UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
ENGENHARIA E GESTÃO DO CONHECIMENTO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA E GESTÃO DO CONHECIMENTO

Maria Isabel Araújo Silva dos Santos

A SEGURANÇA DO SEGREDO: PROPOSTA DE *FRAMEWORK* DE APLICAÇÃO DOS INSTRUMENTOS DE PROTEÇÃO DO SEGREDO NO AMBIENTE DE INOVAÇÃO DA BASE INDUSTRIAL DE DEFESA

Tese submetida ao Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, da Universidade Federal de Santa Catarina para a obtenção do Grau de Doutora em Engenharia e Gestão do Conhecimento.
Orientador: Prof. Dr. Luiz Otávio Pimentel
Coorientadora interna: Profa. Dra. Gertrudes Aparecida Dandolini
Coorientador externo: Prof. Dr. Edgard Costa Oliveira

Florianópolis
2016

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Santos, Maria Isabel Araújo Silva dos
A Segurança do Segredo : Proposta de Framework de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da Base Industrial de Defesa / Maria Isabel Araújo Silva dos Santos ; orientador, Luiz Otávio Pimentel ; coorientadora, Gertrudes Aparecida Dandolini, coorientador, Edgard Costa Oliveira. - Florianópolis, SC, 2016.
307 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós Graduação em Engenharia e Gestão do Conhecimento, Florianópolis, 2016.

Inclui referências.

1. Engenharia e Gestão do Conhecimento. 2. Proteção do Conhecimento. 3. Ambiente de Inovação. 4. Base Industrial de Defesa. I. Pimentel, Luiz Otávio . II. Dandolini, Gertrudes Aparecida. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento. IV. Titulo.

Maria Isabel Araújo Silva dos Santos

A SEGURANÇA DO SEGREDO: PROPOSTA DE *FRAMEWORK* DE APLICAÇÃO DOS INSTRUMENTOS DE PROTEÇÃO DO SEGREDO NO AMBIENTE DE INOVAÇÃO DA BASE INDUSTRIAL DE DEFESA

Esta tese foi julgada adequada para obtenção do Título de "Doutor" e aprovada na sua forma final pelo Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento.

Florianópolis, 29 de fevereiro de 2015.

_____

Prof. Roberto Carlos dos S. Pacheco, Dr.
Coordenador do Curso

Banca Examinadora:

_____

Prof. Luiz Otávio Pimentel, Dr.
Orientador
Universidade Federal de Santa Catarina

_____

Prof.ª Gertrudes Aparecida Dandolini, Drª,
Coorientadora interna
Universidade Federal de Santa Catarina

Prof. Edgard Costa Oliveira, Dr.
Coorientador externo
Universidade de Brasília

Prof., Dr. Aires Rover
Universidade Federal de Santa Catarina

Prof., Dr. João Artur de Souza
Universidade Federal de Santa Catarina

Prof., Dr. Jordan Paulesky Juliani
Universidade do Estado de Santa Catarina

Paulo Sergio Pagliusi, Ph.D
Information Systems Audit and Control Association

Carlos Alberto Pittaluga Niederauer, Dr.
Conselho Nacional de Desenvolvimento Científico e Tecnológico

Dedico este trabalho ao meu esposo Rubens, às minhas filhas Amanda e Beatriz, à minha irmã Ilza, aos meus pais Carlos *in memorian* e Anália, e ao meu genro Tiago.

AGRADECIMENTOS

Agradeço à Deus que me sustentou para que eu chegasse até aqui.

Destaco a importância desses anos de pesquisa e aprendizado na Universidade Federal de Santa Catarina que resultaram no meu amadurecimento profissional e pessoal, além de construir sólidas pontes de conhecimento e abrir portas para novos saberes e descobertas.

No período que estive em *Floripa*, pessoas "queridas", como se diz na ilha, me acolheram com carinho e me fizeram sentir em casa. Agradeço a D. Zilda, a Bete e o Sérgio, e demais membros dessa linda família do Campeche.

Agradeço às pessoas que marcaram o início da minha caminhada do doutoramento, principalmente ao Almirante Ilques Barbosa Junior pelo privilégio do apoio e a confiança que recebi para iniciar meu curso de doutorado. Agradeço o incentivo que recebi dos amigos que fiz durante a trajetória da "Ciência, Tecnologia e Inovação"; ao Comte De Negri, SO Bispo, Comte Monnerat, e SG Daniele.

Agradeço ao professor Pimentel, meu orientador e mestre querido, com suas sábias orientações – verdadeiras flechas no alvo, pela compreensão, incentivo, oportunidades de crescimento, confiança e amizade. À professora Gertrudes pela amizade, incentivo, coorientação desta pesquisa e dos trabalhos que participei no IGTI.

Ao professor e amigo Edgard pela coorientação, palavras de incentivo e exortações essenciais para a conclusão desta pesquisa, por sua amizade, compreensão e dedicação.

Ao professor João Artur pela amizade, competência, e conhecimentos que incorporei à minha formação como pesquisadora.

Ao professor Cristiano, que além dos ensinamentos em metodologia e liderança, me gratificou com sua amizade, sabedoria, conselhos, e acolhida no LGR. Ao professor Ricardo Custódio, do LabSEC/UFSC, por seus conselhos e exemplo. Agradeço aos professores do EGC que nas disciplinas ministradas transmitiram os conhecimentos e contribuíram para a fundamentação deste trabalho.

Agradeço aos meus amigos de caminhada acadêmica no Grupo de Pesquisa em Propriedade Intelectual, Transferência de Tecnologia e Inovação – GPITTI. Agradeço à preciosidade da amizade da Cristiani Fontanela e da Jaqueline Albino, que vai além das fronteiras da UFSC.

Por fim, agradeço aos amigos e familiares que me acompanharam e oraram para meu sucesso.

Muito obrigada!

No momento em que eles falaram, eu ia escrever, mas ouvi uma voz do céu que dizia: — Guarde em segredo o que os sete trovões disseram.

(Apocalipse 10:4)

RESUMO

A Base Industrial de Defesa representa um conjunto de organizações públicas e privadas, civis e militares, que participam das etapas de pesquisa, desenvolvimento, produção, distribuição, e/ou manutenção de produtos de Defesa. Essas organizações são intensivas em conhecimento, pois utilizam o conhecimento como base das suas atividades, e o incorporam aos produtos, caracterizados pela alta tecnologia agregada. Algumas vulnerabilidades no setor, tais como: pouca participação da sociedade brasileira nos assuntos de Defesa; a escassez de especialistas civis; a necessidade de modernização e inovação tecnológica; gestão dos Direitos de Propriedade Intelectual; compensação comercial, industrial e tecnológica e outras. Aqui, a Gestão do Conhecimento ressalta a diferença no trato do bem tangível e intangível, pois nos processos do ambiente de inovação da Defesa, que envolvem alta tecnologia, a preocupação com a perda de conhecimento deve pautar as atividades de compartilhamento do conhecimento. Outra razão, o fomento à Inovação no Ambiente da BID implica a diminuição da dependência tecnológica estrangeira, devendo-se proteger a novidade do produto. Neste estudo, recorreu-se aos fundamentos de Inteligência e Contra-Inteligência da Doutrina de Inteligência de Defesa para qualificar o conhecimento de Defesa e identificar instrumentos próprios de proteção deste conhecimento. Esta tese elaborou um *framework* para representar a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação a BID, detalhando as dimensões de proteção do segredo e a matriz de aplicação dos instrumentos de proteção. Para isso, foi necessário harmonizar um conjunto de termos e definições para caracterizar o "segredo" no Ambiente de Inovação da BID; identificar os instrumentos de proteção; apresentar o Sistema Sociotécnico para a BID para entender as influências entre subsistema técnico e o subsistema social, bem como as relações com o ambiente externo; caracterizar o Ambiente de Inovação da BID, considerando a atuação dos agentes de Ciência, Tecnologia e Inovação, e os ciclos de vida dos produtos de Defesa de cada Força Armada.

Palavras-chave: Gestão do Conhecimento. Inovação. Segredo Instrumentos de Proteção Intelectual. Segurança do Conhecimento. Segurança do Segredo. Conhecimento de Defesa. Base Industrial de Defesa. *Framework.*

ABSTRACT

The Industrial Defense Base (IDB) represents a group of public and private, civil and military organizations that participate in the research, development, production, distribution, and / or maintenance stages of Defense products. These organizations are knowledge intensive, as they utilize knowledge as the basis of their activities, incorporating it into products characterized by highly aggregate technology. Vulnerabilities in this sector arise from issues related to low participation of Brazilian society in Defense matters, the scarcity of civilian specialists, the need for modernization and technological innovation, management of Intellectual Property Rights, Commercial, industrial and technological compensation, and others. Knowledge Management, in this instance, highlights the difference in the treatment of tangible and intangible goods, as in the innovation processes related to Defense, which involve advanced technology, the concern with the loss of knowledge should guide the activities of knowledge sharing. Moreover, the promotion of innovation in the IDB's environment decreases dependence in foreign technologies, as the product's novelty must be protected. In this study, we relied on the fundamentals of Intelligence and Counterintelligence in the Defense Intelligence Doctrine in order to qualify the concept of Defense knowledge and to identify proper instruments for the protection of this knowledge. This thesis developed a framework to represent the application of the instruments for the protection of secrets in the IDB's Innovation Environment, detailing the dimensions of secrets protection and the application matrix for the protection instruments. To achieve this objective, it was necessary to harmonize a set of terms and definitions in order to characterize the "secret" in the IDB's Innovation Environment; to identify the instruments of protection; to present the IDB's Sociotechnical System and understand the influences between technical and social subsystems, as well as their relations with the external environment; to characterize the IDB's Innovation Environment, considering the actions of the Science, Technology and Innovation agents, and the life cycles of the Defense products of each of the Armed Forces.

Keywords: Knowledge Management. Innovation. Secret. Instruments of Intellectual Protection. Knowledge Security. Security of the Secret (Secret's Security). Knowledge of Defense. Industrial Defense Base. Framework.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABIMDE - Associação Brasileira das Indústrias de Materiais de Defesa e Segurança
ABIN - Agência Brasileira de Inteligência
ABNT - Associação Brasileira de Normas Técnicas
AID - Atividade de Inteligência de Defesa
AM-X - Projeto para modernizar as aeronaves AM-X
APF - Administração Pública Federal
BDTD - Banco Digital Nacional de Teses e Dissertações
BID - Base Industrial de Defesa
BLD - Base Logística de Defesa
BRIC - Países do bloco Brasil, Rússia, Índia e China
CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CASNAV - Centro de Análises de Sistemas Navais
CCEMSP - Centro de Coordenação de Estudos em São Paulo
CDS - Complexo da Defesa e da Segurança
CEPSH - Comitê de Ética em Pesquisa com Seres Humanos
CHM - Centro de Hidrografia da Marinha
CI – Contra-Inteligência
CIT - Células de Inovação Tecnológicas
CMID - Comissão Mista da Indústria de Defesa
CMiD - Conselho Militar de Defesa
COMAER - Comando da Aeronáutica
COMASSE - Comissão Assessora de Ciência e Tecnologia para a Defesa
Comdefesa - Departamento da Indústria de Defesa
COMISCEMEFA - Comissão de Implantação do Sistema de Certificação, Metrologia, Normalização, e Fomento Industrial das Forças Armadas
CONDOP - Condicionantes Doutrinários Operacionais
CoPS - *Complex Product Systems*
CPI - Código da Propriedade Intelectual
CTECCFN - Centro Tecnológico do Corpo de Fuzileiros Navais
CTEx - Centro Tecnológico do Exército
CTMSP - Centro Tecnológico da Marinha em São Paulo
DCN - Declaração de Conteúdo Nacional
DCT - Departamento de Ciência e Tecnologia do Exército
DCTA - Departamento de Ciência e Tecnologia Aeroespacial
DIB - *Defense Industrial Base*

DID - Doutrina de Inteligência de Defesa
DPI - Direitos de Propriedade Intelectual
DPP - Declaração de Processo Produtivo
EBSCOHOST - *Online Research Database EBSCO*
ED - Empresas de Defesa
EED - Empresas Estratégicas de Defesa
EGN - Escola de Guerra Naval
EJIS - *European Journal of Information Systems*
EMA - Estado Maior da Armada
EMCFA - Estado-Maior Conjunto das Forças Armadas
END - Estratégia Nacional de Defesa
ESG - Escola Superior de Guerra
EVTE - Estudo de Viabilidade Técnico-econômica
FA - Forças Armadas
FIESP - Federação das Indústrias do Estado de São Paulo
FINEP - Financiadora de Estudos e Projetos
FIRJAN - Federação das Indústrias do Estado do Rio de Janeiro
GC - Gestão do Conhecimento
GIT - Gerência de Inovação Tecnológica
GR - Gestão de Riscos
GSI/PR - Gabinete de Segurança Institucional da Presidência da República
HNMD - Hospital Naval Marcílio Dias
HRM - Human Resource Management
IAE - Instituto de Aeronáutica e Espaço
ICT - Instituição Científica, Tecnológica e de Inovação
IEAPM - Instituto de Estudos do Mar Almirante Paulo Moreira
IEAv - Instituto de Estudos Avançados da Aeronáutica
IES - Instituição de Ensino superior
IFI - Instituto de Fomento e Coordenação Industrial
IME - Instituto Militar de Engenharia
INPI - Instituto Nacional de Propriedade Industrial
IPC - Instituto Pandiá Calógenas
IPEV - Instituto de Pesquisas e Ensaios em Voo
IPqM - Instituto de Pesquisas da Marinha
ISJ - *Information Systems Journal*
ISR - *Information System Research*
ISTA - *Information Science & Technology Abstracts*
ITA - Instituto Tecnológico de Aeronáutica
JIC - *Journal of Intellectual Capital*
JKM - *Journal of Knowledge Management*

JMIS - *Journal of Management Information Systems*
KC-390 - Projeto para construção de uma aeronave de transporte militar e reabastecimento em voo
KIBS - *Knowledge Intensive Business Services*
KMRP - *Knowledge Management Research and Practice*
KPM - *Knowledge and Process Management*
LAI - Lei de Acesso à Informação
LBDN - Livro Branco de Defesa Nacional
LFM - Laboratório Farmacêutico da Marinha
LO - *The Learning Organization*
MB - Marinha do Brasil
MCTI - Ministério da Ciência Tecnologia e Inovação
MD - Ministério da Defesa
MDIC - Ministério do Desenvolvimento, Indústria e Comércio Exterior
MEM - Material de Emprego Militar
MISQ - *Management Information Systems Quartely*
MPC - Método para a Produção do Conhecimento
MRE - Ministério das Relações Exteriores
NBR - Normas Técnicas da Associação Brasileira de Normas Técnicas
NIT - Núcleo de Inovação Tecnológica
NIT-MB - Núcleo de Inovação Tecnológica da Marinha
OIC - Organizações Intensivas em Conhecimento
OMC - Organização Mundial do Comércio
OMPI - Organização Mundial de Propriedade Intelectual
P&D - Pesquisa e Desenvolvimento
PAED - Plano de Articulação e Equipamento de Defesa
PBCT - Plano Básico de Ciência e Tecnologia
PBE - Prática Baseada em Evidências
PCTI - Política de Ciência, Tecnologia e Inovação para a Defesa Nacional
PD&I - Pesquisa, Desenvolvimento e Inovação
PDCA - *Plan-Do-Check-Action*
PDCTM - Plano de Desenvolvimento Científico-Tecnológico e de Inovação da Marinha
PDN - Política de Defesa Nacional
PDP - Política de Desenvolvimento Produtivo
PED - Produto Estratégico de Defesa
PI - Propriedade Intelectual
PIB - Produto Interno Bruto
PME - Pequenas e Médias Empresas
PNID - Política Nacional da Indústria de Defesa

PNPC - Programa Nacional de Proteção ao Conhecimento
PPGD - Programa de Pós-Graduação em Direito
PPGEGC - Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento
PPGEGC/UFSC - Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina
PRODE - Produto de Defesa
PROQUEST - *Databases, EBooks and Technology Research*
PWR - *Pressurized Water Reactor*
RAP - Relatório de Análise de Patentes
REPROTEC - Relatório de Prospecção Tecnológica
RETID - Regime Especial Tributário para a Indústria de Defesa
RFI - *Request for Information*
RID - Relatório de Inovações Desejáveis
ROB - Requisitos Operacionais Básicos
ROI - *Return on Investment*
RTB - Requisitos Técnicos Básicos
RTLI - requisitos técnicos, logísticos e industriais
SCOPUS - Base de dados bibliográfica da Elservier
SCTA - Sistema de Ciência e Tecnologia da Aeronáutica
SCTEx - Sistema de Ciência e Tecnologia
SCTMB - Sistema de Ciência, Tecnologia e Inovação da Marinha
SD - Sistema de Defesa
SecCTM - Secretaria de Ciência, Tecnologia e Inovação da Marinha
SEG ATV - Segurança Ativa
SEG ORG - Segurança Orgânica
SEPROD - Secretaria de Produtos de Defesa
SGSI - Sistema de Gestão de Segurança da Informação
SIBRATEC - Sistema Brasileiro de Tecnologia
SINDE - Sistema de Inteligência de Defesa
SIPLEx - Sistema de Planejamento do Exército
SIPRI - *Stockholm International Peace Research Institute*
SisCaPED - Sistema de Cadastramento de Produtos e Empresas de Defesa
SISCEMEFA - Sistema de Certificação, Metrologia, Normalização, e Fomento Industrial das Forças Armadas
SISCOMIS - Sistema de Comunicações Militares por Satélite
SisCTID - Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa
Sisfron - Sistema Integrado de Monitoramento de Fronteiras
SisGAAz - Sistema de Gerenciamento da Amazônia Azul

SISLOGD - Sistema de Logística e Mobilização de Defesa
SisMiCat - Sistema Militar de Catalogação das Forças Armadas
SISTED - Sistema de Comunicações Militares Seguras
SLA - *Service Level Agreement*
SN-BR - Submarino Nuclear Brasileiro
SSM - *Soft System Methodology*
TCU - Tribunal de Contas da União
TICs - Tecnologia da Informação e Comunicações
TLE - Termos de Licitação Especial
UFSC - Universidade Federal de Santa Catarina
USP - Universidade de São Paulo
VANT-FAB - Projeto para desenvolver veículos aéreos não tripulados
WIPO - *World intellectual property Organization*

SUMÁRIO

1 INTRODUÇÃO

O recurso mais valioso da sociedade contemporânea é o conhecimento e não mais a terra e o capital, como na sociedade industrial. Vivenciamos uma sociedade intensiva no uso das Tecnologias da Informação e Comunicações (TICs), e apesar de existir uma divergência conceitual sobre o nome da atual sociedade, alguns autores consideram sociedade da informação e sociedade do conhecimento termos sinônimos, como Demo (2000), enquanto outros as diferenciam traçando uma abordagem evolutiva, como Araújo (2009) ao afirmar que a informação serve como insumo para o conhecimento, e que a Sociedade da informação proporcionou a evolução para a sociedade do conhecimento.

Assim como este autor, acreditamos na afirmação da UNESCO (2005)[1] que percebe a sociedade da informação baseada nas descobertas tecnológicas que favorecem o uso adequado e diferenciado das massas de dados, e a sociedade do conhecimento atuando como instrumento de bem-estar individual e comunitário de dimensões sociais, éticas e políticas. Adotamos nesta pesquisa o termo sociedade da informação e do conhecimento por acreditar que tanto o conhecimento como a informação caracterizam a nova sociedade.

É certo que as TICs revolucionaram o cenário econômico e social contemporâneo e facilitaram o reconhecimento da importância da informação e do conhecimento, além de agir como impulsionadoras de mudanças nos processos de gestão e de produção nas organizações. As informações são coletadas, processadas, armazenadas e transmitidas em diferentes formatos (eletrônico, físico e verbal), e possuem um valor para o negócio, assim como possuem riscos, que podem impactar negativamente o negócio da organização.

Neste sentido, o valor da informação ultrapassa os limites tangíveis e codificados e passa para a esfera do intangível e interconectado, que também possui riscos e deve ser protegido, conforme a citação:

> O valor da informação vai além das palavras escritas, números e imagens: conhecimento,

[1] "A sociedade do conhecimento contribui para o bem-estar dos indivíduos e das comunidades, e abrange dimensões sociais, éticas e políticas. Por outro lado, a sociedade da informação, é baseada nas descobertas tecnológicas que tentam fornecer pouco mais do que 'uma massa de dados distintas' para aqueles que não têm as habilidades para se beneficiar dela" (UNESCO, 2005, p.1).

> conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização, e consequentemente, requerem proteção contra vários riscos. (NBR ISO/IEC 27002, 2013b, p. x).

Nas práticas da Administração e da Economia, observamos que a sociedade da informação e do conhecimento impôs às organizações o domínio da administração de seus ativos intelectuais para que pudessem sobreviver e se sustentar em um ambiente competitivo e globalizado da economia moderna.

Bem e Junior (2006, p.1) acrescenta que a vantagem do conhecimento como matéria prima difere do ativo tangível, que diminui na medida em que é utilizado, pois o conhecimento só aumenta quando é utilizado, dividido ou compartilhado, o que o torna um "recurso infinito, que pode trazer grandes vantagens, principalmente em longo prazo".

Aumentar o uso do conhecimento com a prática da gestão implica na ordenação do fluxo de informações na organização, e a tecnologia sozinha não basta para suportar essas necessidades demandadas: é preciso considerar o conhecimento no seu contexto, para que o valor deste seja ressaltado e tenha importância para os ganhos da organização. Neste contexto, Santos e Souza (2010) nos despertam para a necessidade do entendimento de como trabalhar aplicando tratamentos adequados aos novos paradigmas cujos objetos são a informação e conhecimento de valor, e nos orienta que:

> Para lidar com o grande fluxo de informações, não basta disponibilizar diversas tecnologias da informação, é preciso criar um ambiente propício a trabalhar com foco no conhecimento, com estratégias e procedimentos suportados por sistemas adequados aos problemas enfrentados. É recomendável que os sistemas baseados em conhecimento, capazes de interagir com o conhecimento disponível e selecionar conhecimentos de valor ou, ainda, gerar conhecimentos de valor circunstanciado, apenas sejam introduzidos quando seus resultados

> puderem gerar ganhos significativos para a organização. SANTOS e SOUZA (2010, p.271).

Ainda no sentido do aumento do uso do conhecimento, North (2010) enfatiza como "recurso-chave da era Pós-Industrial" três conceitos que sustentam o saber produtivo e que estão em evolução, e são reciprocamente dependentes. O primeiro, a mudança estrutural rumo a uma sociedade do conhecimento, representa uma migração estrutural das atividades intensivas em trabalho e capital para as tarefas intensivas em informação e conhecimentos, onde as empresas "vendem cada vez mais informações, conhecimentos, produtos e serviços inteligentes", e possuem diferentes formas organizacionais e novos papéis para os gestores e os trabalhadores. O segundo, a globalização da economia modifica a divisão internacional do trabalho, e faz as nações industriais se tornarem "nações sábias", acelerando os processos de aprendizagem internacional, e fazendo novos competidores em períodos de tempo mais curto. Por último, as TICs aceleram o fluxo de informação a nível mundial e com baixo custo, resultando em "mudanças de mercado muito mais rápidas e a uma velocidade de inovação maior, que se manifestam na queda de preços, ciclos de vida mais curto do produto, individualização das necessidades dos clientes e nascimento de novos campos de negócios" North (2010, p. 14-15)

Isso colabora para o pensamento de que o conhecimento e a informação mudaram paradigmas e revelaram novas estruturas e padrões para a sociedade e seus segmentos.

Devemos tratar o conhecimento como uma informação valiosa proveniente da mente humana, que contém reflexão, síntese e contexto (DAVENPORT, 1998).

Nonaka e Takeushi, (1997) relatam que estudos realizados em empresas japonesas mostraram que a organização de negócios tanto "processa" o conhecimento quanto o "cria". Assim, a criação do conhecimento organizacional é compreendida como a capacidade da empresa em criar conhecimento, disseminá-lo na organização e incorporá-lo a produtos, serviços e sistemas (NONAKA e TAKEUSHI, 1997).

Nas empresas modernas, o poder econômico e de produção não estão nos seus ativos imobilizados, como: terra, instalações e equipamentos (TOFFLER, 1990; DRUCKER, 1994), mas, nos ativos intangíveis, como o conhecimento, que é capaz de desenvolver e

incorporar inovação aos produtos, processos e serviços (FONTANELA e SANTOS, 2015).

Devemos também enfatizar as informações que circulam, ou que deveriam circular, nos processos da organização e identificar os conhecimentos que são necessários para a boa execução dos processos ou para promover a inovação.

Segundo Santos e Souza (2010), três questões importantes precisam ser observadas:

a) "Sobre o valor da informação e do conhecimento cabe destacar que "estruturalmente, toda informação é expressão do conhecimento, porém, não são todas as informações ou os conhecimentos expressos que são considerados valorosos em uma dada circunstância".
b) "Para um observador externo, "o conhecimento valioso se manifesta em ações ou atividades também valiosas, de acordo com as circunstâncias".
c) "(...) há conhecimentos valorosos que ainda não foram expressos como informação passível de ser comunicada, mas que é pressentido ou imaginado em atitudes ou atividades" (SANTOS e SOUZA, 2010, p.276-277).

Reis (2008, p.48), ao afirmar que a "inovação depende da estratégia de gestão", alerta para a necessidade do alinhamento às estratégias de negócios, da prospecção tecnológica, da capacidade de antecipar necessidades, de gerir os riscos e ameaças, da escolha dos parceiros estratégicos, e de outras práticas de gestão e governança.

As empresas são diferenciadas com base naquilo que sabem, cabendo ao conhecimento a capacidade da vantagem competitiva (DAVENPORT e PRUSAK, 2003).

Neste contexto, as organizações cada vez mais incluem na gestão de seus ativos os bens intangíveis, com a possibilidade de proteção jurídica para sustentar a agregação de valor científico e tecnológico de seus produtos e serviços, porque na economia do conhecimento, ter capital intelectual é ter riqueza. Quando utilizada estrategicamente, a PI, que faz parte do capital intelectual, permite aos seus titulares uma posição vantajosa no mercado. A semelhança de produtos e serviços das empresas poderia confundir os consumidores e usuários, por isso a necessidade de proteger os bens intangíveis por regimes jurídicos de propriedade intelectual, alcançando a exclusividade de mercadorias e o diferencial de serviços. (PIMENTEL, 2010).

A “pesquisa e o desenvolvimento devem ser direcionados para atender às necessidades humanas e desta forma cumprir um importante papel no desenvolvimento social e tecnológico do país” (BOCCHINO et al., 2010, p. 15).

Cabe à Gestão do Conhecimento (GC) desempenhar a coordenação sistemática de pessoas, tecnologias, processos e estrutura organizacional, com o objetivo de agregar valor à organização por meio do uso e reuso de conhecimentos e da inovação (DALKIR, 2011), tornando-a importante para a estratégia organizacional, pois gera a vantagem, produtividade e desenvolvimento para a organização.

Desta mesma maneira, o conhecimento científico e tecnológico se associa ao conhecimento como fator de competitividade e gerador de inovação e desenvolvimento, ao mesmo tempo em que, destaca a velocidade de perda ou ganho do valor econômico do conhecimento, conforme Cardori (2013):

> O conhecimento científico e tecnológico é um dos principais fatores que determina a competitividade entre os diferentes setores produtivos, as empresas e os países, podendo gerar inovação e, consequentemente, desenvolvimento.
> Pode-se dizer que uma das principais evidências da economia baseada no conhecimento incide na aceleração, sem precedentes, com que o conhecimento é criado, acumulado e, até mesmo, na velocidade com que se torna obsoleto e perde valor econômico. CARDORI (2013, p. 43).

A literatura também aponta que a proteção do conhecimento pode ser considerada uma atividade da GC (DAVENPORT, 1998; GOLD, MALHOTRA e SEAGARS, 2001; LUCAS 2010; MAIER 2007). Esta atividade observa critérios para mitigar o uso inadequado, o roubo do conhecimento, os incentivos para proteção, o uso de tecnologia, estabelecimento de políticas e procedimentos para proteção do conhecimento, e outros. (GOLD, MALHOTRA e SEAGARS, 2001).

Sabe-se que a Propriedade Intelectual “decorre diretamente da capacidade inventiva ou criadora do intelecto humano (conhecimento, tecnologia e saberes) de seus criadores”, porém, os Direitos de Propriedade Intelectual não representam o “único meio de proteção ao conhecimento”, pois existem outros instrumentos, como por exemplo: *Know How*, o segredo de negócio e o tempo de liderança sobre competidores. Assim, urge “uma gestão eficiente dos instrumentos de

proteção de propriedade intelectual e dos demais instrumentos, com a finalidade de promover a atividade econômica e estimular a inovação tecnológica" (WIPO/OMPI/INPI, 2015, p. 5 e 7).

Deste modo entendemos que o conhecimento que assegura vantagem competitiva, por intermédio da inovação, necessita de proteção. Dadas as peculiaridades de cada ambiente organizacional e os interesses dos *stakeholders,* cabe identificar os instrumentos de proteção e segurança do conhecimento mais adequados.

O Brasil é um país de dimensão continental que tem buscado vencer os desafios econômicos e sociais contemporâneos, e tem conquistado "mais espaços políticos, exercido maiores influências e conquistado novos mercados, 'perturbando' países de maior poder". A soberania do Brasil se sustenta na existência de uma "confiável base industrial, logística, científica e tecnológica de defesa" que preparam as Forças Armadas para assegurar a defesa nacional. "Nenhum país pode abrir mão de saber e de poder fabricar seus próprios meios de defesa" (CUNHA e AMARANTE, 2011, p.14 -15).

Os diversos normativos de Defesa empregam diferentes nomes para se referirem a Base Industrial de Defesa, por exemplo: a Estratégia Nacional de Defesa (END) utiliza "Indústria Nacional de Material de Defesa"; a Política de Desenvolvimento Produtivo (PDP) refere-se ao "Programa Complexo Industrial de Defesa"; o Sistema Brasileiro de Tecnologia (SIBRATEC) chama de "Complexo Industrial de Defesa". Neste trabalho adotamos a denominação do Ministério da Defesa (MD) e da Política Nacional da Indústria de Defesa (PNID), que chamam de "Base Industrial de Defesa" (BID), e está definida como:

> Base Industrial de Defesa – BID: é o conjunto das empresas estatais e privadas, bem como organizações civis e militares, que participem de uma ou mais das etapas de pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos estratégicos de defesa (BRASIL, 2005b, p. 1)

Os estudos sobre a BID envolvem aspectos da Defesa Nacional e Soberania. A BID incorpora o Complexo da Defesa e da Segurança (CDS)[2], que no ano de 2014 representou aproximadamente R$ 202

[2] O Complexo da Defesa e da Segurança considerou as atividades de Defesa e Segurança, as Indústrias, os Insumos e os Serviços e Distribuição.

bilhões, ou seja, 3,7% do Produto Interno Bruto (PIB) do Brasil (ABIMDE e FIPE, 2015, p.2).

Muta (2014) afirma que a BID fomenta serviços intensivos em conhecimentos com a produção e fabricação de seus produtos estratégicos, que demandam conhecimentos específicos e processos de inovação continuada, pois são executados pelo próprio corpo técnico da BID e "não são conhecimentos que estarão normalmente disponíveis no mercado". Também ressalta que há necessidade do amadurecimento no trato com o intangível para o desenvolvimento social e econômico do país, conforme citação:

> Somos pouco acostumados ao intangível. Sem negligenciar a importância dos produtos industrializados – já em clara crise de crescimento – para o desenvolvimento social e econômico do País, é fundamental dar continuidade à criação dos caminhos do conhecimento, e viabilizar efetivamente a sua aplicação – utilizando-se inclusive de ativos que contribuam para a construção da perenidade e do protagonismo da nação. MUTA (2014, p.38).

Encontramos a definição para Produto Estratégico de Defesa (PED) na PNID, como:

> Produto Estratégico de Defesa: são bens e serviços que pelas peculiaridades de obtenção, produção, distribuição, armazenagem, manutenção ou emprego possam comprometer, direta ou indiretamente, a consecução de objetivos relacionados à segurança ou à defesa do País. (BRASIL, 2005b).

Pimentel (1999) afirma que "a tecnologia tem papel fundamental na economia, como um dos fatores da produção, conjunto que contém os elementos indispensáveis ao processo produtivo de bens capazes de satisfazer as necessidades ou desejos da sociedade" (PIMENTEL, 1999, p. 111-112)

Sobre a Economia de Defesa, o mercado de produtos de Defesa é monopsônico, onde o Estado é o principal comprador, embora exista um mercado internacional de produtos de Defesa controlado pelo Estado e seja de seu interesse promover as vendas e capacitar as empresas da BID,

em harmonia com o objetivo do programa estruturante do Complexo Industrial de Defesa: “recuperar e incentivar o crescimento da base industrial instalada, ampliando o fornecimento para as Forças Armadas brasileiras e exportações” (FRANCO-AZEVEDO, 2013; BRASIL, 2008a).

A seguir descrevemos o problema de pesquisa.

1.1 DESCRIÇÃO DO PROBLEMA

A END ressalta que na Estrutura de Defesa são encontradas vulnerabilidades (BRASIL, 2008b, p. 42-45); algumas delas são:

- Pouco envolvimento da sociedade brasileira.
- Escassez de especialistas civis; descontinuidade orçamentária.
- Obsolescência dos equipamentos das Forças Armadas e dependência de produtos de defesa estrangeiros.
- Insuficiência de cursos para a capacitação de civis.
- Incipiente integração entre os órgãos militares de pesquisa, e destes com os institutos civis de pesquisa.
- Inexistência de planejamento nacional para o desenvolvimento de produtos com a participação dos centros de pesquisa militares e civis.
- Bloqueios tecnológicos impostos por países que dominam a tecnologia.
- Cláusula de compensação comercial, industrial e tecnológica (*off-set*) inexistente em alguns contratos de importação de produtos de defesa, ou mesmo a não-participação efetiva da indústria nacional em programas de compensação. (BRASIL, 2008b, p. 42-45)

A precariedade dos equipamentos das FA, a necessidade de modernização dos equipamentos e produtos utilizados pelas FA, a capacidade de ter produtos de defesa adequados para fazer frente às ameaças aos interesses de Defesa Nacional, nos remete ao fortalecimento da BID com as condições seguras para inovar em seu ambiente de produção e atender as demandas das FA.

