, realmente ou potencialmente, compromete a confidencialidade, integridade ou disponibilidade de um ativo ou ameaça iminente de violação de políticas de segurança.
Informação (*Information*)	Qualquer comunicação ou representação de conhecimento, como fatos, dados ou opiniões em qualquer meio ou forma, incluindo textual, numérico, gráfico, cartográfico, narrativo ou audiovisual.
Integridade (*Integrity*)	Conceito que visa a proteção contra modificação ou destruição indevida de informações e inclui a garantia do não repúdio e da autenticidade das informações.
Internet das Coisas (*Internet of Things*)	São os dispositivos conectados à Internet, além dos computadores, telefones e tablets. Integra também outros dispositivos que podem estar conectados, tais como: fechaduras, geladeiras, TVs, monitores de condicionamento físico etc.
LGPD (GDPR)	Lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[52]. A *General Data Protection Regulation* (GDPR) é a legislação equivalente, porém redigida e aprovado pela União Europeia (UE), impondo obrigações às organizações em qualquer lugar, desde que visem ou coletem dados relacionados a pessoas da UE.[53]
Malware	Hardware, firmware ou software destinado a executar um processo não autorizado que terá um impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema de informação. Um vírus, worm, cavalo de Tróia ou outra entidade baseada em código que infecta sistemas com finalidade maliciosa. Também conhecido por software malicioso.

[51] Top 7 IT security frameworks and standards explained (techtarget.com) - https://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one
[52] L13709 (planalto.gov.br) - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
[53] What is GDPR, the EU's new data protection law? - GDPR.eu - https://gdpr.eu/what-is-gdpr/

Não-repúdio (*Non- Repudiation*)	Conceito que visa garantir que o remetente não negue ter criado, assinado ou enviado determinada informação.[54]
Negação de serviço (*Denial of servic*e - DoS)	Ataque que visa tornar um sistema (serviço) indisponível (negado).[55]
Negação de Serviço Distribuído (*Distributed Denial of Service* - DDoS)	Ataque de negação de serviço executado através do uso de vários computadores.
Patch	Software de correção que, quando instalado, modifica diretamente os arquivos ou configurações do dispositivo relacionadas a um componente de software diferente, visando uma solução imediata para um problema identificado.
Phishing	Uma técnica de engenharia social usada para tentar induzir usuários a fornecer informações pessoais ou a executar ações (por exemplo, baixar e instalar software malicioso) para conseguir tais informações. Normalmente, o perpetrador se faz passar por uma empresa legítima ou por uma pessoa de boa reputação.
Privacidade (*Privacy*)	Garantia de que a confidencialidade e o acesso a certas informações sobre uma pessoa física ou jurídica estejam devidamente protegidos.
Ransomware	É um tipo de malware que impede ou limita os usuários de acessar seu sistema, seja bloqueando a tela do sistema ou bloqueando os arquivos dos usuários até que o resgate (*ransom*) seja pago.[56]
Risco (*Risk*)	O nível de impacto nas operações organizacionais, ativos organizacionais ou indivíduos resultantes da operação de um sistema de informação, dado o impacto potencial de uma ameaça e a probabilidade de ocorrência dessa ameaça.
Roteador (*Router*)	Dispositivo que determina o melhor caminho para encaminhar um pacote de dados para seu destino.
Segurança Cibernética (*Cybersecurity*)	Prevenção de danos, proteção e restauração de computadores, sistemas de comunicações eletrônicas, serviços de comunicações eletrônicas, comunicação com fio e comunicação eletrônica, incluindo as informações neles contidas, para garantir sua disponibilidade, integridade, autenticação, confidencialidade e não-repúdio.

[54] Segurança da Informação (tjam.jus.br) - https://consultasaj.tjam.jus.br/WebHelp/id_seguranca_da_informacao.htm#:~:text=N%C3%A3o%20rep%C3%BAdio%3A%20visa%20garantir%20que,de%20forma%20retroativa%20no%20tempo.

[55] Negação de Serviço – Linha Defensiva - https://linhadefensiva.org/2005/06/01/negacao-de-servico/#:~:text=O%20termo%20nega%C3%A7%C3%A3o%20de%20servi%C3%A7o%20%28%20Denial%20of,de%20%E2%80%9Cnega%C3%A7%C3%A3o%20de%20servi%C3%A7o%E2%80%9D%20a%20consequ%C3%AAncia%20de%20

[56] Ransomware - Definition (trendmicro.com) - https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Segurança da Informação (*Information Security*)	A proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer confidencialidade, integridade e disponibilidade.
SPAM	Mensagens contendo lixo eletrônico ou abuso de sistemas de mensagens eletrônicas para enviar mensagens em massa não solicitadas de maneira indiscriminada.
Spear phishing	Termo usado para descrever qualquer ataque de *phishing* altamente direcionado a um indivíduo ou organização específicos.
SSID	Nome atribuído a um ponto de acesso sem fio que permite às estações distinguir um ponto de acesso de outro.
Switch	Um dispositivo que direciona os dados de entrada de qualquer uma das portas de entrada múltiplas para a porta de saída específica que levará os dados para o destino desejado.
Worm	Um malware autorreplicante que pode ser executado de forma independente, propagando uma versão funcional completa de si mesmo em outros computadores em uma rede e consumir recursos do computador de forma destrutiva.
Vírus (*Virus*)	Malware que se propaga infectando outro programa. Um vírus não pode funcionar sozinho; requer que seu programa hospedeiro seja executado para tornar o vírus ativo.
VPN	Rede virtual construída sobre as redes existentes que pode fornecer um mecanismo de comunicação seguro para transmissão de informações.
Vulnerabilidade (*Vulnerability*)	Fraqueza em um sistema de informações, procedimentos de segurança do sistema, controles internos ou implementação que podem ser explorados ou acionados por uma ameaça.