O fomento à Inovação no Ambiente da BID implica a diminuição da dependência tecnológica estrangeira. Para isso, se faz necessário

proteger a novidade no Ambiente de Inovação da BID, ou seja, utilizar instrumentos de proteção do segredo no Ambiente de Inovação da BID.

Contribuir na discussão acadêmica sobre o processo de desenvolvimento de produtos, o sistema de produção dos produtos de defesa, o ciclo de vida dos produtos, os ambientes de CT&I das FA e os projetos estratégicos nos leva ao entendimento sobre o ambiente de inovação e do desenvolvimento dos produtos da BID.

No segmento da BID, segundo palavras do Presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE), na reunião da Comissão de Relações Exteriores e Defesa Nacional, existem diferenças na forma de produção dos bens tangível e intangível. Também ressalta a importância da GC nos processos que envolvem alta tecnologia, e a preocupação com a perda de conhecimento, conforme citação:

> Alta tecnologia não é igual à mineração. Na mineração você extrai o minério. Se não dá para extrair, você para de extrair. Quando volta a energia, você liga a máquina e extrai o minério. Com o petróleo é a mesma coisa; o petróleo está lá. Com a tecnologia, não. Ela desaparece. É a gestão do conhecimento. O conhecimento faz o *fading*, isto é, ele se esvanece se não houver continuidade. As pessoas saem da indústria de defesa e vão para o banco, ou vão fazer algo no comércio. (BRASIL, 2015b, p. 12).

A despeito da BID contar com um conjunto de empresas cujos serviços e produtos fornecidos são intensivos em conhecimento, poucos trabalhos acadêmicos foram encontrados nas Bases de Teses e Dissertações da CAPES e do IBICT.

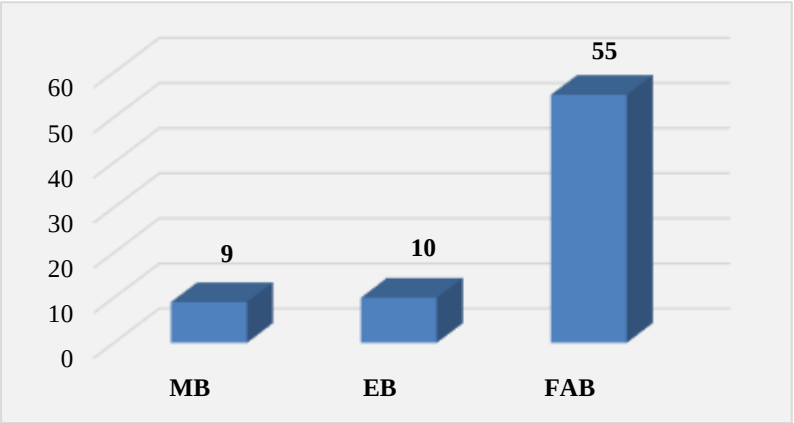
As buscas realizadas nessas bases utilizando os argumentos de pesquisa *Segurança do Segredo* não encontrou registro nas bases. A repetição da busca, com os argumentos *Defesa Nacional*, *Indústria de Defesa*, *Base Logística de Defesa e Base Industrial de Defesa* revelou que as discussões dos pesquisadores se concentram na área da Ciência Política, no tema Defesa Nacional. Nova busca realizada com os argumentos *Indústria de Defesa*, *Base Logística de Defesa e Base Industrial de Defesa*, retornou oito registros, sendo uma tese e sete dissertações. Porém, nenhum dos trabalhos publicados abordou a proteção do Conhecimento ou instrumentos de proteção, ou melhor, nenhum conceito próximo à proteção do segredo, como proteção do

conhecimento, segurança do conhecimento, proteção da informação ou segurança da informação.

Assim, ficou registrado o pouco envolvimento da academia nos assuntos de Defesa Nacional e da BID, a ausência de estudos interdisciplinares, e pouca massa crítica para os assuntos de Defesa e BID.

Os poucos pedidos de registro de patentes depositados no Instituto Nacional de Propriedade Industrial (INPI) pelas Forças Armadas, conforme apresentado no Gráfico 1, pode indicar a aplicação de outros instrumentos de proteção do conhecimento, ou que as informações estejam sob a proteção de sigilo previsto na lei para os assuntos de interesse da Defesa Nacional.

Gráfico 1 - Depósito de pedidos de patentes solicitados pelas FA (1982-2010).



Fonte: Galvão-Netto, 2011, p.5.

Neste contexto, o que se torna evidente para esta pesquisa é que diante da complexidade que envolve a BID e seu ambiente de inovação, bem como sua importância para o desenvolvimento econômico do país, necessitamos conhecer mais sobre o seu ambiente de inovação e como proteger o segredo nesse ambiente, garantindo a novidade para a Inovação.

Assim, o problema de pesquisa desta tese reside na ausência de uma forma sistematizada, ou melhor, um *framework* que represente a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID.

Diante do problema descrito, formulamos as seguintes questões:

a) Quais são os conceitos que permeiam a segurança do segredo?
b) Quais são os instrumentos de proteção que podem ser usados para o segredo no Ambiente de Inovação da BID?
c) Quais são as características do Ambiente de Inovação da BID?
d) Há um *framework* que represente a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID?

A questão de pesquisa formulada para esta tese é *Como aplicar os instrumentos de proteção do segredo no ambiente de inovação da BID?*

1.2 OBJETIVOS

Com o propósito de responder as questões de pesquisa, foram estabelecidos os objetivos geral e específicos.

1.2.1 Objetivo Geral

O objetivo geral é propor o *framework* de aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID.

1.2.2 Objetivos Específicos

Os seguintes objetivos específicos foram formulados para alcançar o objetivo geral:

- Apresentar um conjunto de termos e definições e harmonizá-los para a definição do termo “segredo” no Ambiente de Inovação da BID.
- Apresentar o Sistema Sociotécnico para a BID para entender as influências entre subsistema técnico e o subsistema social, bem como as relações com o ambiente externo.
- Caracterizar o Ambiente de Inovação da BID, considerando a atuação dos agentes de C,T&I, as fases de produção e ciclos de vida dos produtos de Defesa de cada FA.

- Elaborar um *framework* que represente a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação a BID.

1.3 JUSTIFICATIVA E INEDITISMO

A vivência profissional de mais de trinta anos da pesquisadora em órgãos da Administração Pública Federal (APF), como: as diversas organizações de nível estratégico e especializado da Marinha do Brasil; Gabinete de Segurança Institucional da Presidência da República (atual Casa Militar da Presidência da República); e Instituto Nacional de Tecnologia da Informação da Casa Civil da Presidência da República, permitiu perceber a importância da proteção do *segredo* e a carência de uma sistemática para protegê-lo.

Várias políticas e normativos instruem quanto à segurança da informação, que está explicitada em documentos e armazenada em repositório de dados. O Departamento de Segurança da Informação e Comunicações da Casa Militar da Presidência da República (DSIC) tem disponibilizado normativos e capacitações para a implementação de ações de segurança da informação e comunicações na APF. O Programa Nacional de Proteção ao Conhecimento (PNPC) da Agência Brasileira de Inteligência (ABIN) busca desenvolver a cultura de proteção, sensibilizar sobre as ameaças da espionagem econômica, apresentar cuidados básicos de proteção e interagir com órgãos detentores de conchecimento sensíveis. Porém, a capilaridade dessas ações nem sempre chega ao nível do conhecimento e permanece no nível da informação.

Com base nessa experiência e nos conhecimento auferidos ao longo do curso no Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento (PPGEGC), a pesquisadora identificou a oportunidade de contribuir para os estudos na área da proteção do conhecimento ao avançar para a proteção do segredo na área de Defesa, e propor o *framework* que orienta a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID.

O problema de pesquisa surgiu ao se constatar que nos poucos trabalhos acadêmicos sobre BID, alguns sobre a questão da inovação, nenhum deles abordou a questão da proteção sob quaisquer aspectos no ambiente de inovação de Defesa. Daí a oportunidade de desenvolver uma pesquisa sobre a proteção do *segredo* no Ambiente de Inovação da BID, que trata com conhecimentos tecnológicos e de alto valor estratégico.

Cabe ao pesquisador contribuir para a sistematização e avanço do conhecimento na área de pesquisa, ao identificar, produzir, integrar, e

compartilhar as experiências e conhecimento sobre o tema. Assim, os motivos que justificam esta pesquisa são a contribuição para sistematizar a aplicação de instrumentos de proteção em um ambiente de inovação, e sua abordagem interdisciplinar para os estudos de Defesa.

A revelância da pesquisa está no aumento da participação da academia nos estudos de Defesa.

Constatou-se o ineditismo do tema por meio de revisão da literatura em buscas realizadas nas bases de teses e dissertações da CAPES e do IBICT; o argumento de pesquisa *Segurança do Segredo* não encontrou registro nas bases.

Os argumentos *Defesa Nacional*, *Indústria de Defesa*, *Base Logística de Defesa e Base Industrial de Defesa* revelou que as discussões dos autores se concentram na área da Ciência Política e no tema Defesa Nacional. Foram encontrados 6 teses e 38 dissertações.

Para os argumentos *Indústria de Defesa, Base Logística de Defesa e Base Industrial de Defesa*, houve retorno de oito registros, sendo uma tese e sete dissertações. Nenhum dos trabalhos publicados abordou a proteção do Conhecimento ou instrumentos de proteção, ou melhor, nenhum conceito próximo à proteção do segredo.

A não trivialidade deste trabalho foi verificada nas ações de investigação, que se deu em áreas de conhecimento pouco estudadas, propondo contribuir na discussão de novos conceitos e suas relações; e na consideração da complexidade de análise de informações coletadas de forma diversa (pesquisa bibliográfica e documental e outras fontes).

No contexto geral da proteção do conhecimento, os autores evidenciaram a dificuldade existente na adoção dos mecanismos de proteção do conhecimento por diversas razões. Gonçalves (2012) concluiu que os pesquisadores não estão sensibilizados para a proteção do conhecimento, que o processo de patenteamento é percebido como algo complexo, burocrático e moroso, e a falta de preparo das pessoas para o exercício das funções. Jacinto (2008) destacou a necessidade de identificação do conhecimento como patrimônio organizacional e a adequada proteção mantendo os princípios para sua criação e disseminação, e acrescentou que:

> Existe a predominância da abordagem tecnológica para o tratamento da proteção do conhecimento em detrimento da organização de processos institucionais e envolvimento das pessoas no contexto de proteção do conhecimento. A carência de informações para o tratamento da proteção do

> conhecimento no âmbito da GC com foco não tecnológico. (JACINTO, 2008, p.168).

Nos trabalhos acadêmicos publicados sobre Defesa foi possível perceber que se trata de um tema complexo e raramente discutido, embora exista uma chamada formal para a participação da academia desde 2008, como publicado na END:

> Promover maior integração e participação dos setores civis governamentais na discussão de temas ligados à defesa, assim como a participação efetiva da sociedade brasileira, **por intermédio do meio acadêmico** e de institutos e entidades ligados aos assuntos estratégicos de defesa. (BRASIL, 2008b, p.58).

No desenvolvimento desta tese foram submetidos trabalhos, de autoria e co-autoria, sobre os temas pesquisados, tais como: inovação, proteção do conhecimento, e Defesa, que foram aceitos para apresentação e publicados em anais e periódicos científicos:

- ***Open innovation and protection of intellectual property rights in national wind farms***, no III Congresso Internacional de Eficiência Energética, Sistemas de Inovação Climática e Desenvolvimento Sustentável – Florianópolis/SC.
- **A proteção dos ativos intangíveis em organizações de inovação aberta**, no Congresso Nacional do Conselho Nacional de Pesquisa e Pós-Graduação em Direito - **XXIII Congresso Nacional** do CONPEDI – UFPB (ISBN: 978-85-5505-015-2).
- **Habitats de inovação aberta: a gestão do conhecimento nos parques científicos e tecnológicos**, Congresso Nacional do Conselho Nacional de Pesquisa e Pós-Graduação em Direito. – XXIV Encontro Nacional do CONPEDI – UFS (ISBN: 978-85-5505-050-3).
- **Mapeamento das Teses e Dissertações Brasileiras sobre Defesa Nacional e Indústria de Defesa**, Encontro Nacional da Associação Brasileira de Estudos de Defesa - VIII Encontro Nacional da ABED – Brasília/DF.
- A gestão do segredo na inovação aberta, Cadernos de Prospecção - ISSN 1983-1358. (print), 2317-0026

(online), 2015, vol.8, n.2, p.246-254, D.O.I.: 10.9771/S.1983-1358.2015.008.028. VII Encontro Acadêmico de Propriedade Industrial, Inovação e Desenvolvimento (ENAPID) – Salvador/BA.

- **Gestão e Segurança do Conhecimento no Âmbito da Defesa**, I Encontro Regional da Associação Brasileira de Estudos de Defesa da região Centro-Oeste - I ERABED-CENTRO-OESTE. Brasília/DF.
- *A case study of policies for brazilian defense technologies, 25th International Conference for Management of Technology (IAMOT 2016)* - (aprovado o abstract para apresentação) – Orlando/EUA.

Tais aceitações motivaram a continuidade da pesquisa, pois evidenciaram o interesse por parte das entidades promotoras em divulgar os artigos, caracterizando, também a oportunidade no avanço de estudos acadêmicos nestas áreas.

1.4 ESCOPO

Esta tese de doutoramento, cujo objetivo é propor um *framework* que oriente a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID, tem seu escopo delimitado na abrangência da BID. Por esta razão, centrou-se nos instrumentos de proteção disponíveis nas áreas de conhecimento da ciência da informação e das ciências sociais aplicadas.

Desse modo, não são foco deste estudo os mecanismos de proteção disponibilizados pela ciência da computação ou das ciências exatas.

Esta pesquisa limitou-se ao estudo da proteção do segredo no Ambiente de Inovação da BID.

1.5 ADERÊNCIA AO PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA E GESTÃO DO CONHECIMENTO (PPGEGC/UFSC)

O Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, da Universidade Federal de Santa Catarina (PPGEGC/UFSC) possui três áreas de concentração: a Gestão do Conhecimento (GC), a Engenharia do Conhecimento (EC), e a Mídia e Conhecimento (MC), e apresenta como proposta basilar a promoção de

estudos multidisciplinares englobando diferentes disciplinas na busca de um objetivo, e tem como missão a promoção do "ensino, pesquisa e extensão, de forma interdisciplinar, sobre o conhecimento como elemento agregador de valor para a sociedade" (PPEGC, 2016).

A forma interdisciplinar do PPGEGC/UFSC encontra conformidade nas orientações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES, 2013), que em seu "Documento de Área" ressalta a importância da área Interdisciplinar na Pós-Graduação diante da complexidade, diversidade de problemas de diferentes naturezas, e novas realidades que requerem um olhar diferenciado, mesclando saberes entre disciplinas e áreas de conhecimentos próximas e não próximas, conforme citação:

> A importância da introdução de uma área Interdisciplinar no contexto da Pós-graduação, em 2008, decorreu da necessidade de se dar conta de novos problemas que emergem no mundo contemporâneo, de diferentes naturezas e com variados níveis de complexidade, muitas vezes decorrentes do próprio avanço dos conhecimentos científicos e tecnológicos.
> A natureza complexa de tais problemas requer diálogos não só entre disciplinas próximas, dentro da mesma área do conhecimento, mas entre disciplinas de áreas diferentes, bem como entre saberes disciplinar e não disciplinar. Daí a relevância de novas formas de produção de conhecimento e formação de recursos humanos, que assumam como objeto de investigação fenômenos que se colocam entre fronteiras disciplinares. Diante disso, desafios teóricos e metodológicos se apresentam para diferentes campos de saber. (CAPES, 2013, p. 11).

Esta tese é interdisciplinar porque envolve elementos que são objetos de estudo e análise em diferentes áreas. Apoia-se nos conhecimentos das Engenharias, das Ciências Sociais Aplicadas e Humanas ao estudar a proteção do segredo no Ambiente de Inovação da BID. Como parte de uma pesquisa desenvolvida dentro do PPGEGC, e de acordo com Pacheco (2014a) pode-se dizer que esta tese utiliza o conhecimento em um "ciclo de criação coletiva de valor" envolvendo os processos de GC nas diferentes fases da gestão produtiva da BID, e com

a participação de diferentes atores e disciplinas, sendo as disciplinas de base e as correlatas apresentadas abaixo:

a. Direito: propriedade intelectual.
b. Administração: teoria geral; gestão da inovação; gestão de processos.
c. Engenharia de Produção: sistemas de produção.
d. Ciência da Informação: segurança da informação; classificação da informação.
e. Ciência Política: políticas; Defesa Nacional.

A tese se identifica com o PPGEGC/UFSC ao tratar o "conhecimento como fator central de agregação de valores organizacionais e posicionamento da GC, EC e MC como interdisciplinas" (PACHECO, 2014b). Alinha-se às pesquisas desenvolvidas sobre Conhecimento Organizacional, nas temáticas de GC & Inovação (PACHECO, 2014a), visto que estuda o conhecimento em um ambiente de inovação. A pesquisa trabalha conceitos relacionados à GC nas organizações, tais como: conhecimento, inteligência, inovação, proteção do conhecimento e propriedade intelectual; e utiliza as técnicas da EC para formalização e análise de processos intensivos em conhecimento.

O contexto de aplicação do objeto desta tese são as organizações, públicas e privadas, que compõem a BID, que têm como pilar o conhecimento, nas suas atividades e nos seus produtos, conhecidas como organizações intensivas em conhecimento.

Os temas que referenciam essa tese foram estudados por ex-discentes do PPGEGC, conforme o Quadro 1:

Quadro 1 – Trabalhos relacionados ao tema do PPGECG

Autor	Título	Nível	Ano
Roberta Moraes de Bem	*Framework* de gestão do conhecimento para bibliotecas universitárias.	D	2015
Isamir Machado de Carvalho	A dinâmica dos mecanismos de proteção e compartilhamento de conhecimento, no processo de desenvolvimento de software, em uma empresa pública de tecnologia da informação (TI).	D	2014

(Continuação Quadro 1)

Autor	Título	Nível	Ano
Aluizia Aparecida Cardori	A gestão do conhecimento aplicada ao processo de transferência de resultados de pesquisa de instituições federais de ciência e tecnologia para o setor produtivo: processo mediado pelo núcleo de inovação tecnológica.	D	2013
Leslie de Oliveria Bocchino	Proteção legal do conhecimento organizacional: uma abordagem de padrões de projeto.	T	2012
Jéssica Romeiro Mota	A proteção do conhecimento resultante da parceria de pesquisa, desenvolvimento & inovação originado da relação universidade e empresa.	M	2011

Fonte: Elaborado pela autora (2016).

As teses de Carvalho (2014) e Bocchino (2012) se relacionam ao abordar aspectos de proteção para o conhecimento organizacional. Carvalho (2014) tratar a proteção do conhecimento como parte do processo de compartilhamento do conhecimento, e Bocchino (2012) trata dos aspectos legais da proteção do conhecimento. A Dissertação de Mota (2011) por tratar a questão da proteção do conhecimento no âmbito das parcerias estabelecidas para o desenvolvimento e transferência de conhecimento de produtos inovadores. A Tese de Cardori (2013) por tratar a questão da transferência do conhecimento tecnológico resultante das atividades de Pesquisa e Desenvolvimento (P&D) que agrega valor aos produtos. A tese de Bem (2015) por utilizar o framework como ferramenta para compreensão de áreas multi e interdisciplinares.

O estudo aborda temáticas de GC, Inovação, Propriedade Intelectual, segredo industrial, *Frameworks*, BID, Gestão de Riscos, Inteligência e Contra-Inteligência, associando-os e aprofundando-os com a finalidade de propor o *framework* de aplicação dos instrumentos de proteção do segredo no ambiente de inovação da base industrial de defesa.

1.6 METODOLOGIA

A partir do entendimento de que a pesquisa é um "processo formal e sistemático de desenvolvimento do método científico", que tem por objetivo "descobrir respostas mediante o emprego de procedimentos científicos" (GIL, 1999, p.42), e sendo a ciência a "um conjunto de proposições logicamente correlacionadas sobre o comportamento de certos fenômenos que se deseja estudar" (LAKATOS e MARCONI , 2007, p. 80), esta pesquisa classifica-se como pesquisa aplicada.

Assim, com natureza de pesquisa aplicada busca trazer novos conhecimentos sobre a proteção do conhecimento para a área da Gestão do Conhecimento e para os estudos de Defesa ao propor o *framework* que sistematiza os instrumentos de proteção e segurança do segredo no Ambiente de Inovação da BID.

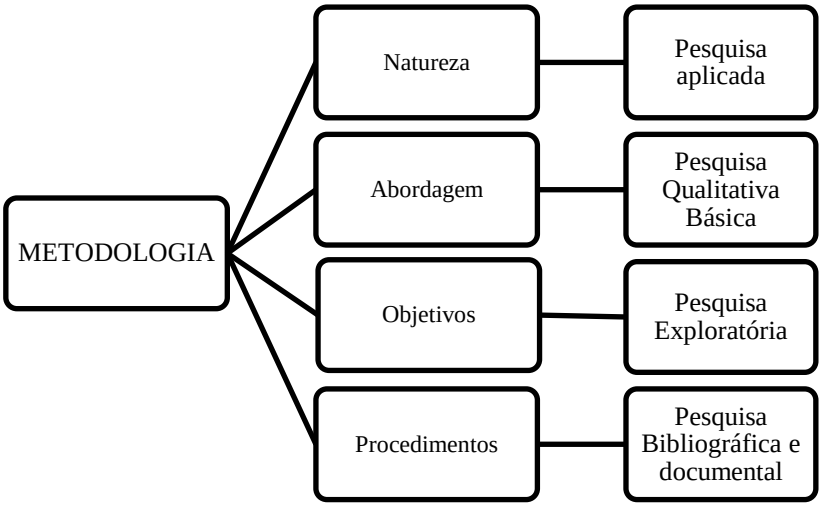
A metodologia, segundo Creswell (2010), aponta que a abordagem da pesquisa envolve a intersecção de filosofia, abordagens da investigação e de métodos específicos. Sendo assim, esta pesquisa adotou como concepção filosófica a do *construtivismo social* e construímos o significado interpretando as interações endógenas e exógenas, as políticas, regulações e instrumentos que operam no Ambiente de Inovação da BID. Isto possibilitou, indutivamente, desenvolver uma sistemática para a aplicação dos instrumentos de proteção e segurança do segredo no Ambiente de Inovação da BID.

Quanto à abordagem, classifica-se como pesquisa qualitativa básica, onde se buscou descobrir e entender a aplicação dos instrumentos de proteção do segredo no ambiente de inovação para a BID. A coleta de dados se deu pela análise de documentos, que foram indutivamente analisados para identificar padrões e temas comuns, e apresentou um relato descritivo dos resultados encontrados, discutindo-os à luz das referências bibliográficas. (MERRIAM, 1992, p. 7)

Quanto aos objetivos, trata-se de uma pesquisa exploratória que teve o objetivo de entender a aplicação de instrumentos de proteção do segredo no ambiente de inovação para a BID. Assim, o procedimento adotado foi a pesquisa bibliográfica em material já publicado.

A Figura 1 sintetiza a metodologia aplicada nesta pesquisa.

Figura 1 – Metodologia



Fonte: Elaboração da autora, 2015, com base em Merriam (1992); Gil (1999); Lakatos e Marconi (2007).

1.7 ESTRUTURA DA TESE

Neste capítulo introdutório, o capítulo 1, apresentamos a descrição do problema; a questão de pesquisa; o objetivo geral e os objetivos específicos; a justificativa e o ineditismo; o escopo; a aderência ao PPGEGC; a metodologia; e por fim, apresentamos a estrutura geral da tese.

O capítulo 2 apresenta a fundamentação teórica. A seção 2.1 inicia com conceitos e definições básicas sobre informação e conhecimento, e avança para a aplicação do conhecimento na organização, a Gestão do Conhecimento e o artefato de conhecimento. A seção seguinte apresenta a visão governamental para o trato do conhecimento sensível, destacando os aspectos principais do Programa Nacional de Proteção ao Conhecimento. A seção 2.3 refere-se à informação e ao conhecimento no âmbito da Defesa, que é assunto da Doutrina de Inteligência de Defesa. A seção 2.5 apresenta como aspectos da segurança e proteção a Gestão de Riscos; a Proteção dos Direitos de Propriedade Intelectual; a Segurança e Proteção da informação e do conhecimento; e o ramo da Contra-Inteligência para a segurança e proteção da informação e do

conhecimento de Defesa. A Seção 2.5 apresenta conceitos e definições da Inovação. A última seção apresenta um conjunto de definições e conceitos para o termo “segredo”.

O capítulo 3 apresenta os procedimentos metodológicos seguidos na pesquisa.

O capítulo 4 responde o primeiro objetivo específico de harmonização de termos e definições para o ambiente de estudo, como: “informação de Defesa”, “conhecimento de Defesa”, e “Segredo”.

O capítulo 5 responde o segundo objetivo específico proposto e apresentar o Sistema Sociotécnico elaborado para a BID.

O capítulo 6 responde o terceiro objetivo específico, com um estudo sobre o ambiente de inovação da BID e a elaboração de um modelo de produção para o ambiente de inovação da BID.

O capítulo 7 apresenta a proposta do *framework* de aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID. A seção 7.1 apresenta as etapas de construção do *framework*; a Seção 7.2 resgata a teoria apresentada nos capítulos anteriores; a seção 7.3 define as dimensões de proteção do segredo; a seção 7.4 apresenta os instrumentos de proteção do segredo; a seção 7.5 apresenta a matriz de aplicação dos instrumentos de proteção do segredo conforme as dimensões de proteção; a seção 7.6 detalha as macro atividades que compõe do *framework*.

As conclusões e as recomendações para pesquisas futuras estão no capítulo 8.

Para finalizar esta tese e melhor ilustrar a pesquisa, tem-se no anexo o extrato da Doutrina de Inteligência de Defesa.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a fundamentação teórica da tese. Organizamos este capítulo em seis seções.

A primeira seção introduz terminologias, conceitos e características dos termos *informação* e *conhecimento*, que serviram de conceitos iniciais para posterior caracterização e definição do *segredo*. Também fundamenta a aplicação do conhecimento no contexto da organização. Outro termo conceituado nesta seção é o artefato de conhecimento.

A segunda seção trata do conhecimento sensível, objeto do Programa Nacional de Proteção o Conhecimento.

A terceira seção apresenta características, terminologias e conceitos da informação e do conhecimento no âmbito da Defesa. Traz conceitos da Inteligência, presentes na Doutrina de Inteligência Militar, para explicar como se produz informações e conhecimentos na área de Defesa. O anexo contém outras definições utilizadas no ramo de Inteligência e na Doutrina de Inteligência de Defesa (DID).

A quarta seção apresenta os principais aspectos da segurança e proteção da informação e do conhecimento, e faz referência à Gestão de Riscos, à Proteção dos Direitos de Propriedade Intelectual, a segurança e proteção da informação e do conhecimento, incluindo os de Defesa que são tratados pela Contra-Inteligência.

A quinta seção conceitua Inovação e a última seção traz conceitos e definições sobre segredo e a legislação pertinente.

2.1 DA INFORMAÇÃO AO CONHECIMENTO

Informação e Conhecimento são termos próximos, que inicialmente foram tratados por áreas de conhecimento distintas. O primeiro pelas Ciências Exatas, “sendo tratada como um conceito matemático para definir a comunicação”, e o segundo pela Filosofia, Sociologia e Ciências Humanas (SIRIHAL e LOURENÇO, 2002, p. 1-4).

Após o avanço das TIC e a ascensão da informação e do conhecimento, “como recursos econômicos fundamentais”, a informação e o conhecimento tornaram-se objeto da mesma área, ou seja, da Ciência da Informação, e marcou o surgimento do termo *dado* (SIRIHAL e LOURENÇO, 2002, p. 1-2).

O termo *dado* pode ser definido como “conjunto de registros qualitativos ou quantitativos conhecido que organizado, agrupado,

categorizado e padronizado adequadamente transforma-se em informação (MIRANDA, 1999), ou como "representação de fatos, conceitos ou instruções de maneira formalizada e adequada para a comunicação, interpretação ou processamento por seres humanos ou por equipamentos eletrônicos" (NBR-11515, 2007). North (2010, p. 34) entende que dado é resultado da transformação de signos (letras, números, e outros signos) por meio de regras de ordenação de código ou sintaxe; os dados são símbolos não interpretados. Arís et al. (2007, p. 54) entende *dado* como um valor discreto que descreve um evento do mundo, não está estruturado, não diz nada sobre o porquê das coisas, nem sobre sua interpretação ou propósito.

Posto que, a Ciência da Informação deu enfoque social à informação, Wiener (1970, p. 27) afirma que a teoria social da informação trouxe a nova proposta para a informação "como um problema de processo, e não como um problema de armazenagem". Neste contexto, Alvarenga Neto (2005) considera importante a discussão epistemológica e conceitual para termos informação e conhecimento, que são considerados fatores-chave da competitividade organizacional, e onde "as definições de dado, informação e conhecimento são marcos teóricos conceituais iniciais e primordiais balizadores das formulações, proposições e discussões atinentes às organizações do conhecimento e à gestão da informação e do conhecimento" (ALVARENGA NETO, 2005, p. 32).

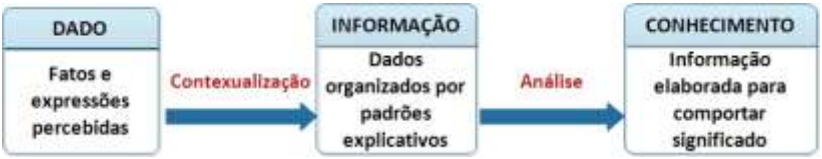
Observando estes termos sob uma perspectiva hierárquica, como apresentado na Figura 2, encontramos unanimidade de conceitos nos três níveis iniciais: dado, informação e conhecimento (ILVONEN, 2013; THIERAUF, 2001; AWAD e GHAZIRI, 2004; HISLOP, 2005). Outros autores aceitam esses três níveis e acrescentam outras etapas na pirâmide.

Figura 2 – Representação Hierárquica

Fonte: Elaboração da autora, 2015, com base em Ilvonen (2013); Thierauf (2001); Awad e Ghaziri (2004); Hislop (2005).

Uma outra forma de olhar os três primeiros níveis hierárquicos (dado, informação e conhecimento) está na observação das fases de transformação de cada elemento, como na percepção de Arís et al. (2007, p. 55) apresentada na Figura 3.

Figura 3 – A Transformação: Dado, Informação e Conhecimento



Fonte: Arís et al (2007, p. 55 - tradução nossa).

Como pode ser visto na Figura 3, o Dado é transformado em Informação ao passar por um processo de contextualização, onde são valorados e organizados. A Informação os recebe e acrescenta padrões explicativos para que ocorra o processo de análise e a consequente transformação em Conhecimento.

Os mesmos autores também percebem que a construção do conhecimento se dá por meio da agregação de valores ao longo da Cadeia de Transformação da Informação, conforme a Figura 4.

Figura 4 – Cadeia de Transformação da Informação

Fonte: Arís et al (2007, p. 55, tradução nossa).

Na Figura 4, o Dado é codificado, agrupado e classificado com a finalidade de se transformar em Informação. A Informação é separada, avaliada e validada para criar sentido e ser transformada em Conhecimento Informativo. A análise do Conhecimento Informativo permite indicar opções, vantagens e desvantagens, e transformá-lo em Conhecimento Produtivo. Como Conhecimento Produtivo deve ser alinhado às metas, e envolver atividades de coordenação e negociação para que efetive em Ação.

Neste contexto, o conhecimento é definido como a informação que passa valor para a organização tomar decisões, ter a vantagem competitiva, e satisfazer as demandas do mercado, e alcançar as oportunidades (ARIS et al., 2007, p. 56).

Davenport (1998) descreveu as diferenças entre dado, informação e conhecimento, caracterizando à luz da interpretação humana, conforme Quadro 2.

Quadro 2 – Dados, Informação e Conhecimento

DADO	INFORMAÇÃO	CONHECIMENTO
Simples observações sobre o estado do mundo.	Dados dotados de relevância e propósito.	Informação valiosa da mente humana.
– Facilmente estruturado. – Facilmente obtido por máquinas. – Frequentemente quantificado. – Facilmente transferível.	– Requer unidade de análise. – Exige consenso em relação ao significado. – Exige necessariamente a mediação humana.	– Inclui reflexão, síntese e contexto. – De difícil estruturação. – De difícil captura em máquinas. – Frequentemente tácito. – De difícil transferência.

Fonte: Davenport (1998, p. 18).

Thierauf e Hoctor (2003) apresentam o relacionamento entre dado, informação, conhecimento e inteligência sob a perspectiva da de vários níveis de abstração na tomada de decisão para a otimizar a gestão na organização, conforme o Quadro 3.

Quadro 3 – Relação de Otimização para Diferentes Níveis de Abstração

NÍVEL DE ABSTRAÇÃO	DEFINIÇÃO	IMPORTÂNCIA DO PROBLEMA	ABORDAGEM PARA A DECISÃO	NATUREZA DO PROBLEMA
Verdade	Em conformidade com a verdade ou realidade	Vital	Consenso	Estruturado e Desestruturado
Sabedoria	Capacidade de julgar profundamente ao longo do tempo	Crítico	Consenso	Estruturado e Desestruturado
Otimização	Operações de monitoramento para a melhor solução	Maior para menor	Consultivo	Estruturado e Desestruturado
Inteligência	Uma excelente percepção para compreender relacionamentos importantes	Extremamente amplo	Consultivo	Desestruturado e semiestruturado
Conhecimento	Obtido de especialistas com base na experiência efetiva	Maior	Grupo consultivo	Semiestruturado
Informação	Dados úteis estruturados para análise	Maior para menor	Assessores	Estruturado e desestruturado
Dado	Fatos não estruturados	Menor para insignificante	Individual	Estruturado

Fonte: Thierauf e Hoctor (2003).

Conforme o Quadro 3, é possível verificar a análise que o autor fez entre a natureza e importância do problema e a abordagem para tomada de decisão. Por exemplo, o Dado tem impacto mínimo e o próprio gerente pode tomar a decisão. A Informação é composta por dados estruturados úteis para os gerentes analisarem e resolverem problemas críticos, e que se uniram a outros importantes recursos da organização (pessoas, máquinas, dinheiro, materiais e gestão), que aprenderam a reduzir seus custos e aumentar os lucros com a Tecnologia da Informação.

Ainda sobre o Quadro 3, o crescente volume de dados e de informações tem causado distração, confusão e pode ser um problema quase incontrolável, que necessita de um bom planejamento e controle sobre as operações por meio de decisões efetivas baseadas no fluxo e atualização da informação. Muitos reconhecem que a qualidade e a oportunidade das informações de negócio são importantes recursos para o gestor, e, assim como o Dado, o volume de informação. O Dado e a Informação têm foco operacional e tático.

No Quadro 3, o conhecimento que é obtido de especialistas com base na experiência efetiva, deve integrar a lista de alcance da informação, para se obter padrões e tendências que permitam ao gerente fazer a transição para a visão e a previsão. A inteligência foca nas estratégias para o sucesso da organização. A inteligência e o conhecimento estão no nível estratégico. A otimização foca no monitoramento das operações para aumentar a eficácia e fornecer soluções aos decisores. A sabedoria envolve a consciência e requer habilidades intuitivas fruto da experiência, e permite que o gerente sábio utilize o conhecimento e inteligência necessária para resolver um problema. Em conformidade com a verdade ou a realidade os pontos de ligação da sabedoria são construídos, e representam o ambiente ético.

2.1.1 Informação

Desde o século XIII, quando Thomas de Aquino (1225-1274) cunhou o termo informação em latim clássico como *informatio*, com o conceito de representação (de "dar forma a"), e implicou-lhe sentidos ontológico, epistemológico, pedagógico e linguístico; o termo tem passado por alterações de significado (CAPURRO, 2007; SIRIHAL e LOURENÇO, 2002; CARDOSO, 1996), como destacado na citação de Cardoso (1996):

> (...) termo cujo uso remonta à Antiguidade (sua origem prende-se ao latim *informare*: dar forma a) sofreu, ao longo da história, tantas modificações em sua acepção, que na atualidade seu sentido está carregado de ambiguidade: confundido frequentemente com *comunicação*, outras tantas com *dado*, em menor intensidade com *instrução*, mais recentemente com *conhecimento*. De toda forma, data deste século o destaque maior ao termo, desde sua apropriação enquanto fator de produção, no cenário de uma economia estruturada com base em estoques de conhecimento, produzidos e disseminados velozmente graças às tecnologias comunicacionais modernas. (CARDOSO,1996, p. 71).

Diferentemente do *dado*, a *informação* tem uma interpretação e propósito, está representada em um contexto por um conjunto de dados estruturados (ARIS, p. 54). A informação "é o meio ou material necessário para extrair e construir o conhecimento" (NONAKA e TAKEUCHI, 1995, p. 63).

A legislação brasileira, Lei Nº 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso a Informação, define a *informação* como "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato", *documento* como a "unidade de registro de informações, qualquer que seja o suporte ou formato", e classifica, qualifica e define outros termos referentes à *informação* como (BRASIL, 2011):

> a) **Informação sigilosa**: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
> b) **Informação pessoal**: aquela relacionada à pessoa natural identificada ou identificável;
> c) **Tratamento da informação**: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

> d) **Disponibilidade**: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
> e) **Autenticidade**: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
> f) **Integridade**: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
> g) **Primariedade**: **qualidade** da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações. (BRASIL, 2011).

Vimos, que a informação pode ser definida, classificada, rotulada e tratada de acordo com a sensibilidade e criticidade para a Organização, onde ela é entendida como ativo essencial, conforme a definição da NBR-16167 (2013a).

> Ativo essencial para os negócios de uma Organização e que consequentemente necessita ser adequadamente protegido, Conjunto de dados relacionados entre si que pode levar à compreensão de algo e que trazem determinado conhecimento, podendo estar na forma escrita, verbal ou imagística, e em meio digital ou físico. (NBR-16167, 2013a, p. 1).

A mesma norma refere-se à classificação da informação a partir da ação de definir o nível de sensibilidade da informação para que a mesma receba a proteção adequada, de acordo com "seu valor, requisitos legais, sensibilidade e criticidade para a Organização" (NBR-16167, 2013a, p.1).

Quanto à classificação da informação, a recomendação da Associação Brasileira de Normas Técnicas (ABNT) é a adoção de esquemas simples e com poucos níveis de classificação para ajudar no processo do fluxo da informação, devendo ter cuidado para que não ocorra um relaxamento na classificação e a falsa sensação de segurança. (NBR-27002, 2013b)

O Quadro 4 resume as características básicas da recomendação da NBR-27002 (2013b) que recomenda a adoção de quatro níveis de classificação.

Quadro 4 - Níveis de Classificação da Informação

NÍVEIS DE CLASSIFICAÇÃO	EXEMPLO DE TITULAÇÃO	CARACTERÍSTICAS BÁSICAS
Nível 1	– Pública – Externa	Informações que podem ou devem ser divulgadas publicamente.
Nível 2	– Interna – Uso Interno	Informações internas a serem divulgadas a todos os colaboradores e prestadores de serviços, desde que estes estejam comprometidos com a confidencialidade das informações.
Nível 3	– Restrita – Reservada – Setorial	Informações restritas que devem ser divulgadas a determinados grupos, áreas ou cargos.
Nível 4	– Confidencial – Secreta	Informações que requerem um tratamento especial e cuja divulgação não autorizada ou acessos indevidos pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégias da Organização.

Fonte: Elaboração da autora, 2015, com base nos dados da NBR ISO/IEC 27002 (2013b).

A recomendação da norma é que os Títulos dos níveis de classificação sejam sugestivos e de rápido entendimento sobre a classificação atribuída à informação.

No contexto tecnológico, a informação é referenciada como *informação tecnológica*. Montalli (1996) a define como "aquela que trata da informação necessária, utilizada e da informação gerada nos procedimentos de aquisição, inovação e transferência de tecnologia, nos procedimentos de metrologia, certificação da qualidade e normalização e nos processos de produção".

No contexto de negócios, surge o termo informação para negócios (*business information*), entendido como o "conjunto de informações destinadas a subsidiar as atividades das organizações no seu processo de desenvolvimento" (BORGES e CAMPELLO, 1997, p.149). Com base nas diversas fontes da informação e interesse para o mundo dos negócios, Vernon (1984) define a informação para negócios como:

> (...) dados, fatos e estatísticas publicados, necessários à tomada de decisão nas organizações de negócios, públicas ou privadas, bem como no governo. Inclui informações mercadológicas, financeiras, sobre bancos e empresas, leis e regulamentos de impostos, informações econômicas e comerciais, bem como informação factual sobre o ambiente no qual os negócios se realizam. (VERNON, 1984, p. 150).

Outra definição para informação para negócios foi proposta por Montalli e Campello (1996) como "aquela que subsidia o processo decisório do gerenciamento das empresas industriais, de prestação de serviços e comerciais, nos seguintes aspectos: companhias, produtos, finanças, estatísticas, legislação e mercado". A mesma autora classifica as fontes de informação como:

> **Fontes de informação técnica:** as normas técnicas, documentos patentes, legislação e publicações oficiais referentes à área.
> **Fontes de informação para negócios:** os relatórios anuais de companhias, diferentes tipos de diretórios, relatórios de pesquisas de mercado, levantamentos sobre mercado, levantamentos industriais, revistas técnicas, manuais, *handbooks*, guias, revistas publicadas pelas próprias companhias, revistas de negócios, publicações estatísticas, catálogos de manufaturas e jornais.
> **Fontes de informação científica:** as monografias, periódicos de pesquisas, artigos de revisões de literatura, *abstracts*, índices e anais de conferências, congressos, eventos científicos. (MONTALLI e CAMPELLO, 1996, p. 2-3).

2.1.2 Conhecimento

A discussão sobre o termo conhecimento teve início na própria história da filosofia, onde os gregos buscavam responder o que era o conhecimento, e se perpetua até hoje. Ao longo dos séculos, verificou-se o trabalho de grandes filósofos para definir e conceituar conhecimento, e aqui, destacamos algumas destas filosofias que influenciam no conceito de conhecimento para GC, conforme MAIER (2007, p.61).

a) Filosofia Grega: Heráclito, Sócrates, Platão e Aristóteles, entre outros, fundaram o pensamento europeu para o termo conhecimento e conceituaram o processo de conhecer ou adquirir conhecimento. A contribuição mais importante destes filósofos para os dias de hoje está na utilização do termo conhecimento não como tipos de conhecimento, mas no uso harmonioso e unificado dos pensamentos físico, ético e político. Também acreditavam na noção de uma realidade objetiva, que podia ser reconhecida, sistematicamente ou cientificamente, observando e analisando o objeto e assim, o conhecimento representaria uma verdade objetiva.
b) Revolução do pensamento: Bacon, Descartes, Hobbes, Hume, Locke e Leibnitz, entre outros desafiaram a equivalência do conhecimento e a fé, e a igreja como a instituição responsável para determinar o que era verdade.
c) Multiperspectivismo. Desde o século IX muitas escolas filosóficas do pensamento surgiram, tais como:
   - Positivismo – que argumenta que o conhecimento é adquirido a partir da observação de uma realidade objetiva, distinguindo o sujeito observador do objeto observado (como a organização de seu ambiente). Um exemplo foi Comte, que formulou a base da ciência natural, aplicada nos fundamentos da ciência da administração.
   - Construtivismo – que reivindica a ideia de que todo o nosso conhecimento é construído em nossas mentes, e contrapondo-se a noções de uma realidade objetiva.
   - Teoria Crítica – surgiu como crítica à teoria tradicional, para superar a tensão entre esta e a realidade, pois a teoria tradicional fora desenvolvida separadamente da realidade da sociedade. Esta teoria

foi desenvolvida pela escola de Frankfurt, representada por Horkheimer, Adorno, Habermas.

- Racionalismo Crítico – desenvolveu o argumento de que todo o nosso conhecimento é provisório e deve estar aberto a alterações empíricas, foi representado por Popper.
- Empirismo – apoia-se no pressuposto de que o conhecimento pode ser criado apenas por experiências, portanto somente as ciências naturais e a matemática podem oferecer o conhecimento seguro e verdades indiscutíveis. É representado por Hobbes, Locke, Hume e Russel.
- Sociologia do conhecimento – vê o conhecimento como socialmente construído. Foi fundado por Mannheim e Scheler, que se apoiaram nas ideias de Francis Bacon.

d) Pragmatismo – não se preocupa com a verdade universal, mas com um conceito mais imediato do conhecimento representando a realidade local da nossa experiência (o que funciona). É representado por Peirce, James, Lewis e Dewey. (MAIER, 2007, p.61).

Existiam diferenças fundamentais entre o racionalismo e o empirismo, porém os filósofos ocidentais concordavam no conceito introduzido por Platão de que conhecimento era a "crença verdadeira e justificada". (NONAKA e TAKEUCHI, 1997, p. 24). Os filósofos caracterizaram o conhecimento em três dimensões, como: conhecimento sensível e intelectual; aparência e essência; e opinião (crença) e saber.

Outra abordagem relacionada à escola de pensamentos, citada por Freire (2012, p. 82-83), baseada na visão de Francelin (2004), que acrescenta o relacionamento das pessoas com o mundo para melhor compreender o significado do conhecimento, por meio das dimensões: mito, razão, senso comum, arte, e observação pela experiência. O mito corresponde ao entendimento da relação indivíduo-objeto percebida pela Teologia, onde o conhecimento "é o que é sentido pela fé". A razão, que rompe o paradigma religioso e apresenta a "força da palavra como caminho para a formatação do conhecimento". O senso comum, onde o indivíduo percebe "o objeto pela ótica de sua cultura ética e moral, (...) e o conhecimento é o senso comum, os paradigmas dominantes da comunidade no qual o indivíduo está inserido". Na arte "o conhecimento

é gerado pelo gosto subjetivo pessoal. O conhecimento então é individual, criativo, subjetivo e mutável, originado da interpretação sensível do artista e do observador". Na observação pela experiência a Ciência, "o caminho é a experimentação, (...) o conhecimento é impessoal, isento e universal.

Assim, como ocorreu com a informação, o conceito do conhecimento evoluiu ao longo dos anos. O Quadro 5, elaborado a partir dos trabalhos de Freire (2012) e Steil (2007), apresenta uma compilação dos conceitos mais recentes. Optamos por manter alguns dos conceitos na língua inglesa, por fidelidade à publicação.

Quadro 5 – Definições do Termo Conhecimento

CONCEITO	AUTOR
O conhecimento é composto por processo dinâmico de um sistema de crenças pessoais justificadas. É o resultado da interação entre o conhecimento explícito e o tácito.	Nonaka, 1991, 1994; Nonaka e Takeuchi, 1997
the insights, understandings, and practical know-how that we all possess – is a fundamental resource that allows us to function intelligently.	Wiig, 1996 - wikipedia
Conhecimento é capacidade humana de caráter tácito, que orienta para a ação. Baseado em regras, é individual e está em constante transformação. O conteúdo revela-se em ações de competência individual, pois, na prática, se expressa através do conhecimento explícito, habilidades, experiências, julgamentos de valor e rede social. Não há como definir conhecimento de forma completa com apenas uma palavra.	Sveiby, 1998
O conjunto de informações combinado com experiências, vivências e intuição, que possibilitam ao indivíduo interpretar, avaliar e decidir.	Davenport e Prusak, 1998
Unlike data, knowledge is created invisibly in the human brain, and only the right organizational climate can persuade people to create, reveal, share and use knowledge.	Davenport et al., 1998

(Continuação do Quadro 5)

CONCEITO	AUTOR
Information transformed in understanding and into capability for effective action or a combination of instincts, ideas, rules, and procedures that guide actions and decisions.	Kemp et al., 2000.
O conhecimento é construído a partir de relações sociais sucessivas, é fruto de uma interação do homem com o mundo, estruturando-se pelo viés da interpretação individual.	Maturana e Varela, 2001
São os dados e informações que os indivíduos utilizam na ação, na prática diária, para a realização de tarefas e produção de novas informações.	Schreiber et al., 2002
Um conjunto constituído de cognição e habilidades que os homens empregam na resolução de problemas, incluindo a teoria e prática, regras do dia a dia e formas de agir.	Probst, 2002
Conhecimento é um conjunto de informações, elaborado crítica e valorativamente, por meio da legitimação empírica, cognitiva e emocional.	Angeloni, 2002
É a combinação de fatores como contexto, interpretação, experiência pessoal, aplicabilidade e processo cognitivo, que se somam à informação.	Siqueira, 2005
O conhecimento deriva da informação, mas é mais rico e significativo do que esta, pois inclui consciência, familiaridade e compreensão adquiridas pela experiência, possibilitando comparações, identificação das consequências e novas conexões.	Servin, 2005
Knowledge comprises all cognitive expectancies—observations that have been meaningfully organized, accumulated and embedded in a context through experience, communication, or inference—that an individual or organizational actor uses to interpret situations and to generate activities, behavior and solutions no matter whether these expectancies are rational or used intentionally.	Maier, 2007

(Continuação do Quadro 5)

CONCEITO	AUTOR
Dados são interpretados como sinais que alimentam os nossos sentidos, aos milhões por minuto. Informação é o dado com significado. Conhecimento é um corpo completo, formado de dados e informação, em que são transportados e resultam em ações que produzem novas informações. Dá-se o nome de conhecimento à relação que se estabelece entre um sujeito cognoscente e um objeto. Assim, todo conhecimento pressupõe dois elementos: o sujeito que quer conhecer e o objeto a ser conhecido. Por extensão, dá-se o nome de conhecimento ao saber acumulado pelo homem através das gerações.	Fialho, 2009, 2011

Fonte: Elaboração da autora, 2015, com base em FREIRE (2012, p. 83-86) e STEIL (2007, p. 14-15).

As escolas de pensamento tiveram um efeito profundo sobre as conceituações encontradas para o conhecimento na GC e na implementação de iniciativas de GC (HELOU, 2015; MAIER, 2007, p.62). Os diversos conceitos sobre conhecimento conduzem a diferentes perspectivas sobre conhecimento organizacional e, portanto, a diferentes conceitos de intervenções em uma forma de organização de lidar com o conhecimento (SCHNEIDER 1996, p.17).

2.1.2.1 Aplicação do conhecimento na organização

Probst, Raub e Romhardt (2002, p.11) afirmam que "O conhecimento é o único recurso que aumenta com o uso", e que as empresas devem aprender a administrar seus ativos intelectuais para sobreviver e competir na sociedade contemporânea. Ao contrário da evolução de técnicas e ferramentas refinadas para administrar os fatores clássicos de produção (mão-de-obra, capital e terras), não se vê a mesma evolução para as ferramentas profissionais para administrar ativos de conhecimento, ocasionando pouco uso de seus recursos intelectuais.

Desta forma, dependendo do contexto e da utilização, o termo conhecimento pode assumir vários significados. Pode significar desde informações armazenadas e processadas até o conhecimento dos indivíduos, armazenados em suas cabeças ou em documentos. (ILVONEN, 2013). Maier (2007, p. 64) afirma que o conhecimento pode

ser usado *na* organização e *para* a organização de forma variada, tais como: fator de produção, por ser a base para todas as decisões e atividades organizacionais; como produto, porque pode ser comercializado; e como fator de diferenciação das organizações, que tem o conhecimento como ativo mais importante.

Essa abordagem de Maier (2007) sobre a aplicação do conhecimento nos remete à importância do valor do conhecimento incorporado em bens, produtos e serviços oferecidos pelas organizações, assim como o conhecimento individual e organizacional que circulam na organização.

Considerando ser o conhecimento ativo intangível, as organizações necessitam conhecer e atribuir valor a este bem. Deste modo, identificamos algumas das categorias de metodologias de avaliação disponíveis para ativos intangíveis, apresentadas por Sveiby (2001), conforme Quadro 6.

Quadro 6 – Categorias de Metodologias de Avaliação dos Ativos Intangíveis

CATEGORIA	DESCRIÇÃO	VANTAGENS	DESVANTAGENS
Direct Intellectual Capital Methods (DIC)	Estima o valor monetário dos ativos intangíveis pela identificação do valor de seus componentes, ou como um coeficiente agregado.	– Retrata de forma mais realista a saúde da organização. – Pode ser aplicada em todos os níveis da organização. – São mais precisos que medidas financeiras tradicionais. – São úteis para organizações que não visam lucro.	– Dificultam a comparações por serem personalizados a cada organização. – Resistência por parte dos gestores tradicionais. – Pode gerar grandes volumes de dados.
Scorecard Methods (SC)	Identifica e representa graficamente os ativos intangíveis. Utiliza métodos equivalentes ao método DIC.		
Market Capitalization Methods (MCM)	Calcula o valor do ativo intangível a partir da diferença entre a capitalização de mercado de uma companhia e os ativos dos acionistas (*stockholders' equity*) como o valor de seus recursos importantes ou ativos intangíveis. ”	– Por contemplarem avaliações financeiras, são bastante úteis em fusões e aquisições (M&A) e para avaliações de mercado. – São utilizados para comparações entre empresas do mesmo segmento. – São construídos sobre bases contábeis tradicionais e são comunicados e aceitos mais facilmente.	– São sensíveis as estimativas de taxa de juros. – São pouco utilizados para organizações não lucrativas.
Return on Assets methods (ROA)	É a razão da média da receita bruta, em determinado período, pela média dos valores dos ativos tangíveis. O resultado é comparado com a média do seu segmento. A diferença é multiplicada pela média dos seus ativos tangíveis para calcular a média anual de receitas dos intangíveis. Dividindo a média superior pelo custo médio de capital ou uma taxa de juros, pode-se obter uma estimativa do valor dos Ativos Intangíveis ou Capital Intelectual.		

Fonte: Elaboração da autora, 2015, com base em *GlobalBrands -Sveiby* Associados, 2001).

Para Bukowitz e Williams (2002), o capital intelectual pode ser considerado como alugado, arrendado ou emprestado dos proprietários/detentores do conhecimento, e esclarece que:

> Uma distinção importante entre capital intelectual e o que tradicionalmente tem sido considerado gerador de valor nas organizações – os ativos físicos "tangíveis" – é que ele nem sempre é propriedade da organização. Isso significa que obter benefícios do conhecimento ou do capital intelectual não está sob o controle direto da organização. (BUKOWITZ e WILLIAMS, 2002, p.18)

Tal afirmação reforça o valor do conhecimento para a organização, além de enfatizar as diferentes formas de aquisição do conhecimento.

2.1.2.2 Gestão do Conhecimento

Maier (2007, p.22) nos apresenta a origem da GC datada no final dos anos 60 e início dos anos 70, com as publicações de Zand (1969) sobre gestão do conhecimento organizacional, e de Rickson (1976) que usou o termo *gestão do conhecimento* para descrever a criação e aplicação do conhecimento técnico. Nos anos 80 o termo ressurgiu no contexto que conhecemos hoje, com os trabalhos de Sveiby e Lloyd (1987), Wigg (1988), e outros.

O Comitê Executivo do Governo Eletrônico entende a GC, no âmbito das políticas de governo eletrônico, como:

> (...) um conjunto de processos sistematizados, articulados e intencionais, capazes de incrementar a habilidade dos gestores públicos em criar, coletar, organizar, transferir e compartilhar informações e conhecimentos estratégicos que podem servir para a tomada de decisões, para a gestão de políticas públicas e para inclusão do cidadão como produtor de conhecimento coletivo. (GOV.BR, 2015).

A abordagem sobre a GC é complexa e vasta. Vários autores já discorreram sobre o tema apresentando seus modelos, *frameworks*, ferramentas, características e diferenças. Aqui nos limitaremos a

identificar os principais conceitos que embasaram a compreensão das atividades de GC, sem a pretensão de esgotar o assunto.

Maier (2007) nos apresenta algumas das abordagens que influenciaram o desenvolvimento de teorias, tais como:

a) Ciência da Organização e Gestão de recursos humanos: mudança organizacional e gestão da mudança, desenvolvimento organizacional, aprendizagem organizacional, memória organizacional, inteligência organizacional (inteligência competitiva), cultura organizacional, Teoria da evolução das organizações, e gestão de recursos humanos;
b) Ciência da computação e sistemas de gestão da informação: abordagem do processamento das informações, teoria de sistemas, e inteligência artificial;
c) Ciência da Gestão: gestão estratégica, e outras abordagens como: gestão da inovação, e gestão da mudança;
d) Psicologia e Sociologia: psicologia organizacional, sociologia organizacional, e sociologia do conhecimento. (MAIER, 2007, P.23-33 – **tradução nossa**)

O mesmo autor também nos apresenta um resumo dos campos de pesquisa que formam as raízes da GC, conforme o Quadro 7.

Quadro 7 - Raízes da Gestão do Conhecimento

CAMPOS DE PESQUISA	CARACTERÍSTICAS
Mudança organizacional	Está preocupada com as mudanças dentro das organizações e mudanças de organizações, conta com a ajuda de modelos de desenvolvimento, de seleção e de aprendizagem, que representam um guarda-chuva de termos para as áreas como desenvolvimento organizacional ou aprendizagem organizacional.
Desenvolvimento organizacional	É uma estratégia metodológica para a intervenção, iniciada através de consultoria e planejada pela administração com a ajuda de um agente de mudança, que apoia o desenvolvimento das organizações no que diz respeito ao pessoal, aspectos interpessoais, estruturais, culturais e tecnológicos.
Aprendizagem organizacional	Abordagens que compartilham a hipótese comum de que os fenômenos (observável) de mudança nas organizações estão conectados com (não observável) o coletivo ou processos interpessoais de aprendizagem em um nível micro social (grupo), bem como em um nível macrossocial (organização).
Memória organizacional	É utilizada em analogia com a memória de um indivíduo para denotar a memória coletiva de uma organização que é capaz de armazenar coisas percebidas, experimentadas ou autoconstruídas para além da duração da ocorrência real, e, em seguida, recuperando-as num momento posterior.
Inteligência organizacional	Fornece um foco pouco diferente no processamento da informação organizacional do que a aprendizagem organizacional com ênfase no processamento coletivo de informações e tomada de decisão.

(Continuação do Quadro 7)

CAMPOS DE PESQUISA	CARACTERÍSTICAS
Cultura organizacional	É uma grande medida de fenômeno implícito apenas observável indiretamente com a ajuda de conceitos tais como confiança, normas, padrões, regras não escritas, símbolos, e artefatos que os membros da organização compartilham e que fornecem orientação. A cultura organizacional é o resultado de um processo de aprendizagem e é transmitida em um processo de socialização.
Teoria da evolução de organizações	Aplica as teorias de evolução originalmente desenvolvidas nas disciplinas de filosofia, biologia e ciências sociais para as organizações, por exemplo, a abordagem ecológica da população, sistemas de auto-organização, caos organizado e "gestão evolutiva".
Gestão de recursos humanos	Em um sentido institucional denota um subsistema organizacional que prepara, elabora e implementa decisões de pessoal para garantir a disponibilidade e a eficácia de pessoal, por exemplo, o planejamento de demanda de pessoal, recrutamento, treinamento, desenvolvimento, demissão de empregados.
Abordagem de processamento da informação	Desenvolve um modelo que explica o comportamento individual (por exemplo: resolução de problemas, tomada de decisão), com base em achados da psicologia utilizando conceitos cognitivos, tais como: atitude, personalidade e definição da situação, bem como, memória de curto prazo e longo prazo.
Teoria de Sistemas	É toda uma disciplina científica que visa a formulação de leis gerais e regras sobre os estados e comportamentos de sistemas e oferece a base de muitas investigações, teorias e conceitos desenvolvidos no âmbito da ciência da organização e sistemas de gestão da informação.

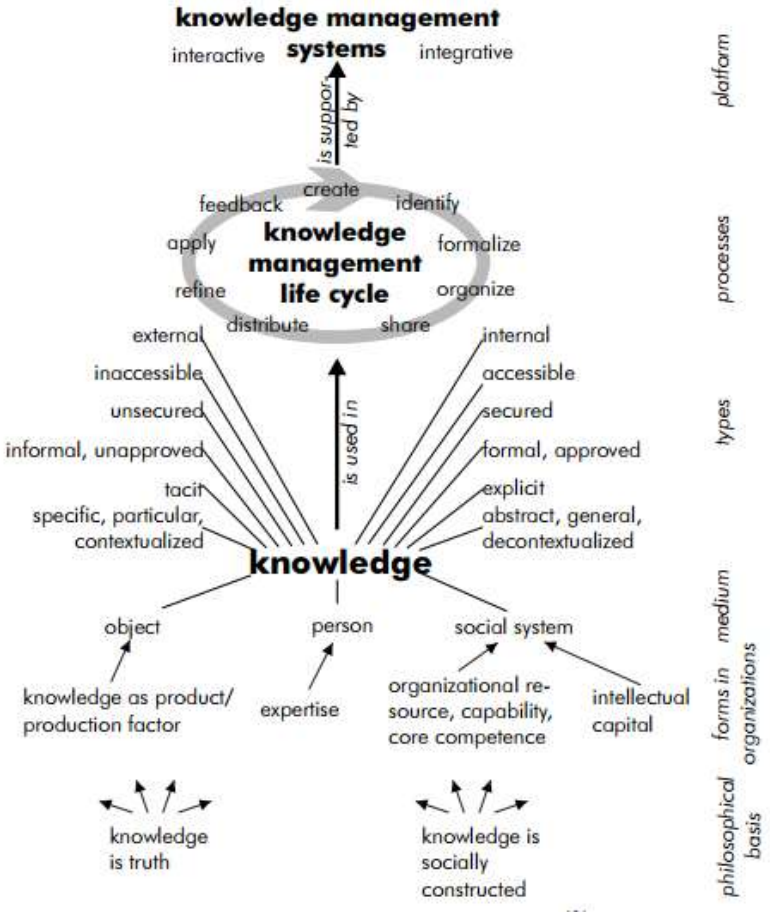
(Continuação do Quadro 7)

CAMPOS DE PESQUISA	CARACTERÍSTICAS
Inteligência artificial	Tenta estabelecer uma analogia entre problema humano e de computador resolvendo e aplicando um conjunto comum de métodos, por exemplo, lógica matemática, heurísticas de reconhecimento de padrões e de pesquisa, para uma grande variedade de domínio de problema.
Gestão estratégica	Determina as metas de longo prazo e o posicionamento de uma organização. Abrange o processo de formulação, implementação e avaliação de estratégias relacionadas à toma da de decisão e decisões operacionais.
Outras abordagens da gestão	Se concentram em outros aspectos da gestão, tais como: gestão da inovação e gestão evolutiva.
Psicologia organizacional	Campo que estuda o comportamento humano e experiência em organizações.
Sociologia organizacional	Campo da sociologia, que analisa as semelhanças estruturais e os sistemas sociais das organizações.
Sociologia do conhecimento	Conhecimento organizacional construído socialmente com várias visões de mundo.

Fonte: Maier (2007, P.34-35 - tradução nossa).

Maier (2007, p.78) propõe uma Plataforma de Sistemas de Gestão do Conhecimento, conforme a Figura 5, onde consolida aspectos relevantes da GC, desde a sua origem em bases filosóficas até as plataformas de utilização do conhecimento. O autor agrupa as origens do conhecimento nas organizações em: Conhecimento como produto e fator de produção que se relaciona com objetos e produtos; a expertise que é associada com as pessoas; e os recursos organizacionais (capacidades e principais competências) juntamente com o capital intelectual que alimentam ao sistema social. Maier (2007) cita também algumas características que tipificam o conhecimento e as fases do ciclo de vida da GC.

Figura 5 – Plataforma dos Sistemas de Gestão de Conhecimento



Fonte: Maier (2007, p. 78)

Um dos grandes desafios para a GC é a utilização de instrumentos de proteção, legais e institucionais, visando resguardar conhecimentos valiosos pois estes asseguram vantagem competitiva às organizações.

Apesar da relevância da proteção do conhecimento, a pesquisa realizada por Heisig (2008), analisou 160 modelos de GC e constatou que das 165 atividades previstas nos modelos, apenas três (0,01%) visaram a proteção do conhecimento. E dos 114 fatores críticos de sucesso dos

modelos analisados, apenas um considerou a proteção do conhecimento e outro a proteção da propriedade intelectual no produto.

2.1.2.3 Artefato de Conhecimento

Segundo Holsapple (2003, p. 98), um artefato de conhecimento é um objeto que transmite ou detém representações utilizáveis do conhecimento. No entanto, não tem qualquer conhecimento capacidade de processamento. O conhecimento incorporado em um artefato pode ser de natureza tácita, explícita ou implícita.

O autor apresenta como exemplos de artefatos de conhecimento: fitas com vídeos para treinamentos, livros, memorandos, planos de negócios impressos, manuais, documentos de patentes, arquivo de referências rápidas, instalações, layouts e produtos (por exemplo, o conhecimento incorporado em um carro).

O artefato que pertence a uma organização fica sob seu controle, e o acesso é liberado apenas para alguns de seus empregados.

2.2 PROGRAMA NACIONAL DE PROTEÇÃO AO CONHECIMENTO

O Art. 4 da Lei nº 9.883, de 7 de dezembro de 1999, estabelece a competência da ABIN para planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade.

Assim, a ABIN, como órgão responsável por planejar e executar a proteção dos conhecimentos sensíveis, que são "aqueles que, por sua natureza e potencial necessitam de medidas especiais de proteção, tendo em vista sua importância estratégica para a defesa dos interesses nacionais e a segurança do Estado e da sociedade" (BRASIL, 1999b), criou o Programa Nacional de Proteção ao Conhecimento (PNPC), cuja responsabilidade de execução está no Departamento de Contra-Inteligência da ABIN. (ABIN, 2015)

O público-alvo do PNPC são as instituições nacionais, públicas ou privadas, que geram ou custodiam conhecimentos sensíveis para o Brasil. As principais áreas de atividades são (ABIN, 2015):

- Defesa Nacional.
- Pesquisa, desenvolvimento e inovação científica e tecnológica.

- Energia, incluídas novas fontes alternativas.
- Minerais e materiais estratégicos.
- Conhecimentos dos povos indígenas e das comunidades tradicionais.
- Agronegócio.
- Desenvolvimento socioeconômico.
- Educação e promoção de cultura de proteção do conhecimento sensível. (ABIN, 2015).

O PNPC atua por meio de Acordos de Cooperação Técnica ou Convênios entre a ABIN e as instituições interessadas, e tem como objetivos (ABIN, 2015):

- Conscientizar os detentores de conhecimentos sensíveis nacionais sobre as ameaças a que estão sujeitos.
- Fomentar o desenvolvimento da cultura de proteção do conhecimento sensível, inclusive do conhecimento tradicional associado à biodiversidade brasileira.
- Apresentar medidas de proteção para esses conhecimentos e assessorar na sua implementação.
- Interagir com órgãos governamentais e instituições nacionais detentores de conhecimentos sensíveis. (ABIN, 2015)

A proposta do PNPC é atuar de forma integrada em quatro segmentos, a saber (ABIN, 2015):

1. Proteção física e do ambiente: medidas de proteção dos locais onde são elaborados, tratados, manuseados, custodiados ou armazenados conhecimentos, informações, dados e materiais sigilosos.
2. Proteção de documentos e conformidade: medidas de proteção para a elaboração, o manuseio, o trânsito, a difusão, a recepção, o armazenamento e o descarte de documentos sigilosos, bem como a sua adequação às leis e normas que regem o negócio da instituição.
3. Proteção na gestão de pessoas: medidas de proteção que visam a dificultar o ingresso de pessoas não desejáveis na instituição, além de assegurar padrões de comportamento

profissional e ético adequados aos funcionários admitidos, a fim de salvaguardar os conhecimentos sensíveis.

4. Proteção de sistemas de informação e continuidade: medidas de proteção que visam a garantir o funcionamento da infraestrutura tecnológica de suporte ao acesso, ao armazenamento e à comunicação de dados, informações e conhecimentos sensíveis, destinados a garantir a sua integridade, disponibilidade e confidencialidade, além de prover o restabelecimento desses serviços em caso de sinistro. (ABIN, 2015).

A implementação do programa na instituição parceira acontece por fases, podendo ser realizadas todas as quatro fases ou somente algumas, de acordo com as necessidades das instituições, são elas (ABIN, 2015):

1. Sensibilização: são atividades de conscientização dos profissionais da instituição para a adoção de medidas, procedimentos e comportamentos adequados, de acordo com a natureza sensível dos assuntos aos quais tenham acesso.
2. Identificação de alvos e ameaças: são atividades que identificam o que deve ser protegido e o nível de ameaça existente.
3. Diagnóstico: são atividades de avaliação do sistema de proteção da instituição parceira, a fim de identificar vulnerabilidades e recomendar ações, procedimentos e controles de segurança, tendo por base a metodologia de proteção do conhecimento sensível desenvolvida pela Abin; a legislação vigente; e as características funcionais da instituição parceira.
4. Acompanhamento: são atividades conjuntas de acompanhamento e avaliação da execução das ações previstas, bem como apoio e assessoramento na implementação de recomendações de segurança, podendo incluir:
    - *Normatização***:** consultoria e assessoramento para a elaboração de políticas e normas internas concernentes à proteção de conhecimentos.
    - *Classificação***:** atividades que visam a orientar e a exercitar a aplicação de critérios legais e institucionais, para a classificação de

> documentos contendo assuntos sensíveis. (ABIN, 2015)

2.3 INFORMAÇÃO E CONHECIMENTO NA ÁREA DE DEFESA

Na área militar as atividades de produção e proteção de informações e de conhecimentos são orientadas pela Doutrina de Inteligência de Defesa (DID).

2.3.1 Doutrina de Inteligência de Defesa

A Doutrina de Inteligência de Defesa – MD52-N-01 (DID), aprovada pela Portaria Normativa Nº 537/MD, de 21 de dezembro de 2005, é o documento que rege a produção e a proteção de informação e conhecimento no âmbito dos órgãos integrantes do Sistema de Inteligência de Defesa (SINDE), formado pelos órgãos de inteligência do MD e das FA, a quem compete "reduzir o grau de incerteza da ocorrência de um determinado cenário de interesse da Defesa" (ESG, 2005, p. 11).

O grau de sigilo deste documento foi revogado de acordo com o Art. 24 da Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso a Informação (BRASIL, 2011).

A DID apresenta um conjunto de conceitos[3], princípios[4], normas[5], métodos[6] e processos[7] que orienta e disciplina a Atividade de Inteligência no âmbito do SINDE, e possui características próprias por ser: assessorial; básica; dinâmica; objetiva; normativa; e unitária (ESG, 2005). As definições destas caraterísticas e outros conceitos básicos são apresentados no ANEXO.

A Atividade de Inteligência de Defesa (AID) caracteriza-se como uma atividade de cunho técnico e militar, apoiada em processo mental,

---

[3] Conceitos são "uniformizações de entendimentos destinados ao estabelecimento de uma linguagem comum" (ESG, 2005, p. 13).

[4] Princípios são as "bases orientadoras da Doutrina, alicerçadas na teoria e nas convicções éticas das Forças Armadas (FA) " (ESG, 2005, p. 13).

[5] Normas são as "bases para procedimentos" (ESG, 2005, p. 13).

[6] Métodos são os "caminhos ou orientações para se alcançar resultados de modo racional e com o maior proveito possível" (ESG, 2005, p. 13).

[7] Processos são os "modos de se efetivarem as etapas recomendadas nos métodos" (ESG, 2005, p. 13).

que busca produzir e salvaguardar conhecimentos de interesse de Defesa. É exercida em dois ramos inseparáveis, são eles (ESG, 2005, p. 16):

a) "Inteligência: ramo voltado para a produção de conhecimentos, relativos a fatos e situações atuais ou potenciais que afetem o processo decisório no âmbito da Defesa.
b) Contra-Inteligência (CI): ramo voltado para a detecção, identificação, neutralização, obstrução e prevenção da atuação da Inteligência adversa e das ações de qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de tecnologia da informação) de interesse da Defesa" (ESG, 2005, p. 16)

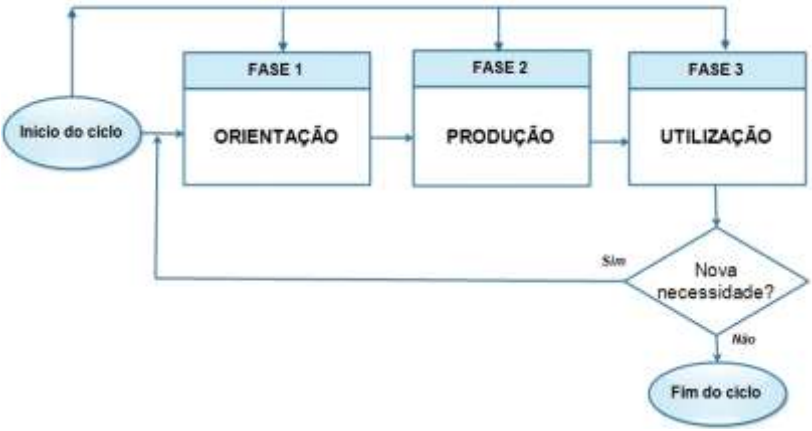
A AID segue onze princípios básicos, que são:

1. "Amplitude: que consiste em obter os mais completos resultados nos trabalhos desenvolvidos.
2. Clareza: significa que o conhecimento produzido deve permitir imediata e completa compreensão por parte do usuário.
3. Controle: implica que a produção do conhecimento deve seguir uma sistemática que permita o seu acompanhamento em todas as suas fases.
4. Exploração sistêmica: significa que as fontes e os órgãos integrantes do SINDE devem ser sistematicamente explorados por meio de um gerenciamento metódico, baseado no conhecimento completo de suas capacidades e limitações.
5. Imparcialidade: todas as ações devem ser praticadas sem a interferência de preconceitos, subjetivismos e outras influências que possam causar distorções em seus resultados.
6. Integração: onde todos os dados e conhecimentos obtidos devem ser processados a fim de que o produto resultante seja um conhecimento integrado.
7. Interação: implica em estabelecer e/ou adensar relações de cooperação que possibilitem otimizar esforços para a consecução dos objetivos.
8. Objetividade: todas as ações devem ser orientadas para objetivos previamente definidos e perfeitamente enquadrados nas finalidades da AID.

9. Oportunidade: significa que o conhecimento deve ser produzido em prazo que assegure o aproveitamento adequado de seus resultados.
10. Segurança: impõe a adoção de medidas de salvaguarda adequadas.
11. Simplicidade, implica planejar e executar ações de modo a evitar complexidade, custos e riscos desnecessários" (ESG, 2005, p. 16)

O Ciclo de Atividade de Inteligência de Defesa compreende as fases de produção dos trabalhos da AID, composto por três fases distintas: a orientação, a produção e a utilização; conforme a Figura 6.

Figura 6 – Ciclo da Atividade de Inteligência de Defesa



Fonte: Elaboração da autora, 2015, com base em ESG (2005. p. 16).

Na Figura 6, embora o ciclo seja contínuo e sequencial, as fases podem ser desenvolvidas simultaneamente. Na fase Orientação são definidos os objetivos de inteligência, que constarão nos Planos da AID. Na fase Produção ocorre o desenvolvimento dos trabalhos da AID. Na fase Utilização emprega-se o resultado dos trabalhos da AID para atender às necessidades previstas, e o ciclo pode ser realimentado com novas necessidades.

2.3.2 Ramo da Inteligência

O ramo da Inteligência é o responsável pela produção do conhecimento de Defesa, que orienta planejamento do preparo e do emprego das Forças Armadas (FA), e exerce atividades de acompanhamento, estudo, produção e difusão de conhecimentos. Por estar diretamente relacionada ao conhecimento de Defesa e, para que a comunicação seja clara e concisa, minimizando distorções e incompreensões, a Inteligência utiliza uma linguagem específica.

Fundamenta-se em três noções fundamentais (ESG, 2005, p. 19-20), como descrito abaixo:

1. "Verdade: é a perfeita concordância dos fatos ou das situações (objeto) com a imagem que fazemos deles (conteúdo de pensamento).
2. Estados da mente humana perante a verdade: considera que a mente é imperfeita e que a realidade é complexa. Reconhece a existência de quatro estados da mente em relação à verdade, que são:
   - Certeza: a mente aceita integralmente a imagem por ela mesma formada, como correspondente ao objeto, sem o temor de enganar-se. A mente, quando conduzida ao estado de certeza pela evidência, encontra a verdade.
   - Opinião: a mente acata a imagem por ela mesma formada como correspondente a determinado objeto, porém com receio de enganar-se.
   - Dúvida: a mente encontra, em situação de equilíbrio, razões para aceitar e, também, razões para negar que a imagem por ela mesma formada esteja em conformidade com determinado objeto.
   - Ignorância: caracterizado pela inexistência de qualquer imagem de determinado objeto ou de uma realidade específica.
3. Graus de complexidade do trabalho intelectual: são três as atividades realizadas por ser humano para conhecer determinados fatos ou situações, são elas:
   - Conceber ideias - é a simples concepção, na mente, da imagem de determinado objeto, sem adjetivá-lo.
   - Formular juízos - é a atividade pela qual a mente estabelece uma relação entre ideias.

- Elaborar raciocínios - é a atividade pela qual a mente, a partir de dois ou mais juízos conhecidos, alcança outro que deles decorre logicamente" (ESG, 2005, p. 19-20)

Os tipos de conhecimento definidos na AID são: (ESG, 2005):

a) "Informe: conhecimento resultante de juízo formulado pelo analista de Inteligência sobre a narração de fato ou situação passada ou presente. É a narração de um fato ou situação à qual foi aplicada uma técnica de avaliação de dados, tendo recebido um juízo de valor quanto à sua credibilidade.
b) Informação: Conhecimento resultante de raciocínio elaborado pelo analista de Inteligência que expressa sua certeza sobre situação ou fato passado ou presente.
c) Apreciação: Conhecimento resultante de raciocínio elaborado pelo analista de Inteligência que expressa sua opinião sobre situação ou fato passado, presente ou futuro imediato.
d) Estimativa: Conhecimento resultante de raciocínio elaborado pelo analista de Inteligência que expressa a sua opinião sobre a evolução futura de um fato ou de uma situação" (ESG, 2005, p. 19-20).

A AID classifica o conhecimento quanto ao nível de utilização e validade no tempo, como descrito a seguir. (ESG, 2005)

a) "Quanto ao nível de utilização:
   - Conhecimento Estratégico: conhecimento requerido para a formulação das Avaliações Estratégicas dos órgãos componentes da Defesa, de planos e de políticas no nível nacional ou internacional, referentes à Defesa Nacional.
   - Conhecimento Operacional: conhecimento requerido para planejar, conduzir e sustentar operações militares de grande envergadura, a fim de que sejam alcançados objetivos estratégicos dentro de um Teatro de Operações ou Zona de Operações.
   - Conhecimento Tático: conhecimento requerido para a condução de operações de combate no nível tático.

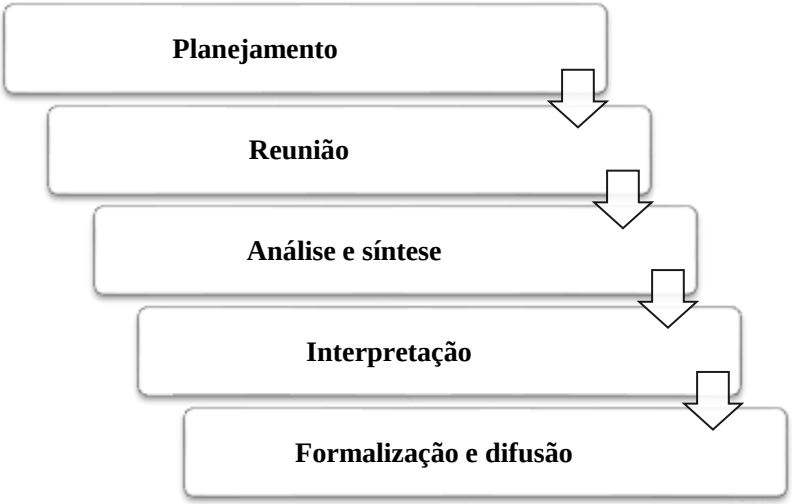
b) Quanto à validade no tempo:
   - Conhecimento Básico: conhecimento pouco sensível à ação do tempo. Compreende conhecimentos de geografia, de demografia, de política, biográficos, da estrutura geral das forças e das características operacionais de áreas do país ou do exterior.
   - Conhecimento Corrente: conhecimento altamente sensível à ação do tempo e que trata de assuntos e atividades em andamento, ou recentemente concluídos, apresentando reflexos para a conjuntura atual" (ESG, 2005),

O Método para a Produção do Conhecimento (MPC) envolve a sequência ordenada de procedimentos executados pelo analista, de forma racional e lógica, para dotar credibilidade ao conhecimento produzido. Os atributos pessoais do analista, sua experiência e seu embasamento cultural favorecem o sucesso da atividade, conforme citação:

> O Método para a Produção do Conhecimento (MPC) consiste na sequência ordenada de procedimentos executados pelo analista de forma racional e lógica. O emprego do método não deve ser entendido como condição suficiente para o êxito de um trabalho de Inteligência, mas, como condição necessária. Outros fatores concorrem para o sucesso na produção de conhecimentos, como os atributos pessoais do analista, sua experiência e seu embasamento cultural. No entanto, o emprego do método contribui para garantir que todos os aspectos do problema sejam considerados, produzindo conhecimento com base científica, uniformizando procedimentos e assegurando que o usuário confira credibilidade ao conhecimento produzido. (ESG, 2005, p. 22).

As etapas de produção são: planejamento; reunião; análise e síntese; interpretação; e formalização e difusão, como apresentado na Figura 7.

Figura 7 – Etapas para a Produção do Conhecimento de Defesa



Fonte: Elaboração da autora, 2015, com base em ESG (2005, p. 23).

O ramo de Inteligência utiliza a Técnica de Avaliação de Dados, que compreende as fases de: julgamento da fonte; julgamento do conteúdo; e a determinação do grau de credibilidade do dado.

Para o julgamento da fonte são observados aspectos sobre a autenticidade, confiança e competência, que permite aferir à fonte o grau de: idônea; regularmente idônea; regularmente inidônea; e não avaliada. O julgamento do Conteúdo objetiva determinar o grau de veracidade do conteúdo do dado, de acordo com sua semelhança, coerência e compatibilidade.

A determinação do grau de credibilidade do dado é determinada pelo analista que produziu o conhecimento, transformando o dado em Informe, é expresso por código alfanumérico. O detalhamento dos significados atribuídos na fase de análise dos julgamentos e da atribuição dos respectivos graus, constam do ANEXO.

2.4 ASPECTOS DA SEGURANÇA E PROTEÇÃO

Existe proximidade entre os termos *proteção do conhecimento* e *segurança do conhecimento* (ILVONEN, 2013, p. 108). Alguns autores consideram que a *proteção do conhecimento* é parte integrante da GC

(DAVENPORT e PRUSAK, 1998, GOLD, MALHOTRA E SEGARS, 2001; LUCAS 2010; MAIER, 2007).

No entanto, muitos artigos que abordam a *proteção* como uma parte importante da GC acabam por deixá-la de fora de sua investigação e não discutem a aplicação dos mecanismos de proteção, limitando-a à poucos elementos de um questionário (por exemplo, GOLD, MALHOTRA E SEGARS, 2001; DONATE e CANALES 2012).

Ilvonen (2013) realizou uma revisão sistemática nos principais *journals* da área da Informação e Conhecimento. Para a área da Informação, os cinco mais importantes *journals* pesquisados foram: *MIS Quartely* (MISQ), *Information System Research* (ISR), *Journal of Management Information Systems* (JMIS), *European Journal of Information Systems* (EJIS) e *Information Systems Journal* (ISJ), no período de busca dos anos 2002 – 2012. O resultado da pesquisa está na Tabela 1.

Tabela 1 – Sumário da Revisão Sistemática da Literatura na Área da Informação

FONTE	ARTIGOS	CONHECIMENTO	SEGURANÇA	SEGURANÇA DO CONHECIMENTO
MISQ	430	29	8	0
ISR	322	12	11	0
JMIS	459	34	10	0
EJS	506	23	9	0
ISJ	273	14	3	0
Total	**1990**	**112**	**41**	**0**

Fonte: Ilvonen (2013, p. 94, tradução nossa)

Foi constatado pela autora, conforme a Tabela 1, a existência de uma discussão com as palavras-chave “conhecimento” e “segurança”, porém de pequena expressão ao se comparar com o número total de artigos apresentados, e a falta de interesse na segurança do conhecimento. Os artigos consideraram o conhecimento sob o ponto de vista dos sistemas de informação como um objeto que pode ser codificado, e nem

todos o consideram um bem codificável, devido à dificuldade em capturá-lo. A combinação mais próxima do termo segurança do conhecimento foi a discussão sobre proteção e compartilhamento.

Para a revisão dos *journals* da área da GC, a autora considerou na perspectiva de segurança no conhecimento os temas: confiança, risco, proteção e segurança. Assim, selecionou os *journals*: *Journal of Knowledge Management* (JKM), *Journal of Intellectual Capital* (JIC), *The Learning Organization* (LO), *Knowledge and Process Management* (KPM) e *Knowledge Management Research and Practice* (KMRP). O resultado desta busca está na Tabela 2.

Tabela 2 - Sumário da Revisão Sistemática da Literatura na Área da GC

FONTE	ARTIGOS	SEGURANÇA	RISCO	PROTEÇÃO	CONFIANÇA	SEGURANÇA DO CONHECIMENTO
JKM	649	1	4	85	10	3
JIC	370	0	2	0	3	0
LO	367	0	3	0	6	0
KPM	253	1	0	0	1	0
KMRP	331	0	5	0	13	0
Total	**1970**	**2**	**14**	**85**	**33**	**3**

Fonte: Ilvonen (2013, p. 96, tradução nossa)

Como observado pela autora, O termo risco foi comumente relacionado à perda financeira e nos raros casos relacionados à GC foi visto como mitigador do risco de perda do conhecimento com a rotatividade dos empregados porque o conhecimento não era documentado. Dos 85 artigos relacionados à proteção, 38 artigos abordaram o termo em um contexto separado proteção do conhecimento, 18 artigos relacionam aos Direitos de Propriedade Intelectual (DPI), 15 artigos mencionaram a proteção como parte da GC, 5 artigos como proteção do conhecimento pessoal, que pode ser considerada uma barreira para o compartilhamento na GC, e 5 artigos discutiram a proteção do

conhecimento na retenção, nas alianças estratégicas e como um elemento estratégico da GC.

Em consequência, a perspectiva de proteção no campo da gestão do conhecimento fornece um bom ponto de partida para uma análise mais aprofundada dos elementos que conceituam a segurança conhecimento. (ILVONEN, 2013, p. 108).

2.4.1 Gestão de Riscos

As organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco" (NBR ISO 31000, 2009).

A NBR-ISO-31000 (2009) apresenta os princípios da Gestão de Riscos (GR) e ressalta que para a eficácia desta gestão convém que princípios apresentados sejam atendidos em todos os níveis da instituição. Dentre os princípios destacamos: a GR cria e protege valor; a GR é parte integrante de todos os processos organizacionais; a GR é parte da tomada de decisões; a GR aborda explicitamente a incerteza; a GR baseia-se nas melhores informações disponíveis; a GR considera fatores humanos e culturais; e a GR é dinâmica, iterativa e capaz de reagir a mudanças.

A Norma ainda esclarece, com relação ao princípio que a GR facilita a melhoria contínua da organização, que é conveniente que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos da sua organização.

A ameaça é um evento que pode dificultar, ou impedir, que o objetivo seja alcançado. Por sua vez, o risco é a probabilidade de que a ameaça se concretize.

A GR compreende um conjunto de atividades coordenadas para dirigir e controlar os riscos em uma organização. A GR possui uma estrutura composta de componentes para a concepção, implementação, monitoramento, análise crítica e melhoria contínua, e é regida por políticas e planos estabelecidos para a organização. (NBR ISO 31000, 2009).

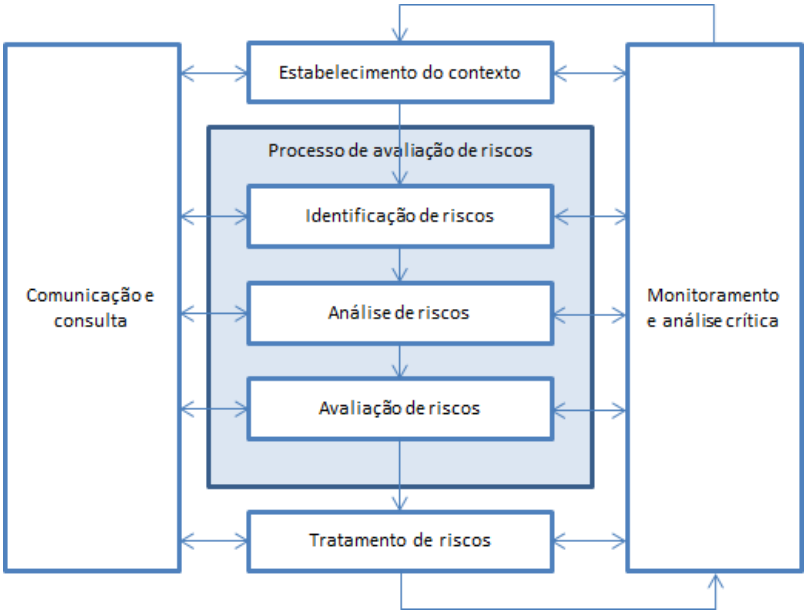
Para gerenciar riscos as organizações desenvolvem atividades que identificam e analisam os riscos. Os riscos identificados são então avaliados e, se necessário, submetidos a tratamento que os eliminem ou os ajustem aos níveis aceitáveis estabelecidos em critérios de risco.

O estabelecimento do processo de gestão de riscos possibilita que a organização obtenha benefícios como: Aumentar a probabilidade de

atingir os objetivos; aprimorar a identificação de oportunidade e ameaças; conformidade com requerimentos legais e normas internacionais; aprimorar os controles e reduzir perdas e tornar a organização mais resiliente.

A Norma recomenda que o processo de Gestão de Riscos, apresentado na Figura 8, seja parte integrante da gestão, incorporado na cultura e nas práticas, e adaptado aos processos de negócios da organização.

Figura 8 – Processo de Gestão de Riscos



Fonte: NBR ISO 31000 (2009, p.14).

Sobre a Figura 8, a Norma estabelece que:

- Convém que a Comunicação e Consulta seja feita às partes interessadas, internas e externas, durante todo o processo.
- Convém que o Estabelecimento de Contexto articule os objetivos e defina os parâmetros externos e internos que serão considerados na gestão de riscos.

- Convém que sejam definidos os Critérios de Risco para a avaliação da significância do risco.
- Convém que na Análise de Risco seja desenvolvida a compreensão dos riscos.
- A Avaliação de riscos considera a Análise de Risco para auxiliar na tomada de decisões quanto à necessidade de tratamento de risco e à necessidade de implementação do tratamento.
- Convém que o Tratamento de Riscos envolva a seleção da opção(ões) para modificar os riscos e a implementação das opção(ões) escolhida(s).
- Convém que o Monitoramento e Análise Crítica sejam planejados como parte do processo de Gestão de Riscos e envolvam a checagem (vigilância regulares) ou resposta a um fato específico. (NBR ISO 31000, 2009).

Recentemente, a gestão empresarial tem valorizado a GR como instrumento de proteção. Apesar da reconhecida importância dos ativos de conhecimento, elas priorizam a mitigação dos riscos de mercado, de crédito e os operacionais, e deixam para um plano secundário, ou desprezam os riscos que afetam os ativos intangíveis, chamados de *riscos de conhecimento* (MAIER, 2007, p. 137).

2.4.1.1 Ameaças e Fatores de Risco para os Dados

Sendo o dado a parte elementar da informação e conhecimento, deve-se considerar sua proteção e segurança nos ambientes operacionais onde ocorre a geração e o armazenamento dos dados.

A NBR-11515 (2007) cita as ameaças que devem ser consideradas no ambiente físico, tais como: incêndio; explosão; intempéries (raio, vendaval, e outros); água (vazamento e transbordamentos); impacto de veículos e aeronaves; falta de energia, curtos-circuitos, e outros danos elétricos; atos ilícitos (roubo, assalto, sabotagem, infidelidade, e outros); problemas com a climatização; descarga eletrostática; emissões eletromagnéticas; campos magnéticos; umidade e fungos; roedores e insetos; poeira; vibração; efeitos químicos; e disparo de armas de fogo.

A mesma norma apresenta os fatores que devem ser considerados, pois influenciam a segurança física dos dados, são eles: localização; construção; infraestrutura elétrica; climatização; móveis, utensílios e equipamentos; medidas, sistemas de controle de acesso e barreiras de

segurança; sistemas de detecção e combate a incêndio, alagamento e outros sinistros; operações de manuseio (produção, manutenção e cópias de segurança); e redundância de dispositivos.

Quanto às cópias de segurança, a recomendação normativa é que os procedimentos de execução estejam documentados e geridos, sejam revisados periodicamente e mantidos atualizados. Essas medidas devem ser compatíveis com a criticidade dos dados.

2.4.1.2 Ameaças e Fatores de Risco para a informação

A GR de segurança da informação é necessária para identificar as necessidades da organização em relação aos requisitos de segurança, e criar sistema eficaz de segurança da informação. É conveniente que essa abordagem esteja alinhada com a GR corporativa, bem como, que proponha medidas de proteção considerando as consequências para o negócio, e a probabilidade de concretização dos riscos. (NBR ISO/IEC 27005, 2011)

A mesma Norma descreve, que, quanto à origem, as ameaças às informações podem ser:

a) Intencional – ações humanas intencionais contra os ativos informacionais.
b) Acidental – ações de origem humana que podem comprometer acidentalmente os ativos de informação.
c) Ambiental (natural) – incidentes que não são provocadas por ações de seres humanos. NBR ISO/IEC 27005, 2011)

Os tipos de ameaças são: dano físico; eventos naturais; paralização de serviços essenciais; distúrbio causado por radiação; comprometimento da informação; falhas técnicas; ações não autorizadas; e comprometimento de funções (NBR ISO/IEC 27005, 2011, p. 53-54).

Deve-se ter atenção às fontes de ameaças de origem humana. O Quadro 8 apresenta a origem das ameaças, a motivação, e as possíveis consequências.

Quadro 8 – Ameaças provocadas por seres humanos à Informação

ORIGEM DAS AMEAÇAS	MOTIVAÇÃO	POSSÍVEIS CONSEQUÊNCIAS
Hacker[8], Cracker[9]	Desafio. Ego. Rebeldia. Status Dinheiro.	*Hacking*. Engenharia social. Invasão de sistemas, infiltrações e entradas não autorizadas. Acesso não autorizado ao sistema.
Criminoso Digital	Destruição das informações. Divulgação ilegal de informações. Ganho monetário. Alteração não autorizada de dados.	Crime digital. Ato fraudulento. Suborno por informação. *Spoofing* (fazer se passar por outro). Invasão de sistemas.
Terrorista	Chantagem. Destruição. Exploração. Vingança. Ganho político. Cobertura da mídia.	Bomba/terrorismo. Guerra de informação. Ataque a sistemas. Invasão de sistemas. Alteração de sistema.
Espionagem industrial	Vantagem competitiva. Espionagem econômica.	Garantir vantagem de um posicionamento defensivo. Garantir vantagem pública. Exploração econômica. Furto de informação. Violação da privacidade das pessoas. Engenharia social. Invasão de sistema. Acesso não autorizado ao sistema.
Pessoal interno	Curiosidade. Ego. Obtenção de informações úteis para serviços de inteligência. Ganho monetário. Vingança. Erros e omissões não intencionais.	Agressão a funcionário. Chantagem. Vasculhar informação de propriedade exclusiva. Uso impróprio de recurso computacional. Fraude e furto. Suborno por informação. Entrada de dados falsificados ou corrompidos. Interceptação. Código malicioso. Venda de informações pessoais. Defeitos (*bugs*) no sistema. Invasão de sistemas. Sabotagem de sistemas. Acesso não autorizado ao sistema.

Fonte: NBR ISO/IEC 27005 (2011).

[8] Hacker: "pessoas peritas em programação de computadores, que entram sem permissão e ilegalmente em sistemas alheios" AMARAL e PRETTO (2009, p. 53)
[9] Cracker: "alguém que invade sistemas de outrem para fazer uso ilícito de seus conteúdos" AMARAL E PRETTO (2009, p. 53)

2.4.1.3 Ameaças e Fatores de Risco para o Conhecimento

Desouza (2007) afirma que os empregados levam a organização à grandes destaques como fizeram Bill Gates com a *Microsoft*, Jack Welch com a *General Electric* e Steve Jobs com a Apple e também podem causar uma parada brusca na organização destruindo a vitalidade dos negócios como fizeram Ken Lay e Jeffrey na Enron. Assim destaca que os empregados são o núcleo do ativo intelectual da empresa. São contratados e recebem treinamentos para usar suas habilidades e conhecimentos em prol dos objetivos da empresa. A gestão dos recursos humanos é uma habilidade crucial para a manutenção e sustentabilidade da organização.

A gestão de recursos humanos deve se preocupar com a retenção dos empregados que são depósitos de conhecimentos e despertam interesses em empresas concorrentes, e com orientações para que os empegados não divulguem, intencionalmente ou não, informações confidenciais, o que pode ocorrer em entrevistas de emprego em empresas do mesmo setor.

O mesmo autor também afirma que embora hodiernamente as ameaças dos crimes cibernéticos tenham ocupado a atenção de muitos governos e empresas, as violações na segurança do conhecimento não necessitam de atividades tão sofisticadas, pois elas residem nos descuidos de práticas organizacionais. Ele cita uma série de causas de violações e recomenda medidas de segurança que podem ser adotadas para mitigar os riscos à segurança do conhecimento.

Quanto aos funcionários, algumas causas de violações apontadas por Desousa (2007) que levam à perda de conhecimento são: desleixo do funcionário ao reutilizar um conhecimento sem observar a compatibilidade com o contexto para qual ele foi criado; não verificar o risco de comprometimento do conhecimento considerando as viagens realizadas pelo funcionário; desatualização de habilidades não satisfazendo mais os requisitos para o exercício da função; competição por funcionários talentosos; e intenção maliciosa do funcionário.

As medidas de segurança capazes de prevenir tais ameaças são: verificar os antecedentes, verificar regularmente a confiança no empregado, realizar atividades de Contra-Inteligência, verificar se os objetivos do funcionário se alinham com os objetivos da organização, instituir programa de incentivos e recompensas, investir na educação dos funcionários sobre segurança do conhecimento.

O Quadro 9 apresenta outros pontos de ameaças para os quais Desouza (2007) sugere causas das violações e medidas de segurança.

Quadro 9 - Pontos de Ameaça, Causas de Violação e Medidas de Segurança para o Conhecimento

PONTOS DE AMEAÇAS	CAUSAS DAS VIOLAÇÕES DE SEGURANÇA	MEDIDAS DE SEGURANÇA
Tecnologias pervasivas	– Perigos de viagens – Tecnologia móvel – Tecnologia de armazenamento e duplicação – Aplicações tecnológicas	– Segurança nas viagens – Segurança dos meios móveis – Cópias e armazenamentos controlados – Garantia nas aplicações
Responsabilidade de parceiros	– Atuação insignificante – Agir com dolo – Vazamento de negócio de parceiros – Circulação de bens intelectuais – Desvio da aliança	– Construção de alianças baseadas na confiança – Monitoramento do comportamento e atuação – Incentivos – Balanceamento dos riscos
Segurança Física	– Invasão de instalações – Entrada de objetos estranhos na instalação – Instalações externas – Ouvir por acaso ou de propósito – Retirada de ativos da instalação – Agressões a empregados – Vizinhos como proteção ou vulnerabilidades	– Projetar as instalações – Pontos de entrada e saída seguros – Atendimento de visitantes – Fazer inspeções periódicas
Crises anormais	– Reconhecer sinais – Preparar para o evento – Responder ao evento – Aprender e reforçar a organização – Perda de ativo intelectual	– Elaborar planos de contingência – Manter cenários alternativos – Ter capacidade de resposta imediata – Desenvolver capacidades

Fonte: Elaboração da autora, 2015, com base em Desousa (2007 - tradução nossa).

Outras importantes contribuições para a construção deste entendimento foram sumarizadas no Quadro 10, onde estão relacionados os mecanismos de proteção e o conhecimento a ser protegido por eles.

Quadro 10 – Proteção do Conhecimento

ÁREAS	CATEGORIAS	MECANISMOS DE PROTEÇÃO DO CONHECIMENTO	CONHECIMENTO A SER PROTEGIDO
Recursos Humanos	Gestão Estratégica	– Identificar as capacidades essenciais. – Proteger as capacidades essenciais e as criações	– Decisões – Capacidades essenciais – Criações
	Gestão de Alianças	– Proteção de capacidades essenciais. – Nomear um gestor do conhecimento. – Definir diretrizes de proteção do conhecimento.	– Conhecimentos essenciais residentes nos empregados envolvidos
	Gestão de Recursos Humanos	– Educar e conscientizar sobre propriedade industrial. – Estabelecer programa de recompensa e avaliação para proteção das capacidades essenciais. – Consultar especialistas para elucidar determinadas situações. – Manter atualizados os cadastros de pessoal e de parceiros.	– Capacidades essenciais – Conhecimento essenciais residentes nos empregados envolvidos
Processos	Fluxos de Conhecimento	– Limitar o acesso ao conhecimento somente para quem necessita conhecer – Estabelecer limites para os conhecimentos que estão fora da necessidade de conhecer	– Conhecimentos compartilhados – Conhecimentos essenciais
	Acessos da Parceria	– Negar o acesso do parceiro às atividades restritas – Negar o acesso do parceiro às instalações restritas – Limitar o acesso do parceiro às pessoas fora da parceria	– Conhecimentos técnicos – Conhecimentos residentes nos artefatos – Conhecimentos essenciais

Continuação do Quadro 10

ÁREAS	CATEGORIAS	MECANISMOS DE PROTEÇÃO DO CONHECIMENTO	CONHECIMENTO A SER PROTEGIDO
Estrutura Legal	Patentes	– Obter patentes para inibir a imitação	– Invenções – Novidade das inovações
	Mecanismos contratuais	– Especificar os conhecimentos proprietários. – Especificar regras para o compartilhamento de conhecimento. – Estabelecer consequências para o descumprimento de regras de acesso e uso indevido dos conhecimentos. – Assinar acordos de não divulgação (confidencialidade) – Não empregar funcionários de parceiros. – Garantir que o conhecimento ou tecnologia compartilhada com o parceiro está protegida por patentes, contrato de sigilo ou direitos autorais.	– Conhecimentos compartilhados – Conhecimento proprietários – Conhecimento essenciais residentes nos ex-empregados

Fonte: Elaboração da autora, 2015, com base em Norman (2001) e Bocchino, et al. (2010).

2.4.2 Proteção dos Direitos de Propriedade Intelectual

Antes de apresentar os principais conceitos de Propriedade Intelectual (PI), é importante entender o significado dos termos. Segundo o Novo Dicionário da Língua Portuguesa, de Aurélio Buarque de Holanda Ferreira, PROPRIEDADE é entendida como o "direito de usar, gozar e dispor de bens e de revê-los do poder de quem quer que injustamente os possua" e "bens sobre os quais se exerce esse direito". O adjetivo "INTELECTUAL" significa "possuir dotes de inteligência".

Para a Organização Mundial de Propriedade Industrial (OMPI) a PI se refere, em sentido amplo, às criações do espírito humano e aos direitos de proteção dos interesses dos criadores sobre suas criações. OMPI [200-?].

Neste contexto, Jungmann (2010) afirma que "a propriedade intelectual não se traduz nos objetos e em suas cópias, mas na informação ou no conhecimento refletido nesses objetos e cópias, sendo, portanto, um ativo intangível "

A PI compreende quatro dimensões. A dimensão Temporal onde são estipulados prazos legais que permitem que o titular possa explorar economicamente com exclusividade os bens e os processos produtivos decorrentes deste direito. A dimensão do Escopo do Direito significa que cada objeto protegido pela PI tem sua delimitação de proteção definida por lei. A dimensão da Segurança Jurídica evita que terceiros possam explorar indevidamente sem a prévia autorização do titular do direito. A dimensão da Territorialidade do direito de propriedade industrial proporciona que os objetos protegidos pelo Direito de Autor tenham validade internacional e os protegidos pela Propriedade Industrial somente no país de depósito (WIPO,OMPI,INPI, 2015)

A legislação brasileira específica para a PI está apresentada no Quadro 11.

Quadro 11 – Legislação Brasileira sobre a Propriedade Intelectual

Legislação	Descrição
Lei no 9.279, de 14.05.1996 (Lei da Propriedade Industrial)	Institui a proteção dos direitos relativos à propriedade industrial, considerado o seu interesse social e o desenvolvimento tecnológico e econômico do País, se efetua por meio de concessão de patentes de invenção e de modelo de utilidade; concessão de registro de desenho industrial; concessão de registro de marca; repressão às falsas indicações geográficas; e repressão à concorrência desleal.
Lei no 9.456, de 25.04.1997 (Lei dos Cultivares)	Institui a proteção dos direitos relativos à propriedade intelectual referente a cultivar se efetua mediante a concessão de Certificado de Proteção de Cultivar, considerado bem móvel para todos os efeitos legais e única forma de proteção de cultivares e de direito que poderá obstar a livre utilização de plantas ou de suas partes de reprodução ou de multiplicação vegetativa, no País.
Lei no 9.609, de 19.02.1998 (Lei do Software)	Institui que a proteção à propriedade intelectual de programa de computador é o mesmo conferido às obras literárias (direitos autorais e conexos). Entende-se por Programa de computador um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

Continuação do Quadro 11

Legislação	Descrição
Lei no 9.610, de 19.02.1998 (Lei do Direito Autoral)	Institui que a proteção dos direitos autorais contempla os direitos de autor e os que lhes são conexos. Autor é a pessoa física criadora de obra literária, artística ou científica. São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro
Lei nº 10.973, de 02.12.2004 (Lei da Inovação) – Alterada em 2016.	Institui medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional do País.
Lei nº 11.196, de 21.11.2005 (Lei do Bem)	Institui o Regime Especial de Tributação para a Plataforma de Exportação de Serviços de Tecnologia da Informação - REPES
Lei no 11.484, de 31.05.2007 (Topografia de circuitos integrados)	Institui incentivos às indústrias de equipamentos para TV Digital e de componentes eletrônicos semicondutores e sobre a proteção à propriedade intelectual das topografias de circuitos integrados.
Lei 13.243, de 11.01.2016 – que alterou a Lei da Inovação.	Dispõe sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação e altera a Lei no10.973, de 2 de dezembro de 2004, a Lei no6.815, de 19 de agosto de 1980, a Lei no 8.666, de 21 de junho de 1993, a Lei no 12.462, de 4 de agosto de 2011, a Lei no 8.745, de 9 de dezembro de 1993, a Lei no 8.958, de 20 de dezembro de 1994, a Lei no 8.010, de 29 de março de 1990, a Lei no 8.032, de 12 de abril de 1990, e a Lei no 12.772, de 28 de dezembro de 2012, nos termos da Emenda Constitucional no 85, de 26 de fevereiro de 2015.

Fonte: Elaboração da autora, 2015.

Observamos no Quadro 11 que o final do século XX marcou a regulação da PI no Brasil.

Segundo Bocchino et al. (2010, p.18) os bens imateriais protegidos pela PI e que possuem legislação específica, são: patente de invenção; patente de modelo de utilidade; registro de desenho industrial; registro de marcas; registro de indicações geográficas; registro de cultivares; registro de topografia de circuitos integrados; registro de direitos autorais; registro de softwares.

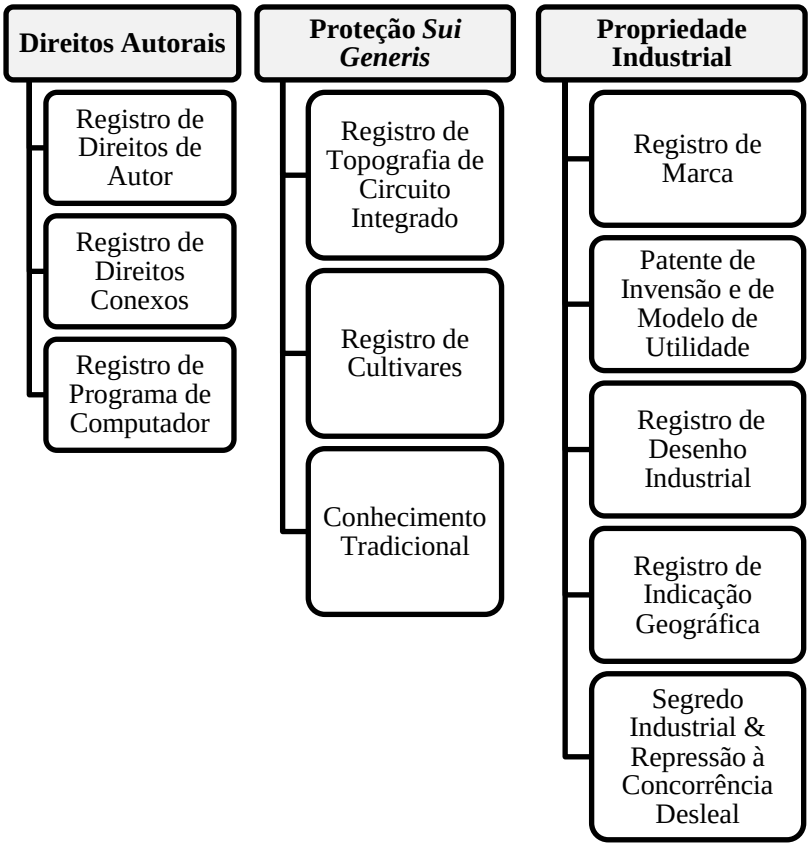
O início da PI como um dos elementos mais estratégicos da política industrial, tecnológica e de comércio exterior do Brasil, foi regulado na Lei nº 9.279/1996, Pimentel (2010a). Neste contexto, Jungmann (2010, p.37) considera a propriedade industrial como "uma importante ferramenta para a promoção do desenvolvimento de um país, pois ela decorre diretamente da capacidade inventiva ou criadora de tecnologia de seus habitantes". No Brasil, cabe ao INPI dar o tratamento devido aos assuntos de Propriedade Industrial.

A Propriedade Industrial representa os "direitos concedidos com o objetivo de promover a criatividade pela proteção, disseminação e aplicação industrial de seus resultados" (WIPO,OMPI,INPI, 2015, p. 5).

Os Direitos de PI diferem dos Direitos de Propriedade Industrial porque estes "envolvem desenvolvimento técnico utilizando atividade inventiva e possuem aplicação industrial" (BOCCHINO et al., 2010, p. 18). A PI utiliza como instrumentos de proteção: a Patente, o Registro, o *Know how*, o Segredo de Negócio e o Tempo de Liderança sobre os competidores.

Contribuindo para o entendimento da PI, elaboramos a Figura 9 representando os instrumentos de proteção da PI para os bens imateriais (ativos intangíveis) que dizem respeito às competências técnicas e a reputação das empresas. Os bens protegidos pela PI e que não pertencem à Propriedade Industrial são: Registro de Cultivares, Registro de Direitos Autorais, Registro de Programa de Computador e Registro de Topografia de Circuitos Integrados. Os instrumentos de proteção da Propriedade Industrial são: Patente de Invenção e Patente de Modelo de Utilidade, e Registro de Desenho Industrial, Registro de Marca, Registro de Indicações Geográficas e Registro de Cultivares.

Figura 9 – Instrumentos de Proteção dos Direitos de Propriedade Intelectual



Fonte: Elaboração da autora, 2015, com base em Brasil (1996; 1997; 1998 a; 1998b; 2007a.)

Os direitos de autor referem-se à proteção de criações do espírito humano, cujo domínio está na proteção das expressões artísticas, literárias e científicas protegem obras, ou seja, as expressões concretas, e não as ideias. (WIPO, OMPI, INPI, 2015)

Os Direitos Autorais abrangem os Direitos de Autor e os Direitos Conexos. No art. 7 da Lei do direito autoral, diz que são "obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro", e como exemplo estão os projetos e esboços

de engenharia e de ciência, e os programas de computador (objeto de lei própria) (BRASIL, 1998b)

A proteção da PI sobre cultivar (novas variedades de plantas) confere por um determinado prazo, um direito exclusivo, para reconhecer os desenvolvimentos dos criadores de novas variedades de plantas. (WIPO, OMPI, INPI, 2015)

A marca é um sinal que individualiza os produtos ou serviços de uma determinada empresa e os distingue dos produtos ou serviços de seus concorrentes, e deve ter caráter distintivo e não deve ser enganosa (WIPO, OMPI, INPI, 2015).

Uma patente é um documento que descreve uma invenção e a protege, pois cria uma situação legal na qual a invenção pode ser explorada somente com a autorização do titular da patente, ou seja, garante ao titular os direitos exclusivos para usar sua invenção por um período limitado de tempo em um determinado país (WIPO, OMPI, INPI, 2015).

O Sistema de Patentes tem duas funções: incentivar o desenvolvimento econômico e tecnológico de um país, protegendo os direitos do titular, e fornecer ao público mundial acesso à informação sobre o desenvolvimento da tecnologia protegida em um país, para estimular a inovação e contribuir para o crescimento econômico de cada país.

Assim, a concessão de patentes se caracteriza na existência de custo e benefício, porque a proteção é territorial e a informação é mundial. Um documento de patente contém a descrição das Informações Tecnológica[10], tais como: *Informações Técnicas* que são encontradas no relatório descritivo, nas reivindicações, no resumo e nos desenhos da invenção (se houver); *Informações Legais* que são extraídas do escopo das reivindicações, as quais fornecem os limites da proteção conferida pela patente, bem como do seu status legal; *Informações Comerciais* que são úteis para as empresas e extraídas dos dados bibliográficos identificadores do nome do inventor, depositante, data de depósito, país de origem, etc; e *Informações para políticas públicas, empresas* são dados extraídos de estatísticas e de análises de tendências dos depósitos de pedidos de patente efetuados em determinados setores, que podem ser

[10] UnB (2015) define a expressão Informação Tecnológica como sendo "todo tipo de conhecimento sobre tecnologias de fabricação, de projeto e de gestão que favoreça a melhoria contínua da qualidade e a inovação no setor produtivo"..

usados na formulação de políticas governamentais e de ações estratégicas do planejamento de empresas.

O registro de Desenho Industrial é um título de propriedade temporário dentro do país, que confere ao titular o direito de excluir terceiros, durante o prazo de vigência do registro, de fabricar, comercializar, importar, usar ou vender a matéria protegida sem sua prévia autorização. Adequa-se a uma grande variedade de produtos industrializados e serve para incentivar o investimento em pesquisa e desenvolvimento de formas originais, capazes de gerar inovação (WIPO, OMPI, INPI, 2015).

As Indicações Geográficas, em seu conceito mais amplo, são indicações que identificam produtos ou serviços em razão de sua origem geográfica, e que incorporam atributos como reputação e fatores naturais e humanos, proporcionando produtos ou serviços com características próprias, que traduzem a identidade e a cultura de um espaço geográfico (WIPO, OMPI, INPI, 2015)

A PI é um instrumento que pode estimular concorrência e incentivar a inovação, visto que, a concorrência é uma disputa benéfica ao sistema econômico que ocorre entre agentes econômicos produtores de um mesmo bem ou serviço no mercado, estimulando-os a produzir bens e serviços novos ou aperfeiçoados. A Concorrência Desleal representa condutas anticompetitivas, causando prejuízo à livre concorrência entre empresas do mesmo segmento produtivo, e a proteção dos direitos de Propriedade Industrial não consegue impedir a variedade de atos de má-fé, tais como a divulgação de informações equivocadas pelo concorrente, criação de confusão e indução ao erro, a propaganda enganosa e a violação de segredo de fábrica e tirar vantagem das realizações de terceiro, geralmente, não são tratadas pela legislação específica da propriedade industrial (WIPO, OMPI, INPI, 2015)

As empresas podem explorar seus ativos intangíveis de forma direta e indireta, por meio da celebração de contrato de licenciamento ou cessão (venda) de direitos de propriedade intelectual ou por contratos de transferência de tecnologia, conforme citação:

> As empresas que possuem ativos intangíveis exploram esses diferenciais quando perseguem os resultados econômicos por meio da atuação direta no mercado. A exploração dos ativos intangíveis também pode ocorrer de forma indireta, por meio da celebração de contrato de licenciamento ou cessão (venda) de direitos de propriedade

> intelectual ou por contratos de transferência de tecnologia. Esses negócios envolvendo direitos de propriedade industrial e outros ativos de propriedade intelectual, organizados a partir de acordos voluntários, compõem o mercado de ativos intangíveis e de transferência de tecnologia.
> No mercado de ativos intangíveis, os detentores de direitos de propriedade autorizam a exploração econômica desses direitos mediante o pagamento de royalties, conforme condições estabelecidas no contrato de licenciamento. Os titulares dos direitos de propriedade industrial também podem ceder esses direitos aos interessados nos termos previstos nos acordos de cessão. (WIPO, OMPI, INPI, 2015).

Quando os ativos intangíveis de uma empresa não possuírem proteção prevista nos Direitos de Propriedade Industrial, porque não possuem requisitos para tal ou for de interesse do detentor, os negócios são firmados por meio de contratos de fornecimento de tecnologia ou prestação de serviços de assistência técnica, como é o caso dos serviços de assistência técnica e do *know how* (WIPO, OMPI, INPI, 2015).

O contrato estabelece o acordo entre as partes, que resulta em obrigações recíprocas e direitos a cada uma delas, com vínculo jurídico (BOCCHINO et al., 2010), e para tal necessita de elementos para sua validação, conforme citação:

> O Código Civil, nos arts. 421 a 853, regulamenta os elementos necessários à validação dos contratos, no que tange aos negócios jurídicos, e sendo o contrato um negócio jurídico, o mesmo deve ser praticado na observância de certos pressupostos, e em alguns casos, um formalismo imposto pela lei. (BOCCHIO et al., 2010, p. 48)

Pimentel (2009b) nos apresenta um modelo de contrato aplicável à proteção do conhecimento, com os elementos necessários para sua validação legal, conforme Quadro 12.

Quadro 12 - Principais cláusulas contratuais

CONTRATO DE (*Título*)	
Preâmbulo	– Qualificação das partes, executores e intervenientes – Aviso de adesão – Considerandos – Definições de termos e expressões – Comunicações
Cláusula	– Objeto – Exclusividade – Territorialidade
Cláusula	– Preço – Condições de pagamento – Garantia de pagamento
Cláusula	– Pagamento intelectual
Cláusula	– Confidencialidade
Cláusula	– Garantia – Responsabilidades
Cláusula	– Outras obrigações – Dados, informações – Requisitos de qualificação pessoal – Atualizações e novas versões – Notificações e auditoria
Cláusula	– Prazo
Cláusula	– Extinção
Cláusula	– Clausula penal
Cláusula	– Alteração contratual – Autonomia das cláusulas – Transferência
Cláusula	– Lei aplicável
Cláusula	– Foro ou cláusula compromissória de arbitragem
Fechamento	– Local e data – Assinaturas dos contratantes e intervenientes – Assinaturas e CPF de duas testemunhas

Fonte: Pimentel (2009b, p. 263).

Quanto aos contratos de tecnologia, SILVEIRA (1985) entende que o objetivo principal está no segredo industrial ou do negócio, que

contém os conhecimentos secretos e não secretos de difícil acesso, relativos a um produto ou processo industrial ou gerencial.

2.4.3 Segurança e Proteção da Informação e do Conhecimento

A segurança em uma organização está relacionada à gestão de seus ativos. Cabe a organização proteger seus ativos, mitigar os riscos, e gerenciar de forma eficiente e eficaz seus recursos, visando seu crescimento e sustentabilidade no mercado. O conhecimento, ou ativos de conhecimento, e a informação, ou ativos de informação, incorporam o grupo de ativos intelectuais da organização. (EDVINSSON e MAMONE, 1998; SVEIBY, 2001; ARAÚJO, 2009).

Ambos possuem valores próprios, e para aqueles considerados valiosos há necessidade de se gerir e de assegurar sua proteção, pois nem todo ativo deve ser protegido devido ao esforço e custos envolvidos. (RYAN, 2006; DESOUZA, 2007; ARAÚJO, 2009; DESOUZA e PAQUETTE, 2011)

A gestão e a segurança devem ir além do conhecimento e da informação, e incluir as pessoas, os processos, e a tecnologia, (DESOUZA e PAQUETTE, 2011; ARAÚJO, 2009).

No âmbito administração pública, a LEI Nº 12.527, de 18 de novembro de 2011 chamada de Lei de Acesso a Informação (LAI), que assegura o direito fundamental de acesso à informação, tem como regra geral a observância da publicidade da informação e considera o sigilo uma exceção (BRASIL, 2011).

É justamente na exceção da LAI que reside algumas das regras da Gestão segurança da informação para os órgãos da Administração Pública, como por exemplo, a de não dar acesso as informações referentes a projetos de P&D cujo sigilo seja imprescindível à segurança da sociedade e do Estado; respeitar as hipóteses legais de sigilo e de segredo de justiça e as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado.

Do art 3º da LAI, retiramos algumas definições úteis ao nosso entendimento sobre a segurança da informação, que são:

- Informação sigilosa: é a informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

- Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.
- Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados.
- Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema.
- Integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino.
- Primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações. (BRASIL, 2011).

Dentre as considerações sobre a segurança da sociedade ou do Estado, previstas no art. 6 da LAI, destacamos:

- Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional.
- Prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas.
- Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional.
- Comprometer atividades de inteligência. (BRASIL, 2011).

Os prazos máximos de restrição de acesso à informação, previstos no Art. 24 da LAI, obedecerão sua classificação quanto ao grau de sigilo, conforme:

- Ultrassecreta: 25 (vinte e cinco) anos.
- Secreta: 15 (quinze) anos.
- Reservada: 5 (cinco) anos. (BRASIL, 2011)

A Política de Segurança da Informação para os órgãos da APF instituída pelo Decreto nº 3.505, de 13 de junho de 2000, define Segurança da Informação como:

> (...) proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaça a seu desenvolvimento (BRASIL, 2000).

Ainda sobre políticas, a NBR ISO/IEC 27002 (2013b) recomenda o estabelecimento da Política de segurança da informação, que é um documento que declara o comprometimento da alta administração e seu apoio aos princípios e metas da segurança da informação, e deve ser publicado e comunicado para todos os funcionários e partes externas.

Com relação ao tratamento de informação classificada, a NBR-16167 (2013a) prevê um conjunto de ações referentes à produção, recepção, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento e eliminação. A norma também destaca o princípio da necessidade de acesso, que pode ser entendido como: "As pessoas somente devem possuir acesso às informações que sejam necessárias, direta ou indiretamente, ao desenvolvimento de suas atividades de trabalho e demais responsabilidades associadas" (NBR-16167, 2013a, p.1 e 3).

A conformidade da organização às boas práticas de governança e gestão da Tecnologia da Informação (TI), tais como *Control Objectives for Information and related Technology* (COBIT) e *Information Technology Infrastructure Library* (ITIL) asseguram benefícios para a segurança da informação.

De acordo com ISACA (2012), o modelo corporativo para governança e gestão de TI do COBIT permite auxiliar as organizações a atingirem seus objetivos de governança, pois considera a importância da tecnologia e da informação na organização, nos ambientes sociais, públicos e corporativos, desde sua criação até sua destruição, e tem por objetivos:

- Manter informações de alta qualidade para apoiar decisões corporativas.
- Agregar valor ao negócio a partir dos investimentos em TI, ou seja, atingir os objetivos estratégicos e obter benefícios para a organização através da utilização eficiente e inovadora de TI.
- Alcançar excelência operacional por meio da aplicação confiável e eficiente da tecnologia.
- Manter o risco de TI em um nível aceitável.
- Otimizar o custo da tecnologia e dos serviços de TI.
- Cumprir as leis, regulamentos, acordos contratuais e políticas pertinentes cada vez mais presentes. (ISACA, 2012)

O ITIL é um modelo para gerenciamento de serviços de TI, que é organizado em torno do ciclo de vida de um serviço dentro de uma organização e abrange as seguintes etapas (ITSMF, 2007):

- Estratégia do Serviço (*Service Strategy*): Define os requisitos e necessidades do negócio.
- Projeto de Serviço (*Service Design*): Define a solução a ser adotada.
- Transição de Serviço (*Service Transition*): Relacionado ao gerenciamento de mudanças
- Operação do Serviço (*Service Operation*): Assegura que os serviços estão sendo atendidos baseado nos Acordos de Nível de Serviços (SLAs)
- Melhoria Contínua do Serviço (*Continual Service Improvement*): Manter a constante melhoria dos serviços baseando-se no ciclo PDCA (*Plan-Do-Check-Action*). ITSMF, 2007)

A revisão da literatura revelou que vários autores desenvolveram diferentes perspectivas de abordagem para estudar o conhecimento e as experiências e habilidades pessoais, por considerarem ativos essenciais para as organizações. Dentre as várias perspectivas, como: a gestão (ILVONEN, 2013; CHOO, 2003; MAIER, 2007), e a criação (NONAKA, 1994; NONAKA et al., 2000; VON KROGH, 2009, 2012); e a importância do conhecimento nas organizações como um ativo organizacional (SVEIBY, 2001; NOLD 2012), e poucos autores

desenvolveram estudos sobre a segurança do conhecimento (DESOUZA, 2007; ARAÚJO, 2009).

Na visão de Ilvonen (2013, p.2), é importante tratar o conhecimento como parte do capital humano, pois o conhecimento refere-se às pessoas que o possui, e que, do ponto de vista da empresa, todos os bens de capital, físico, monetário, e intelectual, devem ser protegidos por atividades de segurança.

Araújo (2009), afirma que tanto o conhecimento como a informação devem ser tratados como capital intelectual da organização, pois a informação é um dos agentes de transformação do conhecimento, conforme citação:

> Por essa razão não se pode promover a gestão do conhecimento sem a gestão da informação. Como o conhecimento, a informação também passou a ser valorada e contabilizada como parte do capital da organização. A informação e o conhecimento passaram a ser identificados e tratados como parte do capital intelectual da organização. (ARAÚJO, 2009, p.99).

Considerando o conhecimento como parte do capital em uma organização, Figueiredo (2005) atribui valor ao conhecimento de acordo com: custo para proteger; preocupação em proteger; r*eturn on investment* (ROI); custo de perda do conhecimento; compromisso futuro; riscos de fuga do conhecimento; valor de mercado do conhecimento; e dificuldade em proteger.

Outras questões requerem atenção, como as levantadas por Araújo (2009), que aponta a perda do conhecimento por meio de problemas de quebra de patentes, de sigilo, de cláusulas contratuais, e outras, conforme citação:

> São comuns os relatos sobre problemas relacionados à perda de conhecimento. Problemas de quebra de patentes, quebra de sigilo, quebra de regras de contrato, tráfico de informações, espionagem, exposição de dados e problemas relacionados à perda de pessoal assombram as organizações. Nos casos relacionados às pessoas, são comuns as situações onde funcionários que detinham conhecimentos essenciais para a realização de atividades na organização foram

> embora por aposentadoria ou em alguns casos recrutados pela concorrência (ARAUJO, 2009, p.89-90)

De outro ponto de vista, Rocha et al. [200?] descrevem que a proteção do conhecimento deve ser vista não somente sobre a questão de proteção do patrimônio, pois existe o caráter estratégico do conhecimento, que envolve a gestão do conhecimento e a proteção do conhecimento, e acrescenta:

> Trata-se não só da capacidade de produção de conhecimento, mas também da capacidade de compartilhá-lo corretamente e protegê-lo quando necessário. Aqui, o ponto de vista passa a ser estratégico, pois o conhecimento estruturado, atualizado, corretamente aplicado e protegido é uma grande vantagem competitiva num mundo globalizado e rápido como o de hoje (ROCHA et al., 200?, p.1)

Neste contexto, porém, a proteção do conhecimento não é tão valorizada por parte das empresas, como afirma Desouza (2007, p.5) "apesar de a parte humana ser o elo mais fraco, quando discutimos proteção do conhecimento é exatamente esta dimensão a menos valorizada pela gerência das empresas".

Segundo Desouza e Paquette (2011), para se gerir o conhecimento quatro componentes são essenciais: conhecimento, pessoas, processos e tecnologia. A condição essencial para a GC é gerir o conhecimento considerado valioso. Diferentes formas de atribuição de valores para o conhecimento influenciam na alocação de recursos para gerenciá-los. Por exemplo, os programas de segurança que protegem o conhecimento estratégico, pois todas as nações têm um grande cuidado em assegurar o conhecimento estratégico no contexto de operações e missões de segurança nacional.

Os autores apresentam que o acesso aos artefatos de conhecimento, programas e processos estejam limitados a: a) pessoas que possuem credenciais de segurança necessárias que determinam os níveis de acesso, e b) aqueles que precisam saber. Dinâmica semelhante ocorre em organizações privadas, que usam uma grande variedade de instrumentos legais para proteger sua propriedade intelectual e atribuir valor ao seu conhecimento.

A proposta de Gold, Malhotra e Seagars (2001) aborda a GC considerando duas capacidades relacionadas à eficácia organizacional: a) a capacidade de infraestrutura de conhecimento, que detalha aspectos da tecnologia, da estrutura e da cultura, e b) capacidade de processos de conhecimento, que aborda aspectos da aquisição, da conversão, da aplicação e da proteção, conforme Figura 10.

Figura 10 – Capacidade da Gestão do Conhecimento e Eficiência Organizacional

Fonte: Gold, Malhotra e Seagars (2001, tradução nossa).

A capacidade da infraestrutura de conhecimento é composta pela *tecnologia*, que é a responsável pela criação de novos conhecimentos por meio da integração dos fluxos de informação e conhecimento; a *estrutura*, que diz respeito a presença de normas e mecanismos de confiança que permitem o compartilhamento do conhecimento no ambiente interno da organização; e a *cultura*, essencial para o processo de inovação porque possibilita a interação entre as pessoas. (GOLD, MALHOTRA e SEAGARS, 2001)

A capacidade dos processos de conhecimento é a essencial para gerir o conhecimento dentro da organização. O processo *aquisição* é

responsável pela obtenção e acúmulo do conhecimento; o processo *conversão* por fazer o conhecimento existente utilizável; o processo *aplicação* pelo uso do conhecimento atual; e o processo de *proteção* é o responsável pela proteção contra o uso ilegal ou inapropriado do conhecimento na organização, garantindo o ciclo de vida do conhecimento. (GOLD, MALHOTRA e SEAGARS, 2001)

Quanto ao processo *proteção*, da abordagem de Gold, Malhotra e Seagars (2001), os autores recomendam observar dez tipos de processo proteção, são eles:

1) Processos para proteger o conhecimento do uso inadequado dentro da organização.
2) Processos para proteger o conhecimento do uso inadequado de fora da organização.
3) Processos para proteger o conhecimento de roubo originário dentro da organização.
4) Processos para proteger o conhecimento contra roubo de fora da organização.
5) Incentivos que encorajem a proteção do conhecimento.
6) Tecnologia que restringe o acesso a algumas fontes de conhecimento.
7) Políticas e procedimentos extensos para proteger os segredos comerciais.
8) A organização valorizando e protegendo o conhecimento incorporado nos indivíduos.
9) Identificação clara do conhecimento restrito.
10) Comunicação clara sobre a importância da proteção do conhecimento. (GOLD, MALHOTRA e SEAGARS, 2001).

Também verificado por Ilvonen (2013), a abordagem de Gold, Malhotra e Seagars (2001) foi adotada por outros autores em seus estudos sobre a Gestão do Conhecimento, como por exemplo: Sandhawalia & Dalcher (2011), Smith (2007) e Ding et al. (2013).

Destacamos Smith (2007), que realizou o estudo utilizando o modelo desenvolvido por Gold, Malhotra e Seagars (2001), onde afirma que a tecnologia, a estrutura organizacional, a cultura organizacional, a aquisição de conhecimentos, a conversão do conhecimento, a aplicação do conhecimento e a proteção do conhecimento são condições prévias exigidas para capacidades efetivas de gestão do conhecimento; e que as capacidades efetivas de gestão do conhecimento são os antecedentes para a eficácia organizacional.

Concluiu que a tecnologia, estrutura e cultura são componentes significativos de capacidade de infraestrutura de conhecimento e que a aplicação do conhecimento, aquisição de conhecimento, de conversão do conhecimento e proteção do conhecimento são componentes significativos de capacidade do processo de conhecimento.

Além disso, tanto a capacidade de infraestrutura de conhecimento e capacidade de processo de conhecimento impactado significativamente a eficácia organizacional. No entanto, nenhuma evidência empírica foi encontrada para sugerir que o recurso de conhecimento relacionado com a estratégia de negócio vai melhorar ainda mais a eficácia organizacional.

Em outros estudos selecionados na base de dados SCOPUS, encontramos as razões: muitos associaram a proteção do conhecimento à inovação; o aspecto humano no processo de proteção como tópico quase unânime nos estudos; a falta de sensibilização ao tema propicia a não adoção de mecanismos de proteção do conhecimento; e o tamanho da empresa influencia a escolha do mecanismo de proteção para a empresa.

A universidade foi outro contexto abordado nos estudos sobre proteção do conhecimento. Em seu trabalho, Gonçalves (2012) constatou que a falta de uma política de proteção de conhecimento na instituição desfavorece a sensibilidade dos pesquisadores para a questão, e não as tornam evidentes, conforme:

> Não ter diretrizes de proteção ao conhecimento talvez "colabore para a falta de sensibilização dos pesquisadores para a proteção do conhecimento e inovação [...] as vantagens da proteção do conhecimento ainda não estão evidentes para os pesquisadores da UEL" (GONÇALVES, 2012, p.132)

Olander; Hurmelinna-Laukkanen; e Heilmann (2011) ao abordarem o ambiente empresarial de Pequenas e Médias Empresas (PME) onde há geração e gestão da inovação, destacam que os funcionários criativos são os recursos mais valiosos, e que o vazamento e a perda de conhecimento são os principais riscos relacionados com o pessoal. Apresentam cinco mecanismos de proteção do conhecimento relacionados à gestão de recursos humanos: recrutamento, educação e treinamento sobre confidencialidade, retenção de funcionários, a captura e difusão de conhecimento internos, e monitoramento, conforme citação:

> Em termos de geração e gestão da inovação, os funcionários criativos são os recursos mais valiosos nas pequenas empresas. Assim, o vazamento de conhecimento é o principal risco relacionado ao pessoal. A proteção dos conhecimentos relacionados com a gestão de recursos humanos é uma forma eficaz de lidar com estes desafios, embora isso nem sempre seja reconhecido por acadêmicos ou por gerentes. Isto é particularmente valioso na salvaguarda do conhecimento existente da empresa, e criando assim as condições para a inovação futura. (...) A contribuição teórica do estudo é apresentar e testar empiricamente uma tipologia de cinco mecanismos de proteção do conhecimento relacionadas com a gestão de recursos humanos: recrutamento, educação e treinamento sobre confidencialidade, retenção de funcionários, a captura e difusão de conhecimento internos, e monitoramento. (OLANDER; HUMELINNA-LAUKKANEN; e HEILMANN, 2011, p. 593 – tradução nossa.)

A preocupação com as pessoas na questão de proteção do conhecimento também é abordada por Jacinto (2008):

> A questão humana como fonte de instabilidade para a segurança relacionada ao conhecimento vem sendo amplamente apresentada, mas insuficientemente tratada. Apesar dos alertas relacionados à importância da conscientização das pessoas a respeito das vulnerabilidades e ameaças a que estão expostas, muito pouco, além de alarmes e pânico é oferecido a elas. (JACINTO, 2008, p. 20)

Embora o mesmo autor se refira ao conhecimento organizacional, essa abordagem pode ser considerada na pesquisa, pois o segredo é um conhecimento:

> Em virtude disso, faz-se necessário estudo que oriente as empresas de modo a se implementar ações que tornem sistemáticos os processos organizacionais de identificação dos riscos e ameaças para a proteção do conhecimento e que incluam as pessoas nesse contexto, a fim de

> estimular o entendimento e sua participação no processo de segurança e privacidade do conhecimento organizacional. (JACINTO, 2008, p. 21)

Gonçalves (2012, p. 21) ressalta o papel das patentes, ao afirmar que As patentes protegem "os direitos do inventor/autor, maximizando a geração de novos conhecimentos por meio da divulgação de informações técnicas, incentivando, portanto, a inovação".

Jacinto (2008) aborda a proteção do conhecimento destacando a Segurança da Informação e o Gerenciamento de Risco, a atenção aos processos organizacionais e as pessoas. Para a Gestão do Conhecimento e sua proteção, destaca as capacidades de infraestrutura e de processos como elementos de proteção do conhecimento. Apresenta a engenharia social como uma ameaça à proteção e privacidade do conhecimento.

> O que se observa é que incidentes de segurança são cada vez mais frequentes em virtude de diversos fatores, dentre eles o fato da maior exposição e velocidade com que o conhecimento é disponibilizado através de recursos computacionais.
> (...) diversas metodologias e soluções tecnológicas são desenvolvidas para sustentar o atendimento à proteção do conhecimento e das informações. O que se observa, no entanto, é que apesar do significativo aumento de melhores práticas e novas tecnologias constantemente ofertadas para o tratamento do problema, pouco se oferece em relação a identificação e tratamento dos riscos e ameaças de segurança e privacidade do conhecimento organizacional do ponto de vista de processos organizacionais e da participação de pessoas nesse contexto. (JACINTO, 2008, p. 20).

Bolisani; Paiola; e Scarso (2013, p. 193) citam que as empresas do tipo *Knowledge Intensive Business Services* (KIBS) vivem um dilema e que precisam estar abertas às relações externas e gerenciar de maneira eficaz a troca de conhecimento com seus fornecedores e clientes, por outro lado, elas têm que proteger o desenvolvimento e a capitalização de ativos cognitivos internos que constituem o *core* de seu negócio. O estudo realizado pelos autores apresenta que:

> No conjunto, a pesquisa mostra que a abordagem de uso da proteção do conhecimento, e em especial dos métodos formais, é freqüente nas empresas KIBS. As descobertas confirmaram que o nível de utilização e tipos de métodos de proteção do conhecimento adotados variam substancialmente entre as indústrias, mas algumas diferenças se comparadas as análises anteriores (...) as empresas KIBS de alta tecnologia (...) tendem a proteger menos seus conhecimentos. Entretanto, os dados confirmam que as grandes companhias são geralmente mais inclinadas a usar métodos de proteção do conhecimento, embora a variação de métodos usados não mudam com o tamanho. (BOLISANI; PAIOLA; e SCARSO, 2013, p. 206 – tradução nossa.)

Outro estudo foi realizado por De Faria e Sofka (2010), que investigaram as escolhas dos gerentes de subsidiárias multinacionais quanto às estratégias de proteção do conhecimento, incluindo além dos métodos formais (patentes, direitos autorais e marcas) aspectos estratégicos (sigilo, prazo, complexidade do projeto). Portanto, as abordagens diferem quanto aos desafios e oportunidades do país sede, e acrescenta:

> Nosso raciocínio teórico nos leva a crer que este efeito pode ser explicado pela necessidade de reciprocidade nas trocas de conhecimento dos países tecnologicamente avançados. Com base na aceitação das vulnerabilidades para os fluxos de conhecimento podem ser estabelecidos um sentimento de confiança entre os parceiros. (DE FARIA e SOFKA, 2010, p. 965- tradução nossa.)

Neste contexto, González-Álvarez,e Nieto-Antolín (2007) também analisaram os fatores que determinam a escolha entre vários mecanismos disponíveis para as empresas apropriarem-se dos resultados das suas atividades inovadoras, tais como: patentes, segredo industrial, custo e tempo de imitação e inovação contínua, e concluíram que as empresas onde o conhecimento tácito predomina optam por usar o segredo industrial, que as grandes empresas optam por usar as patentes como mecanismo de proteção.

A abordagem sobre vazamento de conhecimento foi apresentada no estudo de Vasconcelos e Jamil (2008), relatando que:

> O conceito de vazamento de conhecimento (*knowledge leakage)* ainda representa um ponto pouco discutido na literatura sobre gestão do conhecimento. Outros termos podem ser encontrados para designar este fenômeno: perda ou fuga de conhecimento (*knowledge loss*), escoamento de conhecimento (*knowledge seepage*) ou exposição/revelação de conhecimento (*knowledge disclosure*). (...)
> É importante ressaltar que o vazamento de conhecimento se refere tanto à absorção como à transferência de conhecimento, que acontece na interação das empresas com o seu ambiente de trabalho. As conseqüências ou impactos desse vazamento, na vida das empresas, podem ser positivos ou negativos. (VASCONCELOS e JAMIL, 2008, p. 99)

Assim, o estudo dos autores concluiu que:

> O vazamento é ainda fortemente associado aos impactos negativos e não aos impactos positivos, conforme descrito na literatura. As principais rotas de vazamento positivo de conhecimento foram: contratação de talentos, treinamento, parcerias com universidades tradicionais, além dos benefícios das universidades corporativas. Os consultores foram citados como sendo uma possível rota de vazamento de conhecimento, com impacto negativo, devendo sua atividade ser monitorada. Além disto, foi mostrada grande preocupação com a perda de funcionários "chave" para a concorrência, que representa outra rota de vazamento de conhecimento com impacto negativo. Outras rotas citadas foram: roubo, desleixo ou indiferença do colaborador, falhas no sistema eletrônico, revistas e jornais da empresa, serviços terceirizados e até mesmo a espionagem industrial.
> Pôde-se concluir que as empresas brasileiras pesquisadas já estão atentas para algumas rotas

> de vazamento de conhecimento e para os impactos positivos e negativos deste vazamento, mas muito ainda precisa ser feito para uma gerência eficaz deste processo, visando maximizar os efeitos positivos, minimizar os negativos e proteger o seu conhecimento estratégico. (VASCONCELOS e JAMIL, 2008, p. 113)

Como citado anteriormente, sobre a plataforma do Sistema de Gestão do Conhecimento, Maier (2007, p. 72-73) apontou a proteção do conhecimento valioso como um desafio importante da Gestão do Conhecimento nas organizações. Dentre as medidas para impedir o uso indesejado do conhecimento organizacional apontou as leis de classificação e de propriedade; os instrumentos organizacionais tais como incentivos, regras de conduta, recompensas.

Assim, a concepção dos Sistemas de Gestão de Conhecimento deve descrever como o conhecimento valioso pode ser protegido, evitando, por exemplo, sua saída intencional da organização.

No estudo realizado por Nascimento (2008) são apresentadas algumas diferenciações sobre a forma de garantir a segurança e a proteção da informação e do conhecimento.

A autora destaca que na década de 1950 a 1970 a segurança se limitava ao acesso físico a sistemas de computadores e ocupavam espaços bem definidos dentro da organização. Na década de 1980, o uso dos microcomputadores e a possibilidade de comunicação em rede, ampliou o foco da segurança da informação, conforme a citação:

> (...) o surgimento de microcomputadores e a possibilidade de comunicação em rede, até os dias atuais em que a conectividade e o compartilhamento de recursos, de tempo e da informação alcançaram níveis tão amplos, o foco da sgurança da informação mudou, passando a ter uma abrangêcia muito mais ampla. Cumpre destacar que ao lado da evolução dos sistemas de informação e comunicação temos a evolução das relações políticas, overnamentais, organizacionais, comerciais, por exemplo, para uma sociedade conectada, globbalizada e altamente competitiva, onde as ameaças, os riscos e as vulnerabilidades de segurança aumentam exponencialmente tanto em

> número quando nas formas de atuação. (NASCIMENTO, 2008, p. 137)

Também observou também, a mudança de preocupação das organizações em relação à segurança de seus ativos, que antes era sobre seus ativos patrimoniais e passou a atenção para os ativos de informação (NASCIMENTO, 2008, p. 137)

A mesma autora, destaca, porém, que a Segurança da Informação tem por objetivo "garantir aspectos relacionados à integridade, disponibilidade, autenticidade e sigilo do conhecimento registrado (informação), sem considerar os conhecimentos que circulam na organização". Sua preocupação recai sobre os registros físicos que contém as informações registradas, embora tenham acesso lógico, "seu foco visa àquelas informações que já estão prontas, acabadas e documentadas em estoques de informação", e não "considera os momentos da criação, do processamento, do compartilhamento e da assimilação, ações puramente humanas" (NASCIMENTO, 2008, p. 139-140).

Deste modo, os objetivos, conteúdos e controles da segurança da informação diferem dos da proteção ao conhecimento, como apresentado no Quadro 13.

Quadro 13 – Principais diferenças entre Segurança da Informação e Proteção ao Conhecimento

	SEGURANÇA DA INFORMAÇÃO	PROTEÇÃO AO CONHECIMENTO
OBJETIVOS	– Prevenir, detectar, anular e registrar ameaças reais ou potenciais a dados e informações.	– Prevenir, detectar, anular e registrar ameaças reais ou potenciais a dados e informações e conhecimentos.
	– Garantir o sigilo, a integridade e a disponibilidade de dados, informações e documentos gerados, armazenados, codificados ou em trânsito em uma organização.	– Garantir o sigilo, a integridade e a disponibilidade de dados, informações e conhecimentos gerados, compartilhados e que circulam na organização, em qualquer suporte informacional, especialmente associado a sistemas humanos.
CONTEÚDOS	– Estruturado: documentos, produtos, banco de dados, processos.	– Não estruturado, compartilhado, observado, apreendido: ações, contextos, experiências.
CONTROLES	– Leis: patentes, direito autoral, marcas. – Tecnologia. – Política, normas e procedimentos.	– Conscientização. – Educação. – Cultura.

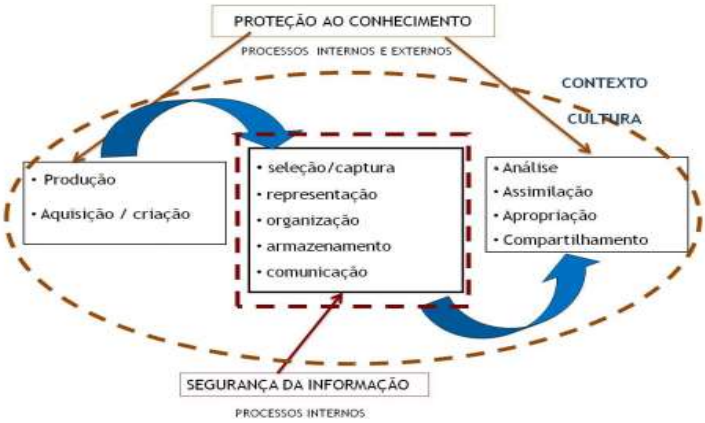
Fonte: Elaboração da autora, baseado em Nascimento (2008, p. 142-143).

Neste contexto, Nascimento (2008) destaca que a Gestão da Informação trata do conhecimento que foi explicitado e documentado, onde se associa à segurança da informação. A Gestão do Conhecimento, por sua vez, inclui o trato ao conhecimento tácito, ao conhecimento em fluxo, que ainda está em processamento, ao que ainda não foi documentado, e por meio da explicitação e do registro desencadeia suas ações de proteção, para que o conhecimento não se perca ou caia no esquecimento. A proteção ao Conhecimento representa um "processo que estabelece relaçoes e interconexões entre as duas formas de gestão" (NASCIMENTO, 2008, p. 142, 143), e é definida como:

> A proteção ao conhecimento abrange todo o escopo dos ativos informacionais de uma organização, olhando para além dos processos internos do ciclo da informação; ela está associada a sistemas humanos na busca/coleta, criação, análise, compartilhamento e assimilação de conhecimentos, bem coo em toda a complexidade envolvida quando se trata com seres humanos, deixando de ser, apenas, uma questão de segurança de estoques de informação corporativos. (NASCIMENTO, 2008, p. 141)

A Figura 11 apresenta a abordagem de Nascimento (2008) sobre os processos que estão relacionados à Segurança da Informação e dos processos relacionados à proteção ao conhecimento.

Figura 11 – Processos de Segurança da Informação e de Proteção ao Conhecimento



Fonte: NASCIMENTO (2008)

O modelo para a proteção ao conhecimento, proposto pela autora, teve por fundamentação a Metodologia de Sistemas Flexíveis (SSM) desenvolvida por Checkland (1999), que possui sete estágios: contextualização; coleta de dados; estruturação formalizada da situação-problema modelo conceitual; comparação do Modelo com a situação-problema; plano de ação; implementação.

2.4.4 Segurança e Proteção da Informação e Conhecimento de Defesa

Iniciamos esse subcapítulo apresentando vários entendimentos extraídos do Manual Básico – Volume I, Elementos Fundamentais, da Escola Superior de Guerra (ESG) sobre segurança no âmbito da Defesa, conforme Quadro 14.

Quadro 14 – Definições de Segurança na Área de Defesa

CONCEITO	FONTE
Segurança é uma necessidade, uma aspiração e um direito inalienável do ser humano.	ESG (2011, p.64)
O entendimento do que seja Segurança permite discernir, sempre, uma noção de garantia, proteção ou tranquilidade em face de obstáculos e ameaças, ações contrárias à pessoa, às instituições ou aos bens essenciais, existentes ou pretendidos.	ESG (2011, p.64)
Assim, o conceito de Segurança, em sentido amplo, abrange a garantia contra todas as formas de ameaça em relação ao indivíduo ou aos grupos sociais, podendo assumir diferentes matizes.	ESG (2011, p.65)
Segurança é a sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza.	ESG (2011, p.65)
A Segurança, sendo uma sensação, não pode ser medida, é abstrata, subjetiva.	ESG (2011, p.65)
Tudo o que pode ameaçar a tranquilidade do Homem, individual ou coletivamente, dificultar ou impedir a proteção que julga ser seu direito, causar temores, e o que é capaz de gerar conflitos, constituem as chamadas **razões de insegurança.**	ESG (2011, p.65)
A sensação de se sentir seguro é função direta da ausência de fatores perturbadores que tenham a capacidade de alterar esse estado; são as **ameaças.** Estas sim têm que ser, além de conhecidas, também avaliadas para que, devidamente tratadas, tenham sua influência reduzida para que se possa manter o estado de segurança adequado.	ESG (2011, p.65)
Segurança é sensação, ao passo que Defesa é ação.	ESG (2011, p.65)

Fonte: Elaboração da autora, 2015, com base em ESG (2011).

No Âmbito da Defesa, as medidas de proteção da informação e do conhecimento são definidas na Doutrina de Inteligência de Defesa (DID), que as reúne com o nome de Contra-Inteligência.

Eventualmente, de forma equivocada, a atividade de Contra-Inteligência, que emprega atos legais e não ofensivos, é relacionada à espionagem, que não limita suas ações para atender seus objetivos.

- Ramo da Contra-Inteligência

A Contra-Inteligência (CI) é o ramo da AID responsável pela salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de tecnologia da informação) de interesse da Defesa, contra a ação adversa de pessoas, órgãos e organizações de Inteligência, ou de outras ameaças (ESG, 2005, p. 27).

> A CI projeta suas ações para além dos limites do SINDE alcançando, por conseguinte, o conhecimento e/ou dado a salvaguardar, onde quer que ele se encontre. Deve-se ressaltar que, fora do âmbito desse Sistema, a proteção dos conhecimentos e/ou dados sigilosos é da responsabilidade dos respectivos custodiantes cabendo, nesse caso, aos Órgãos de Inteligência a responsabilidade de assessorá-los (ESG, 2005, p. 27).

Toda e qualquer atividade de caráter sigiloso relacionada aos interesses da Defesa está relacionada à CI, que "propõe a adoção de medidas que se contraponham, dentre outras, às ações contra sistemas informatizados, à desinformação, à espionagem, às ações de influência psicológica, à sabotagem, ao terrorismo, etc", e tem as seguintes atribuições (ESG, 2005, p. 27):

a. Estabelecer um quadro de ameaças efetivas ou potenciais à salvaguarda dos conhecimentos de interesse da Defesa e seus suportes, representadas pelas ações de serviços de Inteligência adversa e ações de qualquer natureza.
b. Identificar deficiências e vulnerabilidades na salvaguarda dos conhecimentos de interesse da Defesa e seus suportes.
c. Propor medidas que resultem no estabelecimento do nível desejável de salvaguarda dos conhecimentos de interesse da Defesa e seus suportes.

d. Propor ações especializadas a serem empregadas com a finalidade de iludir e confundir o processo decisório adverso. (ESG, 2005, p. 27).

A CI racionaliza a execução de suas ações dividindo-as em dois segmentos: a Segurança Orgânica (Seg Org), e a Segurança Ativa (Seg Atv), que implementam medidas para "detecção, identificação, neutralização, obstrução e prevenção da atuação da Inteligência adversa e das ações de qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos e seus suportes (...) de interesse da Defesa" (ESG, 2005, p. 28).

O segmento Seg Org busca "obter um grau de proteção ideal, por meio da adoção eficaz e consciente de um conjunto de medidas destinadas a prevenir e obstruir as ações de qualquer natureza que ameacem a salvaguarda de dados, conhecimentos e seus suportes de interesse da Defesa", tais como (ESG, 2005, p. 28):

a. Programas de conscientização, destinados a criar mentalidade, motivar e comprometer as pessoas envolvidas.
b. Documentos destinados a formalizar as medidas a serem adotadas.
c. Programa de treinamento continuado sobre os fundamentos, as medidas de Seg Org e outros julgados necessários.
d. Estruturas para gerência, auditoria e validação da Seg Org de um sistema ou de parte dele.
e. Serviços e os mecanismos de Seg Org necessários para dar eficácia às medidas estabelecidas.
f. Medidas de contingência e de controle de danos. (ESG, 2005, p. 28)

As medidas de proteção direta dos dados, dos conhecimentos e seus suportes, são atendidas com a execução de algumas atividades, como (ESG, 2005, p. 28):

a. Proteção do Conhecimento no Pessoal - compreende um conjunto de medidas destinadas a assegurar comportamentos adequados à proteção de qualquer dado e conhecimento.
b. Proteção do Conhecimento na Documentação - compreende o conjunto de medidas voltadas para evitar o comprometimento de documentos, salvaguardando dados e/ou conhecimentos que devam ser protegidos, sigilosos ou

não, neles contidos. Os documentos, por constituírem o suporte mais comum de dados e conhecimentos, tornam-se alvos permanentes das ações hostis, em particular da espionagem.

c. Proteção do Conhecimento no Material - compreende o conjunto de medidas voltadas para protegerem dados e conhecimentos contidos em um determinado material. "Material" é entendido como toda matéria, substância ou artefato que contenha, utilize e/ou veicule dados e conhecimentos, que de posse de elemento(s) e/ou grupo(s) de natureza adversa, possa beneficiá-lo(s) ou atentar contra qualquer segmento de um sistema, de forma direta ou indireta.
d. Proteção do Conhecimento nos meios de TI - é o conjunto de medidas destinadas a preservar o sigilo das atividades de processamento, armazenamento, transmissão de dados digitais e comunicações, bem como a integridade dos sistemas, materiais e programas de TI, no sentido de salvaguardar dados e conhecimentos.
e. Proteção do Conhecimento nas Áreas e Instalações - compreende um conjunto de medidas voltadas para preservar dados e conhecimentos contidos em áreas e instalações. (ESG, 2005, p. 28)

O segmento Seg Atv refere-se à "adoção de medidas de caráter proativo destinado a detectar, identificar, avaliar e neutralizar as ações da Inteligência adversa e outras ações de qualquer natureza, dirigidas contra os interesses da Defesa", e se desdobra em dois grupos de medidas: Contra Ações Psicológicas; e Contraespionagem. Onde, a Contra Ações Psicológicas "é o conjunto de medidas destinado a contrapor-se às ações de influência psicológica, em especial a propaganda adversa, que possam causar prejuízos aos interesses da Defesa", e a Contraespionagem "é o conjunto de medidas destinado a contrapor-se às ações de espionagem", e ao "trabalho deliberado de elementos adversos, vinculados ou não à Inteligência adversa" (ESG, 2005, p. 28-29).

2.5 INOVAÇÃO

A Lei nº 13.243/2016 define Inovação como:

> (...) introdução de novidade ou aperfeiçoamento no ambiente produtivo e social que resulte em novos produtos, serviços ou processos ou que compreenda a agregação de novas funcionalidades ou características a produto, serviço ou processo já existente que possa resultar em melhorias e em efetivo ganho de qualidade ou desempenho (BRASIL, 2016).

Ao tratar da inovação tecnológica, o Manual Frascati faz uma distinção das atividades de inovação tecnológica e de P&D, conforme citação:

> As atividades de inovação tecnológica são o conjunto de diligências científicas, tecnológicas, organizacionais, financeiras e comerciais, incluindo o investimento em novos conhecimentos, que realizam ou destinam-se a levar à realização de produtos e processos tecnologicamente novos e melhores. P&D é apenas uma dessas atividades e pode ser realizada em diferentes estágios do processo de inovação, sendo usada não apenas como uma fonte de ideias inventivas, mas também para resolver os problemas que possam surgir em qualquer etapa do processo, até a sua conclusão. (OCDE, 2013, p. 23).

O Manual de OLSO define inovação, como:

> Uma inovação é a implementação de um produto (bem ou serviço) novo ou significativamente melhorado, ou um processo, ou um novo método de marketing, ou um novo método organizacional nas práticas de negócios, na organização do local de trabalho ou nas relações externas (OCDE, 1997, p. 55).

O mesmo manual define *inovação tecnológica de produto* como “a implantação/comercialização de um produto com características de desempenho aprimoradas de modo a fornecer objetivamente ao

consumidor serviços novos ou aprimorados"; e de *inovação de processo tecnológico* como a "implantação/adoção de métodos de produção ou comercialização novos ou significativamente aprimorados. Ela pode envolver mudanças de equipamento, recursos humanos, métodos de trabalho ou uma combinação destes".

Pimentel (2010a) nos diz que se pode realizar P&D de três maneiras:

> – P&D interna (inovação fechada): a empresa cria um departamento ou núcleo de pesquisa/desenvolvimento e contrata pesquisadores;
> – P&D externa (inovação externa): a empresa contrata a pesquisa e o desenvolvimento no mercado, com universidades e instituições especializadas, faz parcerias – ou ambas as opções; e
> – P&D mista (inovação aberta): a empresa cria um departamento, contrata pesquisadores e faz parcerias P&D visando à inovação. (PIMENTEL, 2010a, p. 370-371).

Tidd, Bessant e Pavitt (2008, p. 20) nos apresentam quatro tipos de inovação: a Inovação de Produto como sendo as "mudanças nas coisas (produtos/serviços) que uma empresa oferece"; a Inovação de Processo referentes as "mudanças na forma em que os produtos/serviços são criados e entregues"; a Inovação de Posição que compreende as "mudanças no contexto em que produtos/serviços são introduzidos"; e a Inovação de Paradigma como sendo as "mudanças nos modelos mentais subjacentes que orientam o que a empresa faz".

Os autores afirmam que a Inovação é um processo central para a organização, e que envolve três fases (TIDD, BESSANT e PAVITT, 2008, p. 87-88), são elas:

1. Fase da Procura, onde se deve "analisar o cenário (interno e externo) à procura de – e processar sinais relevantes sobre – ameaças e oportunidades para mudança".
2. Fase da Seleção, que "levando em consideração uma visão estratégica de como uma empresa pode se desenvolver melhor – sobre a quais desses sinais deve responder".
3. Fase da Implementação, refere-se a "traduzir o potencial da ideia inicial em algo novo e a lançar em um mercado interno ou esterno. Promover a implementação não se constitui em

> um evento isolado, mas exige especial atenção a" aquisição, execução, lançamento, sustentabilidade e aprendizagem.
> - "Aquisição de conhecimentos para possibilitar a inovação".
> - "Execução de projeto sob condições de imprevisibilidade que exigem grade capacidade de resolução de problemas".
> - "Lançamento da inovação no mercado e gerenciamento de seu processo inicial de adoção".
> - "Sustentabilidade de adoção e uso da inovação a longo prazo – ou revisitando a ideia original e modificando-a – reinovação".
> - "Aprendizagem – as empresas têm (mas nem sempre aproveitam) a oportunidade de aprender com a progressão através desse ciclo, de maneira que possam construir sua base de conhecimento e melhorar as formas em que o processo é gerido". (TIDD, BESSANT e PAVITT, 2008, p. 87-88):

Os mesmos autores destacam que o sigilo é um dos fatores que influencia a "capacidade da empresa de se beneficiar comercialmente de sua tecnologia", conforme citação:

> O sigilo é considerado uma forma eficiente de proteção por gestores industriais, especialmente no que se refere a inovação de processo. Entretanto, é improvável que se obtenha proteção absoluta, porque algumas características de processo podem ser identificadas a partir de uma análise do produto final, e porque os engenheiros de processo fazem parte de uma comunidade profissional, que se comunica entre si e passa de uma empresa para outra, de forma que a informação e o conhecimento inevitavelmente acabam vazando. Além disso, há evidência de que, em alguns setores, as empresas que compartilham conhecimento com seu sistema nacional de inovação superam aquelas que não o fazem, e que as que mais interagem com sistemas globais de inovação têm maior desempenho em inovação. Por meio de controle de nível de P&D, verifica-se que empresas cuja pesquisa (publicações e patentes) é bastante citada por

> concorrentes estrangeiros são mais inovadoras que as demais. Em alguns casos, isso ocorre porque o compartilhamento de conhecimento com o sistema global de inovação pode influenciar padrões e modelos dominantes (como veremos adiante) e permitir atrair e manter equipes de pesquisa parcerias e outros recursos vitais. (TIDD, BESSANT e PAVITT, 2008, p. 173-174)

A garantia dos direitos do conhecimento e do desenvolvimento tecnológico deve ser promovido por meio de ações de prevenção, conforme citação:

> Para garantir os direitos do conhecimento e da tecnologia desenvolvida, devem ser providenciadas ações de prevenção desde a criação da ideia na fase inicial do projeto. A confidencialidade no processo da pesquisa e desenvolvimento deve ser praticada através de instrumentos jurídicos, envolvendo todos os participantes, pesquisadores, bolsistas, alunos, parceiros, etc. A novidade de um invento é uma das exigências para a proteção da patente. (BOCCHINO et al., 2010, p. 15)

O conhecimento é o insumo da Inovação, pois está presente em todas as fases do processo de inovação. Por isso, especial atenção deve ser dada aos acordos e contratos firmados para que a proteção do conhecimento seja garantida.

Pimentel (2009b; 2010) nos alerta que os acordos de parceria de PD&I objetivam alcançar resultados voltados para a inovação tecnológica e que os acordos expressam "vontades entre duas partes ou mais pessoas físicas, entre pessoas jurídicas ou físicas e jurídicas" (PIMENTEL, 2009b, p.256), cujas atividades são definidas no Manual de Frascati (OCDE, 2013):

> As atividades de inovação tecnológica são o conjunto de etapas científicas, tecnológicas, organizativas, financeiras e comerciais, incluindo os investimentos em novos conhecimentos, que levam ou que tentam levar à implementação de produtos e de processos novos ou melhorados. A P&D não é mais do que uma destas atividades e

> pode ser desenvolvida em diferentes fases do processo de inovação, não sendo utilizada apenas enquanto fonte de ideias criativas, mas também para resolver os problemas que podem surgir em qualquer fase até a sua implementação. (OCDE, 2013)

Deste modo, o autor afirma que "a novidade, a resolução de uma incerteza na ciência e tecnologia (C&T), ciência ou tecnologia, e destinação do resultado para atividades empresariais, são os elementos-chave do conceito de PD&I", e acrescenta que:

> A PD&I é um processo que pode envolver a pesquisa básica (pesquisa científica) e a pesquisa aplicada (pesquisa tecnológica), mais o desenvolvimento experimental, sempre consiste no cumprimento de uma agenda, de um plano de trabalho, tem um orçamento, tem uma equipe de pesquisadores e, por visar a inovação, logicamente, exige um contrato de confidencialidade. (PIMENTEL, 2010b, p. 20-21)

A Confidencialidade, segundo Pimentel (2010b) atende ao requisito de novidade exigido para a proteção dos direitos de propriedade intelectual. Bocchino et al (2010) esclarece que a "confidencialidade pode ser formalizada por meio de cláusula, declaração ou contrato específico", e ainda:

> A confidencialidade é o regime que limita o acesso a dados, informação ou conhecimento. Porque tem o caráter de secreto, é aquilo que está sob sigilo ou sob reserva para dar vantagem sobre a concorrência, possibilitando pedidos de proteção da propriedade intelectual ou publicação futura. (BOCCHINO, 2010, p. 64)

Pimentel (2010b, p.72) destaca que no Brasil, segundo a Lei de Propriedade Industrial, a violação da confidencialidade é considerada crime de concorrência desleal, e "considera que também comete crime de concorrência desleal quem divulga, explora ou se utiliza, sem autorização, de conhecimentos ou informações obtidas por meios ilícitos, ou a que teve acesso mediante fraude", e acrescenta que:

> A confidencialidade é violada pela divulgação, exploração ou utilização, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, no comércio ou na prestação de serviços, por quem a eles tem acesso, mediante relação contratual ou empregatícia, mesmo após o término do contrato, se, neste estiver estipulado, para as obrigações de confidencialidade um prazo maior do que o prazo de vigência do contrato (ex: prazo de vigência do contrato, cinco anos; prazo de confidencialidade, cinco anos depois de findo o contrato). (PIMENTEL, 2010b, p. 73)

Neste contexto, considerando o conhecimento, a inovação e a PD&I, ganha destaque o contrato de parceria, que é definido pelo mesmo autor, como:

> (...) uma espécie de contrato, porque o contrato é definido como "um acordo de vontades", celebrado entre duas ou mais pessoas jurídicas, entre duas ou mais pessoas físicas, ou entre pessoas físicas e jurídicas. Quando realizado com a participação de um sujeito de direito público será um convênio. (PIMENTEL, 2010b, p. 26)

A proteção garantida nos contratos de parceria de PD&I se caracteriza no conjunto de "elementos intangíveis e tangíveis alocados pelas partes contratantes ou parceiras" descritos por Pimentel (2010b, p. 27) como:

- Recursos humanos e seus conhecimentos, inclusive a propriedade intelectual já existente – o capital intelectual (serviço de pessoas e bens intangíveis).
- Recursos financeiros.
- Recursos materiais, como o laboratório, os equipamentos, os instrumentos e as instalações necessárias para o serviço de PD&I, seus testes e ensaios (bens tangíveis). (PIMENTEL, 2010b, p. 27)

Pimentel (2010b) sugere que para facilitar a elaboração de acordos de PD&I, pode ser adotada a estrutura mínima composta por:

Identificação dos parceiros; Considerandos; Objeto; Definições; Recursos; Prazo da PD&I; Confidencialidade; Titularidade da PI; Exploração, exclusividade, resultados e prazo da PI; Divulgações; Responsabilidades; Outras obrigações; Casos de extinção da parceria; Foro; Publicação em Diário Oficial da União; Assinaturas; e Testemunhas. Também recomenda que conste como anexo o plano de trabalho, incluindo o protocolo de transferência de resultados da PD&I.

2.6 SEGREDO

A origem da palavra segredo vem do Latim *secretus*, que significa "à parte, isolado, oculto". No dicionário Aurélio, significa "coisa que não deve ser sabida por outrem, reserva, discrição, meio pouco conhecido de fazer uma coisa, secreto".

Cepik (2003, p. 151) nos traz a definição de Bok para segredo como "qualquer coisa mantida intencionalmente escondida" (BOK, 1989 apud CEPIK, 2003, p.151), e acrescenta a sua definição para segredo como "uma retenção compulsória de conhecimento, reforçada pela perspectiva de punição em caso de revelação".

O *segredo* é empregado no Direito, referindo-se as atividades comerciais, industriais e empresariais, que portam particularidades teóricas que evoluíram para acompanhar a complexidade das atividades econômicas. Pode-se dizer que a proteção do segredo compreende mecanismos de proteção para a propriedade imaterial da informação tecnológica, por ser de importância estratégica para o país e a indústria. (Flores, 2008)

O mesmo autor, ao buscar diferenciar segredo comercial, industrial e *know-how* afirma que podemos ter:

> (...) segredos comerciais, segredos industriais e know-how, sendo esse último o objeto do contrato, que tanto poderá conter informações industriais ou até mesmo ambas, mas não seria a melhor terminologia utilizar o termo *know how* para contratos que envolvam exclusivamente segredo comercial. (FLORES, 2006, P. 101-102)

Para o mesmo autor, "O segredo industrial é espécie do gênero segredo comercial, já que o fim dos segredos industriais tem por objetivo adquirir competitividade e vantagens comerciais através da produção" (FLORES, 2006, p. 109).

Alguns autores definem *segredo* como um conhecimento ou informação utilizado pela organização como instrumento de vantagem sobre seus competidores, onde a comercialização desses direitos se dá pela transferência de tecnologia, praticando a transmissão de bens imateriais acordados entre as partes como objeto de um negócio jurídico, geralmente formalizado por contratos de transferência de tecnologia. (PIMENTEL, 2005; ZIBETTI, 2001; FLORES, 2008)

Cabe destacar que a patente é o instrumento de proteção mais utilizado para inovações tecnológicas, conforme citação de Jungmann (2010):

> A patente é um título de propriedade temporária concedidos pelo Estado, com base na Lei de Propriedade Industrial (LPI), àqueles que inventam novos produtos, processos ou fazem aperfeiçoamentos destinados à aplicação industrial. É o instrumento de proteção mais utilizado na de inovação tecnológica. Sua importância é fundamental, pois a concessão deste direito de exclusividade garante ao seu titular a possibilidade de retorno do investimento aplicado no desenvolvimento de novos produtos e processos industriais. (JUNGMANN, 2010, p. 27)

De um modo geral, todas as informações confidenciais da empresa que fornecem uma vantagem competitiva podem ser consideradas segredo comercial, abrangem fabricação ou segredos industriais e segredos comerciais. O uso não autorizado de tais informações por outras pessoas que não o titular é considerado uma prática desleal e uma violação do segredo comercial. No Brasil, a proteção de segredo comercial faz parte do conceito geral de proteção contra a concorrência desleal ou é baseada em disposições específicas ou jurisprudência sobre a proteção de informações confidenciais. (WIPO, OMPI, INPI, 2014)

A Lei nº 9.279, de 14 de maio de 1996, que dispõe sobre a Propriedade Industrial, reprime a concorrência desleal e trata no capítulo VI dos crimes de concorrência desleal.

Para o contexto deste trabalho, destacamos:

> Art. 195. Comete crime de concorrência desleal quem:
> [...]

> dá ou promete dinheiro ou outra utilidade a empregado de concorrente, para que o empregado, faltando ao dever do emprego, lhe proporcione vantagem;
> X - recebe dinheiro ou outra utilidade, ou aceita promessa de paga ou recompensa, para, faltando ao dever de empregado, proporcionar vantagem a concorrente do empregador;
> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técni
> co no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
> XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; [....] (BRASIL, 1996)

Jugmann (2010) nos diz que a Propriedade Industrial tem seu foco na atividade empresarial, e que o direito de propriedade industrial reúne um conjunto de direitos e obrigações sobre os bens intelectuais, conforme citação:

> A propriedade industrial tem o seu foco de interesse mais voltado para a atividade empresarial. Tem por objeto patentes de invenção e de modelos industriais, marcas, desenhos industriais, indicações geográficas, segredo industrial e repressão a concorrência desleal, sendo regulamentada pela Lei nº 9.279/96. O direito de propriedade industrial é um conjunto de direitos e obrigações relacionado a bens intelectuais, objeto de atividade industrial de empresas ou indivíduos. Assegura a seu proprietário (titular do direito) a exclusividade de: Fabricação; Comercialização; Importação; Uso; Venda; Cessão. (JUNGMANN, 2010, p.22)

Flores (2006, p.59) afirma que “o segredo de uma tecnologia é capaz de proporcionar uma real vantagem competitiva, e é protegido mundialmente apenas por mecanismos legais indiretos existentes para a representação aos delitos: concorrência desleal ou enriquecimento ilícito”

Neste contexto, Jungmann (2010) esclarece que o segredo industrial preserva a natureza confidencial de uma informação que tenha valor comercial, e é um instrumento muito utilizado em áreas de P&D, conforme citação:

> Pessoas físicas ou jurídicas têm a possibilidade de preservar a natureza confidencial de uma informação e evitar que tais informações, legalmente sob seu controle, sejam divulgadas, adquiridas ou usadas por terceiros não autorizados, sem seu consentimento, desde que tal informação:
> - Seja secreta, no sentido de que não é conhecida em geral, nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão;
> - Tenha valor comercial por ser secreta;
> - Tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.
> O segredo de fábrica ou industrial é muito utilizado em áreas onde a pesquisa e o desenvolvimento tecnológico são intensos, como na indústria de informação e comunicação, petroquímica, farmacêutica, de bebidas, alimentos e cosméticos. (JUNGMANN, 2010, p. 50)

O estudo de KELLI et al. (2010), que investigou a proteção do conhecimento em Pequenas e Médias Empresas (PME), considera o segredo como um método tradicional de proteção do conhecimento, e destaca que a proteção e gestão dos segredos tem grande relevância estratégica para as pequenas economias em transição, e contribui com a afirmação:

> Como a maioria dos empresários estonianos das PME são dos sectores de baixa tecnologia, a implementação de uma adequada estratégia de proteção *trade secret* é vital. Existem várias vantagens para a proteção de *trade secret*. Em primeiro lugar, o âmbito de proteção do *trade*

> *secret* é extensa e inclui o conhecimento não-patenteável. Em segundo lugar, ele não requer o registro ou o cumprimento de todos os procedimentos formais.
> (...). A concentração das atividades do sector a baixa ou alta tecnologia só determina se os empresários irão combinar patentes e proteção *trade secret* , ou se são apenas dependentes da proteção *trade secret* . O reforço da capacidade empresarial para gerir *trade secret* é crucial. (KELLI et al., 2010 – tradução nossa)

No Brasil, a mais antiga teoria relacionada às atividades econômicas foi a Teoria dos atos de comércio, doutrinada pelo Código Comercial Brasileiro, datado de 1850, onde os atos de comércio "pressupunham habitualidade, atuação contínua no exercício da atividade comercial, que basicamente consistia na compra para revenda". As atividades comerciais respondiam pelas atividades econômicas, porém com o desenvolvimento de atividades econômicas mais complexas, como: a industrialização, e prestação de serviços; a "teoria dos atos de comércio tornou-se insuficiente como disciplina jurídica do Direito Comercial". (TEIXEIRA, 2013, p.21)

Com o surgimento da teoria da empresa[11], a partir do Código Civil de 2002, que ampliou o entendimento e alcance da atividade econômica organizada, conforme citação:

> A teoria da empresa é mais ampla que a teoria dos atos de comércio porque alcança qualquer atividade econômica organizada para a produção ou circulação de bens ou de serviços (exceto as atividades intelectuais), e não apenas os atos de comércio.
> No Brasil, foi adotada pelo Código Civil de 2002, por influência da legislação italiana. (TEIXEIRA, 2013, p.21)

Para as atividades industriais no Brasil, a propriedade industrial tem seu fundamento na Constituição Federal de 1988 e no seu regime

[11] Surgiu então, "a partir da vigência do Código Civil Italiano de 1942, a teoria da empresa, como evolução da teoria dos atos de comércio, tendo em vista sua maior amplitude" (TEIXEIRA, 2013, p. 21)

jurídico do Código da Propriedade Intelectual (CPI) – Lei Nº 9,279/96. Devem-se considerar as características da patente explicadas na citação:

> Uma patente confere a seu titular a exploração exclusiva de sua intenção durante um tempo determinado (...), podendo o inventor adotar medidas jurídicas contra aqueles que se utilizarem indevidamente do objeto patenteado, (...)
> No entanto, a concessão de uma patente ocorre após a sua divulgação, tornando-a de conhecimento público, e, após vencido o prazo legal, a patente cai em domínio público, podendo ser utilizado por qualquer pessoa.
> O contrário ocorre com o segredo empresarial. (TEIXEIRA, 2013, p.24).

Para Barbosa (2008, p.1) o segredo industrial "é a informação, técnica ou não, caracterizada por escassez suficiente para lhe dotar de valor competitivo num determinado mercado".

Conforme afirma Barone (2009) "(...) embora o segredo industrial não se encontre propriamente definido na legislação brasileira, é possível obter-se, a partir do texto legal, algumas de suas características e elementos que auxiliam em sua significação".

Assim, entendemos que o segredo industrial é o conjunto de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, que possuem valor comercial e asseguram vantagem competitiva, que não devem ser divulgados, explorados ou utilizados sem autorização, incidindo em crime quem praticar tal ato.

O Segredo empresarial é entendido como "tudo aquilo produtos ou processos produtivos, criado pelo empresário que é mantido sob sigilo, ou seja, todo o conjunto de uma criação que não é patenteada" (TEIXEIRA, 2012).

Rossi (2014) acrescenta que existem vários termos podem designar, de alguma forma, um segredo empresarial:

> Vários são os termos que designam de algum modo um segredo empresarial juridicamente tutelado: know-how (ou *savoir faire*), segredo industrial, segredo de comércio, segredo de fábrica, segredo de negócio, *trade secret*, informação confidencial. Em geral, os conceitos jurídicos dependem

> essencialmente do direito positivo, pois são as tutelas jurídicas que determinam a relevância de certa classificação. Em razão das alterações legislativas, por exemplo, a distinção entre segredo de fábrica e segredo de negócio passou a ser irrelevante, do ponto de vista da tutela jurídica, com a revogação do Decreto-Lei n. 7.903/45 (Código de Propriedade Industrial), pela Lei n. 9.279/96 (Lei de Patentes), pois a lei nova aglutinou essas categorias. A lei brasileira, aliás, não faz qualquer distinção: são protegidos, nos termos do Art. 195, incisos XI e XII, os "conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto" (BRASIL, 1996). Ainda assim, a distinção entre as categorias pode ter alguma relevância no direito contratual, visto que algumas dessas categorias podem ser utilizadas na delimitação do objeto do negócio jurídico. (ROSSI, 2014, p. 2)

A definição para segredo comercial é ampla, inclui métodos de vendas, métodos de distribuição, o perfil do consumidor, as estratégias de publicidade, listas de fornecedores e clientes, e processos de fabricação. As circunstâncias individuais determinam quais informações constituem um segredo comercial. Práticas claramente abusivas no domínio das informações secretas incluem espionagem industrial ou comercial, quebra de contrato e violação de confiança. (WIPO, 2014)

O *know how* consiste na arte de "saber fazer" profissionalmente um bem, que pode ser passada por meio de contratos de transferência, conforme citação:

> *Know how* se constitui em uma arte de fabricação. Envolve a reunião de experiências, conhecimentos e habilidades para produzir um bem. Compõem o know how:
> - A habilidade técnica do profissional, operário ou artífice, que é intransmissível, inseparável da pessoa que detêm este tipo de arte.
> - A parcela da arte que o profissional técnico ensina ao aprendiz, e que, pela assistência pessoal, pode ser repassada em um contrato de transferência de

> tecnologia. A essência do know how está nos conhecimentos técnicos somados àqueles que integram o estado da técnica.de um profissional. (JUNGMANN, 2010, p. 51)

Neste estudo, diante da posição do segredo nas teorias do Direito, e do interesse no conhecimento a ser protegido, contribui para o estudo a definição utilizada sobre segredo empresarial, como: “conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto” (BRASIL, 1996).

3 PROCEDIMENTOS METODOLÓGICOS

O capítulo anterior apresentou a fundamentação teórica da tese e a harmonização de termos e conceitos primordiais para o desenvolvimento da pesquisa.

Este capítulo destina-se a explicar os procedimentos metodológicos adotados, de acordo com os objetivos traçados para a investigação do problema de pesquisa, e seguindo passos, aqui chamados de fases da pesquisa.

Para a elaboração desta tese adotou-se a abordagem de pesquisa qualitativa básica (MERRIAM, 1992), que utiliza como técnica de coleta de dados a pesquisa documental e bibliográfica (VERGARA, 2005; GIL, 2009), e o modo de observação indireto, que compreendeu o levantamento documental e bibliográfico (LAKATOS e MARCONI e LAKATOS, 2009).

A pesquisa foi desenvolvida conforme apresentado na Figura 12.

Inicialmente definiu-se o problema de pesquisa sintetizado na questão que norteou o trabalho. Como aplicar os instrumentos de proteção do segredo no Ambiente de Inovação da BID?

A seguir definiu-se o objetivo geral e os objetivos específicos. Estes foram marcos importantes que pavimentaram o caminho para se atingir o objetivo geral que é propor um *framework* que oriente a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação da BID.

Os objetivos específicos possibilitaram harmonizar termos e conceitos utilizados, conceber o Sistema Sociotécnico para a BID e caracterizar o Ambiente de Inovação da BID.

Na fase seguinte, Fundamentação Teórica, dedicou-se a busca de conhecimentos multidisciplinares que formam a fundamentação teórica aplicável ao ambiente da pesquisa.

A seguir foram definidos os procedimentos metodológicos para a coleta, análise e interpretação dos dados. Como produto desta fase, harmonizou-se terminologias e definições aplicáveis ao Ambiente de Inovação da BID. O entendimento dos dados, normativos e do ambiente possibilitou elaborar o Sistema Sociotécnico com a finalidade de entender as influências, interações e relações entre o subsistema técnico, o subsistema social e o ambiente externo. No arranjo deste Sistema Sociotécnico o papel das Indústrias de Defesa, dos Órgãos de Defesa e da Academia são expressivos.

Também se caracterizou o Ambiente de Inovação da BID e as estruturas de inovação das FA com os respectivos projetos estratégicos e

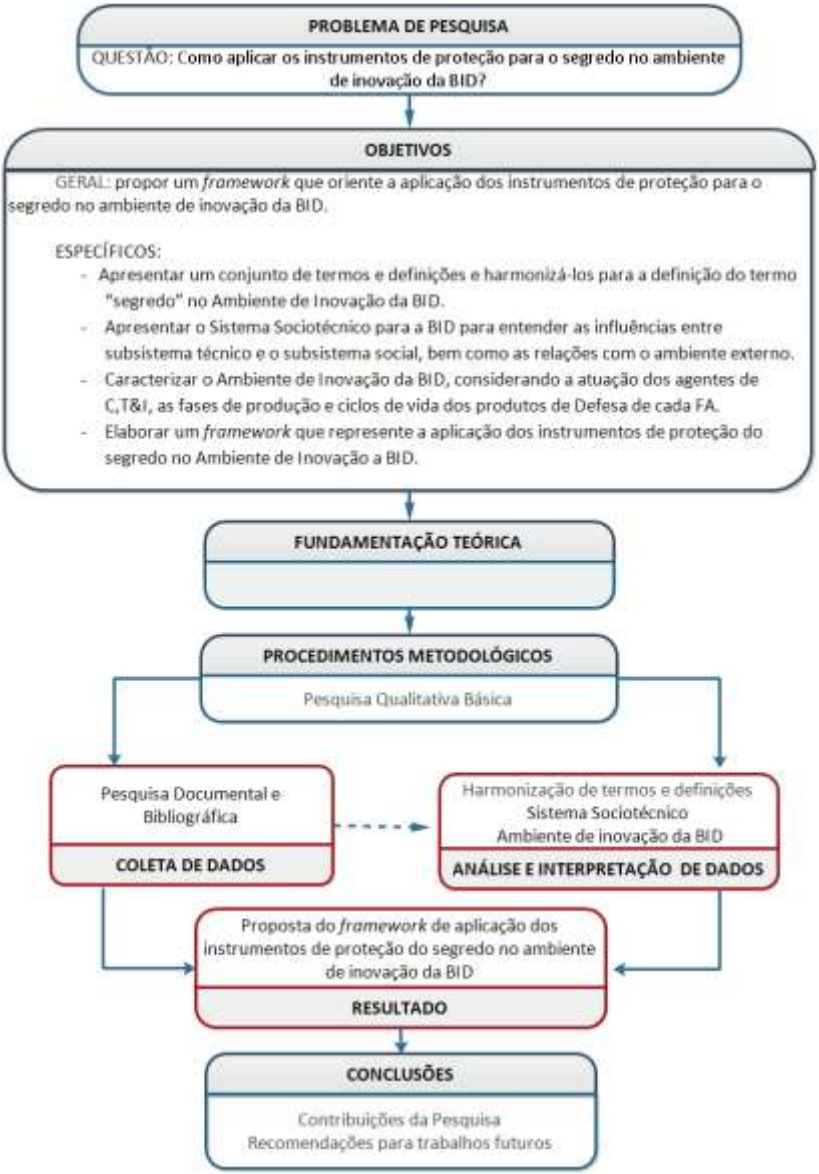
o ciclo de vida dos produtos de defesa. Tal entendimento foi o fundamento para a concepção do Sistema de Produção no Ambiente de Inovação da BID.

Na fase Resultado, a partir dos conceitos harmonizados, do Sistema Sociotécnico e do Sistema de Produção do Ambiente de Inovação da BID, foi possível propor o *framework* que sistematiza a aplicação dos instrumentos de proteção do segredo no ambiente de inovação a BID.

Na última fase foram relacionadas as contribuições da pesquisa e as recomendações para trabalhos futuros.

A seguir apresentamos a Figura 12 com o detalhamento das fases desta pesquisa.

Figura 12 - Fases da Pesquisa



Fonte: Elaboração da autora, 2015.

4 HARMONIZAÇÃO DE TERMOS E DEFINIÇÕES PARA O AMBIENTE DE ESTUDO

De acordo com a fundamentação teórica apresentada e para atender o objetivo de apresentar um conjunto de termos e definições para harmonização que caracterize o "segredo" no Ambiente de Inovação da BID, se fez necessário elaborar um conjunto de terminologias próprias para esta tese.

Este subcapítulo não seguirá o rigor estabelecido pela NBR-13789 (1997), que apresenta princípios e métodos para a elaboração e apresentação de normas de terminologias, porém adota os princípios básicos para a formulação de definições.

Este estudo considerou três ambientes específicos, onde os termos informação e conhecimento ganham especificidades próprias que atendem a terminologia requerida no ambiente, são eles: o ambiente de Defesa, o Ambiente da BID, e o Ambiente de Inovação da BID.

4.1 PRIMEIRO AMBIENTE: EXTERNO

No ambiente externo, vários autores apresentaram definições para os termos dado, informação e conhecimento. Todos foram unânimes em reconhecer a agregação de valor aos dados para se obter a informação, e a essa para se obter o conhecimento.

Assim, consideramos as seguintes definições, contidas na fundamentação teórica, para os termos:

- **Dado**: "conjunto de registros qualitativos ou quantitativos conhecido que organizado, agrupado, categorizado e padronizado adequadamente transforma-se em informação" (MIRANDA, 1999).
- **Informação**: "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato" (BRASIL, 2011).
- **Informação tecnológica**: "aquela que trata da informação necessária, utilizada e da informação gerada nos procedimentos de aquisição, inovação e transferência de tecnologia, nos procedimentos de metrologia, certificação da qualidade e normalização e nos processos de produção" (Montalli, 1996).

- **Informação para negócios**: “aquela que subsidia o processo decisório do gerenciamento das empresas industriais, de prestação de serviços e comerciais, nos seguintes aspectos: companhias, produtos, finanças, estatísticas, legislação e mercado” (Montalli, 1996).
- **Conhecimento: “**construído a partir de relações sociais sucessivas, é fruto de uma interação do homem com o mundo, estruturando-se pelo viés da interpretação individual” (Maturana e Varela, 2001). “Deriva da informação, mas é mais rico e significativo do que esta, pois inclui consciência, familiaridade e compreensão adquiridas pela experiência, possibilitando comparações, identificação das consequências e novas conexões” (Servin, 2005).

4.2 SEGUNDO AMBIENTE: DEFESA

Para o ambiente de Defesa, consideramos as definições apresentadas na seção anterior, e acrescentamos outras para conceituar um novo termo que representa a informação de interesse de Defesa, são elas:

- **Inteligência**: “ramo voltado para a produção de conhecimentos, relativos a fatos e situações atuais ou potenciais que afetem o processo decisório no âmbito da Defesa” (ESG, 2005).
- **Contra-Inteligência**: “ramo voltado para a detecção, identificação, neutralização, obstrução e prevenção da atuação da Inteligência adversa e das ações de qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de tecnologia da informação) de interesse da Defesa” (ESG, 2005).
- **Informe**: “conhecimento resultante de juízo formulado pelo analista de Inteligência sobre a narração de fato ou situação passada ou presente” (ESG, 2005).
- **Informação**: “Conhecimento resultante de raciocínio elaborado pelo analista de Inteligência que expressa sua certeza sobre situação ou fato passado ou presente” (ESG, 2005).

- **Apreciação**: “Conhecimento resultante de raciocínio elaborado pelo analista de Inteligência que expressa sua opinião sobre situação ou fato passado, presente ou futuro imediato” (ESG, 2005).
- **Estimativa**: “Conhecimento resultante de raciocínio elaborado pelo analista de Inteligência que expressa a sua opinião sobre a evolução futura de um fato ou de uma situação” (ESG, 2005).
- **Informação para Negócios:** “conjunto de informações destinadas a subsidiar as atividades das organizações no seu processo de desenvolvimento” (BORGES e CAMPELLO, 1997, p.149).

Com base nestes conceitos definimos a Informação de Interesse da Defesa, chamada aqui de Informação de Defesa, como:

INFORMAÇÃO DE DEFESA
Conjunto de dado e informação, processados ou não, de origem endógena e exógena que é de Interesse de Defesa.

A Figura 13 apresenta a estrutura de conceitos utilizada para formar o conceito de Informação de Defesa.

Figura 13 – Representação da Informação de Defesa

Fonte: Elaboração da autora, 2015.

O braço Inteligência provê insumos por intermédio dos diversos formatos que possuem características próprias na fase de elaboração. A outra fonte de insumos contém informações para negócios e informações de tecnologia que são provenientes da indústria, do meio acadêmico e do governo. A pertinência, a relevância e o valor dos insumos são verificados e analisados quanto ao Interesse de Defesa, possibilitando a partir destes filtros, a elaboração da Informação de Defesa.

Para a definição do termo Conhecimento de Defesa, consideramos, também, as seguintes definições contidas na fundamentação teórica:

- **Conhecimento Estratégico**: "conhecimento requerido para a formulação das Avaliações Estratégicas dos órgãos componentes da Defesa, de planos e de políticas no nível

nacional ou internacional, referentes à Defesa Nacional " (ESG, 2005)

- **Conhecimento Operacional**: "conhecimento requerido para planejar, conduzir e sustentar operações militares de grande envergadura, a fim de que sejam alcançados objetivos estratégicos dentro de um Teatro de Operações ou Zona de Operações" (ESG, 2005).
- **Conhecimento Tático**: "conhecimento requerido para a condução de operações de combate no nível tático" (ESG, 2005).
- **Conhecimento Básico**: "conhecimento pouco sensível à ação do tempo. Compreende conhecimentos de geografia, de demografia, de política, biográficos, da estrutura geral das forças e das características operacionais de áreas do país ou do exterior" (ESG, 2005).
- **Conhecimento Corrente**: "conhecimento altamente sensível à ação do tempo e que trata de assuntos e atividades em andamento, ou recentemente concluídos, apresentando reflexos para a conjuntura atual" (ESG, 2005).
- **Artefatos de Conhecimento** é um "objeto que transmite ou detém representações utilizáveis do conhecimento" (HOLSAPPLE, 2003).

Assim, o conhecimento que atende o interesse da Defesa chamamos de Conhecimento de Defesa, e definimos como:

CONHECIMENTO DE DEFESA
Conhecimento de Interesse da Defesa obtido a partir da análise e interpretação de Informações de Defesa, Conhecimentos produzidos pela Inteligência, e outros Conhecimentos.

Para a composição do conceito conhecimento de defesa foram agregados outros conceitos, como representado na Figura 14.

Figura 14 – Representação do Conhecimento de Defesa

Fonte: Elaboração da autora, 2015.

Como representado na Figura 14, o Conhecimento de Defesa é bastante holístico e é produzido a partir informações imbricáveis que vão da interpretação e compreensão de Informações de Defesa, passa por conhecimentos produzidos pela inteligência e chega aos conhecimentos relacionados às diversas atividades estratégicas de defesa. Atributos como pertinência, relevância e valor das informações são verificados e analisadas quanto ao Interesse de Defesa, possibilitando a elaboração do Conhecimento de Defesa.

4.3 TERCEIRO AMBIENTE: INOVAÇÃO DA BID

Para o Ambiente de Inovação da BID, consideramos as seguintes definições e conceitos contidos na fundamentação teórica:

- **Segredo:** como um conhecimento ou informação utilizado pela organização como instrumento de vantagem sobre seus competidores, onde a comercialização desses direitos se dá

pela transferência de tecnologia, praticando a transmissão de bens imateriais acordados entre as partes como objeto de um negócio jurídico, geralmente formalizado por contratos de transferência de tecnologia. (PIMENTEL, 2005; ZIBETTI, 2001; FLORES, 2006)

- **Segredo comercial**: todas as informações confidenciais da empresa que fornecem uma vantagem competitiva e abrangem fabricação ou segredos industriais e segredos comerciais. (WIPO, 2014)
- **Segredo industrial**: "espécie do gênero segredo comercial, já que o fim dos segredos industriais tem por objetivo adquirir competitividade e vantagens comerciais através da produção" (FLORES, 2006)
- **Segredo empresarial: "**conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto" (BRASIL, 1996). "Tudo aquilo produtos ou processos produtivos, criado pelo empresário que é mantido sob sigilo, ou seja, todo o conjunto de uma criação que não é patenteada". (TEIXEIRA, 2013).
- **Direito de propriedade industrial**: "conjunto de direitos e obrigações relacionado a bens intelectuais, objeto de atividade industrial de empresas ou indivíduos, que assegura a seu proprietário (titular do direito) a exclusividade de: Fabricação; Comercialização; Importação; Uso; Venda; Cessão". (JUNGMANN, 2010)
- **Know-How: "***Know how* se constitui em uma arte de fabricação. Envolve a reunião de experiências, conhecimentos e habilidades para produzir um bem. Compõem o *know how*: a habilidade técnica do profissional, operário ou artífice, que é intransmissível, inseparável da pessoa que detêm este tipo de arte; a parcela da arte que o profissional técnico ensina ao aprendiz, e que, pela assistência pessoal, pode ser repassada em um contrato de transferência de tecnologia. A essência do *know how* está nos conhecimentos técnicos somados àqueles que integram o estado da técnica.de um profissional". (JUNGMANN, 2010)
- **Concorrência Desleal:** representa condutas anticompetitivas, causando prejuízo à livre concorrência entre

empresas do mesmo segmento produtivo (WIPO, OMPI, INPI, 2015)

- **Contra-Inteligência: "**ramo da AID responsável pela salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de tecnologia da informação) de interesse da Defesa, contra a ação adversa de pessoas, órgãos e organizações de Inteligência, ou de outras ameaças" (ESG, 2005).
- **Segurança Orgânica**: "busca obter um grau de proteção ideal, por meio da adoção eficaz e consciente de um conjunto de medidas destinadas a prevenir e obstruir as ações de qualquer natureza que ameacem a salvaguarda de dados, conhecimentos e seus suportes de interesse da Defesa" (ESG, 2005)
- **Segurança Ativa**: "adoção de medidas de caráter proativo destinado a detectar, identificar, avaliar e neutralizar as ações da Inteligência adversa e outras ações de qualquer natureza" (ESG, 2005)
- **BID**: "o conjunto das empresas estatais e privadas, bem como organizações civis e militares, que participem de uma ou mais das etapas de pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos estratégicos de defesa" (BRASIL, 2005b).

Deste modo, nesta pesquisa definimos o termo Segredo com a finalidade de atender os interesses de defesa, ou seja, o objeto de proteção para o ambiente deste estudo, como a seguir:

SEGREDO
No Ambiente de Inovação da BID, é o conjunto de Informação de Defesa e de Conhecimento de Defesa, inclusive os artefatos de conhecimentos, que em função da criticidade, do valor que possui e da importância estratégica é classificado como sigiloso ou de acesso restrito, e que não pode ser de domínio público, pois envolve novidade, segredos e direitos de propriedade industrial da BID; e é passível de proteção, por instrumentos legais e administrativos e por atividades de Inteligência e Contra-Inteligência.

A Figura 15 apresenta a estrutura de formação do conceito de Segredo.

Figura 15 – O Segredo no Ambiente de Inovação da BID

Fonte: Elaboração da autora, 2015

Como representado na Figura 15 o Segredo é o conjunto de conhecimentos produzidos pela Inteligência e Contra-Inteligência; Informação e Conhecimento de Defesa; e segredos da BID, que podem estar contidos em artefatos de conhecimentos.

Cada nova demanda para o Ambiente de Inovação da BID poderá se constituir em novo segredo. A verificação deve ser meticulosa e poderá ser feita analisando:

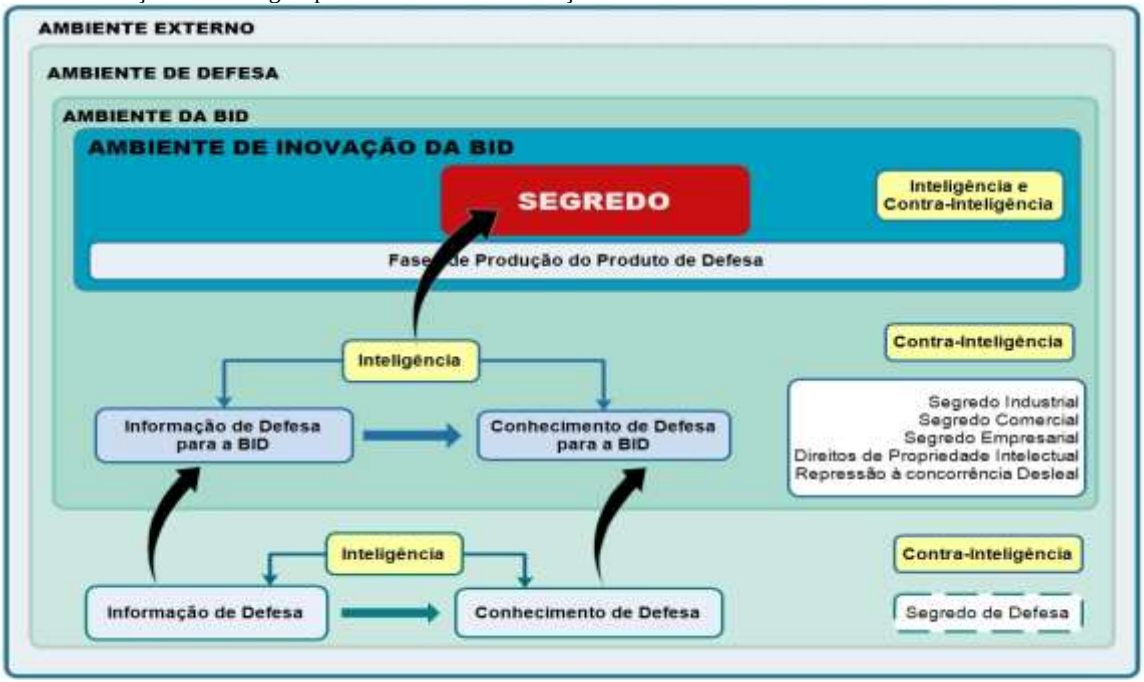
- Critérios que possam afetar o sucesso do projeto estratégico de interesse para a segurança nacional.

- Tecnologias que serão utilizadas
- Segredos da BID

4.4 CONCLUSÃO DO CAPÍTULO

A partir da harmonização dos termos e definições foi possível elaborar um infográfico que represente a evolução terminológica específica para o Ambiente de Inovação da BID, conforme apresentado na Figura 16.

Figura 16 – Harmonização terminológica para o Ambiente de Inovação da BID



Fonte: Elaboração da autora, 2015.

Deste modo, a Figura 16 apresenta os ambientes considerados nesta tese, contemplando a harmonização dos termos específicos.

O Ambiente Externo envolve o Ambiente de Defesa e representa tudo que está fora das fronteiras do Ambiente de Defesa. Neste ambiente se localizam outros órgãos da APF, empresas, universidades, a sociedade e as nações. As relações e interações entre os ambientes representados não foram alvo desta pesquisa. A ênfase recaiu sobre o fluxo de informação e conhecimento.

No domínio do Ambiente de Defesa se localizam *stakeholders* como o MD e as FA bem como as políticas e estratégias de defesa. Se destacou neste ambiente a atividade de Inteligência que produz Informações e Conhecimentos de Defesa a partir de insumos internos e externos ao Ambiente de Defesa, a atividade de Contra-Inteligência que empreende ações que visam salvaguardar o conhecimento de qualquer ameaça externa e o Segredo.

Se delimitou dentro do Ambiente de Defesa o Ambiente da BID, onde se encontram as Indústrias de Defesa, setores do MD e os ICT das FA. A Figura 16 detalha que a atividade de Inteligência no Ambiente da BID recebe insumos da atividade de Inteligência do Ambiente de Defesa. No domínio da BID também são representados os segredos que lhe são inerentes e a atividade de Contra-Inteligência.

O Ambiente de Inovação da BID se encontra mais segregado no interior do Ambiente da BID. O fluxo de Informações e Conhecimentos de Defesa para a BID juntamente com o *Know How* e conhecimentos protegidos da indústria originam o segredo no Ambiente de Inovação da BID. A disposição dos ambientes apresentados na Figura 16 induz a entender que menos pessoas possuem acesso ao Ambiente de Inovação da BID e ao segredo, e também que os conhecimentos e seus arranjos possuem maior relevância estratégica e valor e são mais sensíveis. Aqui a atividade de Contra-Inteligência representa a gama de instrumentos de proteção do segredo que devem ser aplicados para prover a segurança necessária.

5 SISTEMA SOCIOTÉCNICO PARA A BID

Neste capítulo apresentamos apresentados os conceitos e as informações consideradas para elaborar o Sistema Sociotécnico para a BID.

O Sistema Sociotécnico representa as relações e interações entre o subsistema técnico e o subsistema social, bem como as relações com o ambiente externo.

Ao trazer abordagem sistêmica para esta tese, buscou-se a apropriação do conceito de sistemas para entender as caraterísticas singulares dos "elementos" da BID, que se combinam para formar "um todo complexo e orientado para uma finalidade" (CHIAVENATO, 2003, p. 475-476).

Consideramos que as organizações que compõem a BID são sistemas abertos que possuem características próprias, tais como: a) comportamento probabilístico e não determinístico diante das mudanças em seus ambientes (variáveis externas); b) partes de algo maior e compostas por partes menores (sistemas dentro de sistemas); c) partes são interdependentes e inter-relacionadas; d) homeostase (estado firme, estado de equilíbrio) por meio da liderança e comprometimento, diante das mudanças do ambiente, mantendo a unidirecionalidade e progresso em relação ao fim, conciliando a homeostasia e a adaptabilidade; e) fronteiras definidas; f) morfogênese (capacidade de modificar a si mesma e sua estrutura própria para corrigir erros); e f) resiliência (CHIAVENATO, 2003, p. 480-482).

Dos vários modelos de organização de sistemas abertos, destacamos o Modelo Sociotécnico de Tavistock[12] como ponto inicial para a construção do Sistema Sociotécnico para a BID. O modelo de Tavistock considera a organização como um sistema sociotécnico estruturado sobre dois subsistemas. O subsistema técnico que compreende as tarefas a serem desempenhadas, as instalações físicas, os equipamentos e instrumentos utilizados, as exigências da tarefa, as utilidades e técnicas operacionais, o ambiente físico, e a operação das tarefas. É o responsável pela eficiência potencial. O subsistema social compreende as pessoas, as relações sociais entre os indivíduos, e as exigências de trabalho. Transforma a eficiência potencial em eficiência

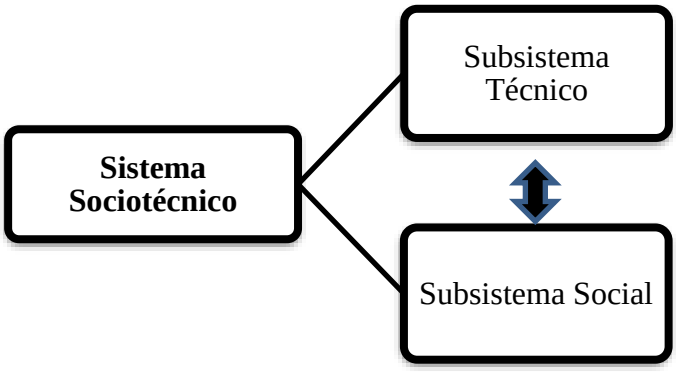
[12] O termo *sociotécnico* foi definido em 1960 por Fred Emery e Eric Trist, pesquisadores em desenvolvimento organizacional do *Tavistock Institute of Human Relations* em 1960. (Maté e Silva, 2005).

real. (CHIAVENATO, 2003, p. 486-487). Assim, a abordagem sociotécnica mantém certa interseção mútua e recíproca, conforme citação do autor:

> Os subsistemas tecnológico e social acham-se em uma interação mútua e recíproca e cada um determina o outro, até certo ponto. A natureza da tarefa influencia (e não determina) a natureza da organização das pessoas, bem como as características psicossociais das pessoas influenciam (e não determinam) a forma em que determinado cargo será executado. [...] O modelo de sistema aberto proposto pela abordagem sociotécnica parte do pressuposto de que toda organização "importa" várias coisas do meio ambiente e utiliza essas importações em processos de "conversão", para então "exportar" produtos e serviços que resultam do processo de conversão CHIAVENATO (2003, p. 487).

A Figura 17 ilustra a composição de um sistema sociotécnico.

Figura 17 – Sistema Sociotécnico

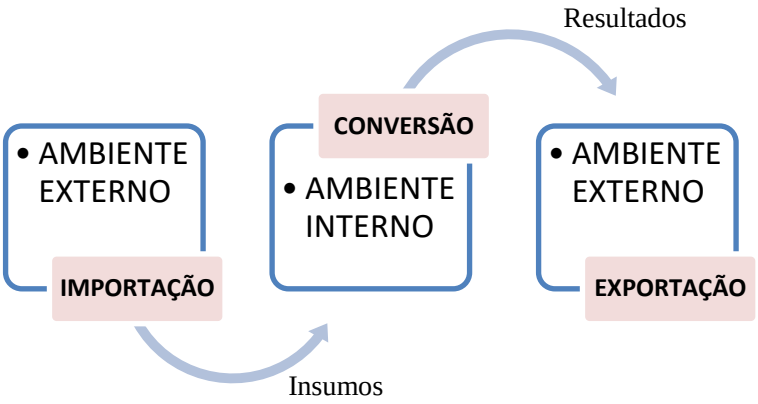


Fonte: Elaboração da autora, baseado em CHIAVENATO (2003, p. 487).

Como esperado de um sistema aberto, à luz da abordagem sociotécnica, toda organização importa insumos do ambiente, processa-

os internamente segundo os propósitos de sua necessidade, e exporta o resultado. A Figura 18 apresenta o fluxo geral de um sistema aberto.

Figura 18 – Fases da Abordagem Sociotécnica



Fonte: Elaboração da autora, 2015, baseado em CHIAVENATO (2003)

Sendo a BID o conjunto das empresas estatais ou privadas que participam de uma ou mais etapas de pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos estratégicos de defesa – bens e serviços, ao aplicar a abordagem sociotécnica ao seu ambiente, identificamos os principais componentes dos subsistemas técnico e social, como apesentados a seguir.

5.1 SUBSISTEMA TÉCNICO

Como dito anteriormente, o Subsistema técnico é o responsável pela eficiência potencial. Para conceber o Subsistema Técnico da BID citamos a seguir os principais componentes de sua estrutura.

5.1.1 Ministério da Defesa

O Ministério da Defesa (MD), órgão da Administração Pública Federal, tem a função de:

> (...) coordenar o esforço integrado de defesa, bem como contribuir para a garantia da soberania, dos poderes constitucionais, da lei e da ordem e do patrimônio nacional, assim como, para a salvaguarda dos interesses nacionais e o incremento da inserção do Brasil no cenário internacional. (BRASIL, 2010b, p. 1).

Por meio de sua Secretaria de Produtos de Defesa (SEPROD), a qual compete assessorar na formulação e atualização das políticas, além de acompanhar sua execução (BRASIL, 2012c):

- Política Nacional de Ciência, Tecnologia e Inovação de Defesa, visando ao desenvolvimento tecnológico e à criação de novos produtos de defesa;
- Política Nacional da Indústria de Defesa; e
- Política de Obtenção de Produtos de Defesa.

Também é de competência da SEPROD atuar junto ao Governo Federal para estabelecer normas especiais de incentivo à indústria de defesa no mercado nacional e internacional; além de supervisionar e fomentar as atividades de tecnologia industrial básica de interesse comum das FA; as atividades de C,T&I de desenvolvimento e industrialização de novos produtos de defesa; e as atividades de obtenção de informações de tecnologia militar e do Sistema Militar de Catalogação (SisMiCat). (BRASIL, 2012c, p. 62-6364).

5.1.2 Indústrias de Defesa

Atualmente, no Sistema de Cadastramento de Produtos e Empresas de Defesa (SisCaPED) tem 301 empresas cadastradas como indicado no Quadro 15.

Quadro 15 – Empresas Cadastradas no SisCaPED

Situação de Cadastro	Total
Empresas Cadastradas	301
Empresas Estratégicas de Defesa (EED)	63
Empresas de Defesa (ED)	10

Fonte: Elaboração da autora, 2015, com base em Brasil (2015a).

5.1.3 Instituições de Ciência e Tecnologia das Forças Armadas

De acordo com a Lei Nº 13.243/2016, a Instituição Científica, Tecnológica e de Inovação (ICT) é definida como:

> (...) órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter científico ou tecnológico ou o desenvolvimento de novos produtos, serviços ou processos (BRASIL, 2016).

A Marinha possui dez Institutos de Ciência e Tecnologia (ICT)s e vinte e três laboratórios, o Exército possui um ICT e quatorze laboratórios, e a Aeronáutica conta com três ICTs e setenta e nove Laboratórios. O Quadro 16 apresenta a relação dos ICTs de cada FA.

Quadro 16 – Instituições de Ciência e Tecnologia (ICT) das Forças Armadas

FORÇA ARMADA	INSTITUIÇÃO DE CIÊNCIA TECNOLOGIA E INOVAÇÃO
Marinha	– Centro de Análises de Sistemas Navais (CASNAV) – Centro de Hidrografia da Marinha (CHM) – Centro Tecnológico da Marinha em São Paulo (CTMSP) – Centro Tecnológico do Corpo de Fuzileiros Navais (CTECCFN) – Escola de Guerra Naval (EGN) – Hospital Naval Marcílio Dias (HNMD) – Instituto de Estudos do Mar Almirante Paulo Moreira (IEAPM) – Instituto de Pesquisas da Marinha (IPqM) Laboratório Farmacêutico da Marinha (LFM) – Secretaria de Ciência, Tecnologia e Inovação da Marinha (SecCTM)
Exército	– Centro Tecnológico do Exército (CTEx)
Aeronáutica	– Instituto de Aeronáutica e Espaço (IAE) – Instituto de Estudos Avançados (IEAv) – Instituto de Fomento e Coordenação Industrial (IFI)

Fonte: Elaboração da Autora, 2015.

5.1.4 Academia

A Marinha possui escolas e centros de instrução voltados para o ensino militar, e o Centro de Coordenação de Estudos em São Paulo (CCEMSP) para a formação de engenheiros militares por meio da parceria com a Universidade de São Paulo (USP).

O Exército, além de suas escolas e academia destinadas ao ensino de estudos militares, tem no Instituto Militar de Engenharia (IME) a responsabilidade pelo ensino superior de Engenharia e pesquisa básica, para civis e militares.

A Aeronáutica também possui suas escolas e academia voltadas ao ensino de estudos militares, mas cabe ao Instituto Tecnológico de Aeronáutica (ITA) a formação de profissionais de nível superior nas especializações de interesse da Força Aérea e do setor aeroespacial, conforme a citação:

> (...) promover, por meio de educação, ensino, pesquisa e extensão, o progresso das ciências e tecnologias relacionadas ao campo aeroespacial. Destina-se, também, à formação de profissionais de nível superior nas especializações de interesse da Força Aérea e do setor aeroespacial em geral. Esse instituto está subordinado ao Departamento de Ciência e Tecnologia Aeroespacial (DCTA). É um dos elementos essenciais para o desenvolvimento do complexo científico-tecnológico aeroespacial. (BRASIL, 2012, p. 151)

5.1.5 Plano de Articulação e Equipamento de Defesa (PAED)

O Plano de Articulação e Equipamento de Defesa (PAED) foi apresentado no LBDN, em 2012, com o objetivo estabelecido conforme a citação:

> O PAED consubstancia, de forma coerente, os projetos estratégicos das forças Armadas que visam a atender às demandas por novas capacidades da defesa. (...) Para tanto, os projetos deverão integrar a estrutura programática orçamentária dos sucessivos Planos Plurianuais da União (PPA) no horizonte temporal de 20 anos (2012 a 2031) (BRASIL, 2012c, p. 192).

5.2 SUBSISTEMA SOCIAL

O subsistema social compreende as pessoas, as relações sociais entre os indivíduos, e as exigências de trabalho cabendo a ele a transformação da eficiência potencial em eficiência real. Os principais agentes e as exigências de trabalho, contidas em dispositivos legais e doutrinas, serão apresentados a seguir.

5.2.1 Fundamentos das Relações

Esta seção foi fundamentada nas doutrinas apresentadas no Manual Básico da Escola Superior de Guerra (ESG). A ESG é um instituto de altos estudos e pesquisas, e que tem a missão de articular e consolidar conhecimentos voltados ao exercício das funções de assessoramento e planejamento da segurança nacional no âmbito do Ministério da Defesa (BRASIL, 2012c).

Objetivos Nacionais

Segundo o Manual Básico da Escola Superior de Guerra existem três classificações para o termo Objetivos: os Individuais, os Grupais e os Nacionais. Neste estudo, importam os Objetivos Nacionais, que são definidos como aqueles que a Nação busca alcançar, a partir da identificação de necessidades, interesses e aspirações. Quanto a sua natureza, eles podem ser classificados em: Fundamentais, de Estado, e de Governo (ESG, 2011, p. 21-25), a saber:

> – Objetivos Fundamentais –são aqueles que visam atingir os mais elevados interesses da Nação e preservação de sua identidade, que são: democracia, integridade nacional, integridade do patrimônio nacional, paz social, progresso e soberania.
> – Objetivos de Estado – são Objetivos Nacionais intermediários que visam atender as necessidades, interesses e aspirações, considerados de alta relevância para a conquista, consolidação e manutenção dos Objetivos Fundamentais.
> – Objetivos de Governo – são Objetivos Nacionais intermediários, para atender de imediato as necessidades, interesses e aspirações, decorrentes de situações conjunturais em um ou mais períodos de Governo (ESG, 2011, p. 21-25).

Poder Nacional

O Poder Nacional é entendido como a "capacidade que tem o conjunto de Homens e Meios que constituem a Nação para alcançar e manter os Objetivos Nacionais, em conformidade com a Vontade Nacional". Ele se estrutura em cinco Expressões: Política; a Econômica; Psicossocial; Militar e Científica e Tecnológica, que facilita sua aplicação no processo de planejamento. O Quadro 17 apresenta as dimensões da relação entre as Expressões, que são manifestações do Poder Nacional, com os Fundamentos do Poder Nacional, que são observados como elementos básicos da nacionalidade. Ele pode ser lido por linha ou coluna, permitindo a análise do Poder Nacional a partir do enfoque das manifestações ou Fundamentos (ESG, 2011, p. 30-37).

Quadro 17 – Dimensões da Relações entre as Expressões e os Fundamentos Poder Nacional

PODER NACIONAL					
FUNDA-MENTOS	**EXPRESSÕES**				
	Política	**Econômica**	**Psicosso-cial**	**Militar**	**C&T**
Homem	Povo	Recursos	Pessoa Humana	Recursos	Recursos Humanos
Terra	Território	Recursos Naturais	Ambiente	Território	Recursos Naturais e Materiais
Instituições	Institui-ções Políticas	Instituições Econômi-cas	Institui-ções Sociais	Institui-ções Militares	Institui-ções C&T

Fonte: ESG (2011, p.36).

Políticas

Entende-se Política como "a arte de fixar objetivos e orientar o emprego dos meios necessários à sua conquista". Cabe à sociedade nacional, por meio da Política, estabelecer os seus objetivos e, nestes apoiada, compor uma ordem social justa, distinguir o setor público do privado, estruturar o Estado, garantir os direitos individuais e inserir-se no contexto internacional. As Políticas de classificam em (ESG, 2011, p. 43-46):

> – Política de Governo: é o "conjunto dos Objetivos de Governo, bem como a orientação para o emprego do Poder Nacional, atuando em consonância com a conjuntura".
> – Política Nacional: se manifesta quando se busca aplicar racionalmente o Poder Nacional, orientando-o para o Bem Comum, por meio do alcance e da manutenção dos Objetivos Fundamentais. "Política Nacional é o conjunto dos Objetivos Fundamentais bem como a orientação para emprego do Poder Nacional, atuando em conformidade com a Vontade Nacional".
> – Política de Estado: é o "conjunto de Objetivos de Estado, bem como a orientação para o Emprego do Poder Estatal, atuando em consonância com os relevantes interesses nacionais" (ESG, 2011, p. 43-46).

Estratégia Nacional

A Estratégia é entendida como "A arte de preparar e aplicar o poder para conquistar e preservar objetivos, superando Óbices de toda ordem. " (ESG, 2011, p. 49).

Segurança Nacional

Mesmo sendo encargo do Estado, a Segurança Nacional envolve a aplicação do Poder Nacional como um todo. A "Segurança Nacional é a sensação de garantia para a Nação, da conquista e manutenção dos seus Objetivos Fundamentais proporcionada pela aplicação do seu Poder Nacional. " Faz referência aos Objetivos Fundamentais da Nação, pois garante a busca e preservação dos objetivos de Soberania, Democracia,

Integração Nacional, Integridade do Patrimônio Nacional, Progresso e Paz Social (ESG, 2011, p.68-69).

> A **Segurança Nacional** decorre da necessidade de proteção da sociedade como um todo e da preservação dos Objetivos Fundamentais, por intermédio do atendimento das necessidades, interesses e aspirações nacionais, obtido pela consecução dos Objetivos de Estado e de Governo. (ESG, 2011, p, 68)
> A preservação da **Segurança Nacional** é, fundamentalmente, um encargo do Estado, uma vez que ele é a instituição concentradora do **poder coercitivo** por excelência e representa, por delegação, os interesses da Sociedade Nacional. A responsabilidade pela preservação da **Segurança Nacional**, no entanto, não é exclusiva do **Estado**, mas de toda a **Nação**, cuja sobrevivência reclama a cooperação da comunidade nacional e de cada indivíduo. (ESG, 2011, p, 69)

Defesa

A Defesa "é um ato ou conjunto de atos realizados para obter ou resguardar as condições que proporcionam a sensação de Segurança. " (ESG, 2011, p.66)

Defesa Nacional

A Defesa Nacional representa o "conjunto de atitudes, medidas e ações do Estado, com ênfase na Expressão Militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais e manifestas. " (ESG, 2011, p. 70)

Política de Defesa Nacional

A Política de Defesa Nacional é entendida como:

> Política de Defesa Nacional é o conjunto de Objetivos de Governo bem como a orientação do Poder Nacional no sentido de conquistá-los e mantê-los, superando ameaças e agressões de

> qualquer natureza que se manifestem, ou possam manifestar-se, contra a Segurança e o Desenvolvimento da Nação. (ESG, 2011, p.72)

5.2.2 Dispositivos Legais

Relacionados à BID

A Portaria Normativa Nº 764/MD, de 27 de dezembro de 2002, institui a Política e Diretrizes de Compensação Comercial, Industrial e Tecnológica do Ministério da Defesa, com os objetivos de promover o crescimento tecnológico e qualitativo das indústrias de defesa e aquisição de novas tecnologias; fortalecer os setores de interesse do MD para aumentar a carga de trabalho e a competitividade das indústrias de defesa; ampliar o mercado de trabalho, criando novas oportunidades e especialização; obter recursos externos para elevar a capacitação industrial e tecnológica; e incrementar a nacionalização das tecnologias e a independência do mercado externo (BRASIL, 2002)

A Portaria Normativa Nº 1.317/MD, de 4 de novembro de 2004, aprova a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional (PCTI), coma finalidade de apresentar os objetivos estratégicos, orientar as instituições, estimular a pesquisa, fomentar o desenvolvimento industrial, e gerar produtos inovadores. São objetivos estabelecidos na PCTI (BRASIL, 2004a):

> – Ampliação do conteúdo tecnológico dos produtos e serviços de interesse da Defesa Nacional.
> – Elevação do nível de capacitação de recursos humanos.
> – Aprimoramento da infraestrutura de Ciência e Tecnologia (C&T) de apoio a programas e projetos de interesse da Defesa Nacional.
> – Criação de um ambiente favorável à inovação e à competitividade industrial.
> – Implantação de mecanismos de financiamento das atividades de Ciência, Tecnologia e Inovação (C,T&I) de interesse da Defesa Nacional.
> – Ampliação do interesse dos diversos segmentos da sociedade pelas iniciativas nas áreas de C,T&I voltadas para a Defesa Nacional.

> – Aprimoramento da imagem de excelência institucional.
> – Integração das iniciativas de C,T&I de interesse da Defesa Nacional, conduzidas nas organizações militares de Pesquisa e Desenvolvimento (P&D),nos institutos e nas universidades civil.
> – Estabelecimento de política de valorização de recursos humanos, baseada em resultados.
> – Implantação de sistemática que integre o planejamento estratégico, o ciclo de desenvolvimento de produtos e serviços de interesse da Defesa Nacional e a avaliação de resultados (BRASIL, 2004a).

A Portaria Nº 611/MD, de 12 de maio de 2005, criou a Comissão Militar da Indústria de Defesa (CMID), tendo como algumas das atribuições: fomentar e coordenar as atividades de pesquisa, desenvolvimento, produção e exportação de produtos de defesa; e incentivar a capacitação dos recursos humanos (BRASIL, 2005c).

A Portaria Normativa Nº 899, de 19 de julho de 2005, aprovou a Política Nacional da Indústria de Defesa (PNID), onde definiu a Base Industrial de Defesa e Produto Estratégico de Defesa, como (BRASIL, 2005b):

> I -Base Industrial de Defesa (BID): é o conjunto das empresas estatais e privadas, bem como organizações civis e militares, que participem de uma ou mais das etapas de pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos estratégicos de defesa; e
> II - Produto Estratégico de Defesa como “bens e serviços que pelas peculiaridades de obtenção, produção, distribuição, armazenagem, manutenção ou emprego possam comprometer, direta ou indiretamente, a consecução de objetivos relacionados ``a segurança ou à defesa do país (BRASIL, 2005b).

A PNID objetiva conscientizar a sociedade sobre a importância do fortalecimento da BID, diminuir a dependência externa dos produtos de defesa, reduzir carga tributária, aumentar a capacidade de aquisição, melhor a qualidade tecnológica dos produtos, aumentar a

competitividade, e a capacidade de mobilização industrial (BRASIL, 2005b).

A Portaria Normativa Nº 777/MD, de 31 de maio de 2007, cria a Comissão de Implantação do Sistema de Certificação, Metrologia, Normalização, e Fomento Industrial das Forças Aramadas (COMISCEMEFA), com a atribuição de estudar, analisar, acompanhar e assessorar nos assuntos pertinentes à implantação do Sistema de Certificação, Metrologia, Normalização, e Fomento Industrial das Forças Aramadas (SISCEMEFA) (BRASIL, 2007b).

A Lei Nº 12.598, de 21 de março de 2012, estabelece normas especiais para compras, contratações e desenvolvimento de produtos e de sistemas de defesa; dispõe sobre regras de incentivo à área estratégica de defesa, conforme parágrafo único do Art. 1º:

> Parágrafo único. Subordinam-se ao regime especial de compras, de contratações de produtos, de sistemas de defesa, e de desenvolvimento de produtos e de sistemas de defesa, além dos órgãos da administração direta, os fundos especiais, as autarquias, as fundações públicas, as empresas públicas e privadas, as sociedades de economia mista, os órgãos e as entidades públicas fabricantes de produtos de defesa e demais entidades controladas, direta ou indiretamente, pela União, pelos Estados, pelo Distrito Federal e pelos Municípios (BRASIL, 2012a).

Ao instituir o Regime Especial Tributário para a Indústria de Defesa (RETID) para as Empresas Estratégicas de Defesa que produzem ou desenvolvem bens de defesa nacional ou prestem serviços de manutenção, conservação, modernização, reparo, revisão, conversão e industrialização de PRODE, fortalece a BID e favorece o desenvolvimento econômico. Quanto aos produtos amparados pela Lei supracitada, estes devem se enquadrar nas considerações do art. 2º, são elas (BRASIL, 2012a):

> I - **Produto de Defesa - PRODE** - todo bem, serviço, obra ou informação, inclusive armamentos, munições, meios de transporte e de comunicações, fardamentos e materiais de uso individual e coletivo utilizados nas atividades

> finalísticas de defesa, com exceção daqueles de uso administrativo;
> II - **Produto Estratégico de Defesa - PED** - todo Prode que, pelo conteúdo tecnológico, pela dificuldade de obtenção ou pela imprescindibilidade, seja de interesse estratégico para a defesa nacional, tais como:
> a) recursos bélicos navais, terrestres e aeroespaciais;
> b) serviços técnicos especializados na área de projetos, pesquisas e desenvolvimento científico e tecnológico;
> c) equipamentos e serviços técnicos especializados para as áreas de informação e de inteligência;
> III - **Sistema de Defesa - SD** - conjunto inter-relacionado ou interativo de Prode que atenda a uma finalidade específica;(...) (BRASIL, 2012a)

O Decreto Nº 7.970, de 28 de março de 2013, regulamenta os dispositivos da Lei Nº 12.598/2012, e cria a Comissão Mista da Indústria de Defesa (CMID), com a finalidade de assessorar o Ministro da Defesa em processos decisórios e em proposições de atos relacionados à indústria nacional de defesa. São atribuições do CMID (BRASIL, 2013):

> – Propor e coordenar estudos relativos à PNID.
> – Promover a integração entre o MD e órgãos e entidades públicos e privados relacionadas à BID.
> – Emitir parecer e propor ao Ministro da Defesa as classificações de bens, serviços, obras ou informações como Produto de Defesa – PRODE.
> – Emitir parecer e propor ao Ministro da Defesa as classificações de conjunto inter-relacionado ou interativo de Produto de Defesa como Sistema de Defesa (SD).
> – Propor ao Ministro da Defesa a classificação de PRODE como Produto Estratégico de Defesa (PED).
> – Propor ao Ministro da Defesa o credenciamento de Empresa de Defesa como Empresa Estratégica de Defesa (EED).
> – Propor ao Ministro da Defesa políticas e orientações sobre processos de aquisição,

> importação e financiamento de PRODE, PED e SD.
> – Apreciar e emitir parecer sobre os Termos de Licitação Especial – TLE (BRASIL, 2013).

Sobre a catalogação e o credenciamento, este Decreto, estabelece que os PRODE sejam catalogados como previsto no Sistema Militar de Catalogação das Forças Armadas (SISMICAT), e as exceções são analisadas conforme sua participação na cadeia produtiva da indústria nacional de defesa ou sua destinação finalística de defesa e propostas pelo CMID. Prevê que as empresas que desejarem o credenciamento no SISMICAT como Empresa de Defesa (ED), deverão solicitá-lo no SISMICAT, apresentando a Declaração de Processo Produtivo (DPP) ou a Declaração de Conteúdo Nacional (DCN) dos seus PRODE ou SD (BRASIL, 2013).

Sobre o TLE, o Decreto estabelece que deve ter indicação clara e precisa do objeto, e apresentar a análise entre benefício e custo e as razões da opção de utilização do procedimento licitatório abrangido no RETID. O TLE poderá conter informações tais como: o percentual mínimo de conteúdo nacional; capacidade inovadora exigida; contribuição para aumentar a capacidade tecnológica e produtiva da base industrial de defesa; sustentabilidade do ciclo de vida do PRODE; garantia de continuidade das capacitações tecnológicas e produtivas (BRASIL, 2013a).

Outros dispositivos que regulamentam o RETID são o Decreto Nº 8.122, de 16 de outubro de 2013 (BRASIL, 2013c), e a Instrução Normativa RFB Nº 1.454 (BRASIL, 2014) que dispõe sobre a aplicação do RETID.

A Portaria Normativa Nº 3.214/MD, de 26 de novembro de 2013, dispõe sobre a organização e funcionamento da CMID, criada pelo Decreto Nº 7.970/2013. (BRASIL, 2013c)

Relacionados ao Sigilo, Segredo Industrial e Pedido de Patente

O art, 75 da Lei N. 9.279, de 14 de maio de 1996, estabelece que quando o objeto do pedido de patente originário do Brasil for de interesse da Defesa Nacional, o mesmo se processará em caráter sigiloso, prevê o trâmite do pedido e a indenização de criação, assim como, veda o depósito no exterior de um pedido de patente cujo objeto seja sigiloso, conforme a citação (BRASIL, 1996):

> Art. 75. O pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso e não estará sujeito às publicações previstas nesta Lei.
>
> § 1º O INPI encaminhará o pedido, de imediato, ao órgão competente do Poder Executivo para, no prazo de 60 (sessenta) dias, manifestar-se sobre o caráter sigiloso. Decorrido o prazo sem a manifestação do órgão competente, o pedido será processado normalmente.
>
> § 2º É vedado o depósito no exterior de pedido de patente cujo objeto tenha sido considerado de interesse da defesa nacional, bem como qualquer divulgação do mesmo, salvo expressa autorização do órgão competente.
>
> § 3º A exploração e a cessão do pedido ou da patente de interesse da defesa nacional estão condicionadas à prévia autorização do órgão competente, assegurada indenização sempre que houver restrição dos direitos do depositante ou do titular. (BRASIL, 1996)

Embora o art 1º do Decreto Nº 2.553, de 16 de abril de 1998, que regulamenta os arts. 75 e 88 a 93 da Lei 9.279, de 14 de maio de 1996, estabeleça competências para órgãos hoje extintos, as demais determinações estão em vigor e regulam os direitos e obrigações referente à propriedade industrial, conforme citação (BRASIL, 1998c):

> Art 1º A Secretaria de Assuntos Estratégicos da Presidência da República é o órgão competente do Poder Executivo para manifestar-se, por iniciativa própria ou a pedido do Instituto Nacional da Propriedade Industrial - INPI, sobre o caráter sigiloso dos processos de pedido de patente originários do Brasil, cujo objeto seja de interesse da defesa nacional.
>
> § 1º O caráter sigiloso do pedido de patente, cujo objeto seja de natureza militar, será decidido com base em parecer conclusivo emitido pelo Estado-Maior das Forças Armadas, podendo o exame técnico ser delegado aos Ministérios Militares.
>
> § 2º O caráter sigiloso do pedido de patente de interesse da defesa nacional, cujo objeto seja de natureza civil, será decidido, quando for o caso,

> com base em parecer conclusivo dos Ministérios a que a matéria esteja afeta.
> § 3º Da patente resultante do pedido a que se refere o caput deste artigo, bem como do certificado de adição dela decorrente, será enviada cópia ao Estado-Maior das Forças Armadas e à Secretaria de Assuntos Estratégicos da Presidência da República, onde será, também, conservado o sigilo de que se revestem tais documentos. (BRASIL, 1998c)

Como dito, foram extintos a Secretaria de Assuntos Estratégicos da Presidência da República, o Estado Maior das Forças Armadas, e os Ministérios Militares passaram à três Comandos distintos para cada força: da Marinha, do Exército e da Aeronáutica. Verifica-se a necessidade de revisão do dispositivo legal para que se estabeleça seu propósito e obediência.

O art. 22 da Lei Nº 12.527, de 12 de maio de 2011, mantém a restrição de acesso à informação das hipóteses legais de sigilo, segredo de justiça, segredo industrial, e não se aplica o acesso prevista na lei para as informações referentes a projetos de P&D de Defesa; e dispõe sobre a proteção e controle de informações sigilosas por parte de entidades públicas e privadas, conforme o arts. 7 e 25 a 26 (BRASIL, 2011):

> Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter:
> [...]
> § 1º O acesso à informação previsto no caput não compreende as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado. [...]
> Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.
> § 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das

> atribuições dos agentes públicos autorizados por lei.
> § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.
> § 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.
> Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas.
> Parágrafo único**.** A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei. (BRASIL, 2011)

A Lei supracitada prevê também a classificação da informação e acesso restrito e o controle por meio de credenciais de segurança, conforme os arts. 23 25:

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; [...]
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; [...]
> Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas

> por seus órgãos e entidades, assegurando a sua proteção.
> § 1o O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei. (BRASIL, 2011)

5.2.3 Políticas e Estratégias para a BID

A Política de Defesa Nacional (PDN)

A Política de Defesa Nacional (PDN), que foi aprovada pelo Decreto Nº 5.484, de 30 de junho de 2005, representa uma referência de alto nível para o planejamento em Defesa que visa estabelecer "objetivos e diretrizes para o preparo e o emprego da capacitação nacional, com o envolvimento dos setores militar e civil, em todas as esferas do Poder Nacional". Seus princípios estão em conformidade com a Constituição Federal. Embora o Brasil seja um país pacífico, "Um dos propósitos da Política de Defesa Nacional é conscientizar todos os segmentos da sociedade brasileira de que a defesa da Nação é um dever de todos os brasileiros". A PDN está dividida em duas partes, a primeira de cunho político e a segunda estratégico, como apresentado a seguir: (BRASIL, 2005a).

A primeira parte consiste em:

> a) Segurança e Defesa: onde Segurança significa a condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais; e a Defesa Nacional significa um conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças

> preponderantemente externas, potenciais ou manifestas.
> b) Ambiente internacional, que pode ser ameaçado por disputas de áreas marítimas, pelo domínio aeroespacial e por fontes de água doce e de energia, pela invasão das fronteiras, por crises econômicas globais, além das ameaças advindas dos avanços da TICs que criam vulnerabilidades que podem ser exploradas com o objetivo de inviabilizar o uso dos nossos sistemas ou facilitar a interferência à distância.
> c) Ambiente regional e o entorno estratégico refere-se à situação geopolítica do Brasil no subcontinente da América do Sul. (BRASIL, 2005a)

A segunda parte consiste em:

> a) Prevenção - reside na valorização da ação diplomática como instrumento primeiro de solução de conflitos e em postura estratégica baseada na existência de capacidade militar com credibilidade, apta a gerar efeito dissuasório.
> b) Fortalecimento da capacitação do País no campo da defesa é essencial e deve ser obtido com o envolvimento permanente dos setores governamental, industrial e acadêmico, voltados à produção científica e tecnológica e para a inovação. O desenvolvimento da indústria de defesa, incluindo o domínio de tecnologias de uso dual, é fundamental para alcançar o abastecimento seguro e previsível de materiais e serviços de defesa.
> d) Integração regional da indústria de defesa, a exemplo do Mercosul, deve ser objeto de medidas que propiciem o desenvolvimento mútuo, a ampliação dos

> mercados e a obtenção de autonomia estratégica (BRASIL, 2005a).

Das diretrizes estabelecidas na PDN destacamos a seguir aquelas relacionadas a este estudo, que são (BRASIL, 2005a):

> a) Garantir recursos suficientes e contínuos que proporcionem condições efetivas de preparo e emprego das Forças Armadas e demais órgãos envolvidos na Defesa Nacional, em consonância com a estatura político-estratégica do País.
> b) Incentivar a conscientização da sociedade para os assuntos de Defesa Nacional.
> c) Estimular a pesquisa científica, o desenvolvimento tecnológico e a capacidade de produção de materiais e serviços de interesse para a defesa.
> d) Intensificar o intercâmbio das Forças Armadas entre si e com as universidades, instituições de pesquisa e indústrias, nas áreas de interesse de defesa.
> e) Contribuir ativamente para o fortalecimento, a expansão e a consolidação da integração regional com ênfase no desenvolvimento de base industrial de defesa.
> f) Criar novas parcerias com países que possam contribuir para o desenvolvimento de tecnologias de interesse da defesa. (BRASIL, 2005a)

A Estratégia Nacional de Defesa (END)

A END, aprovada pelo Decreto Nº 6.703, de 18 de dezembro de 2008, estabelece ações estratégicas de médio e longo prazo, com objetivo de modernizar a estrutura nacional de defesa que se apoia em três eixos estruturantes: a reorganização das FA; a reestruturação da Indústria Brasileira de Material de Defesa; e a política de composição dos efetivos das FA. (BRASIL, 2008b, p. 5).

O interesse deste estudo recai sobre o eixo estruturante da reestruturação da Indústria de Defesa, que visa atender as necessidades de equipamento das FA enfatizando o desenvolvimento de tecnologias nacionais, para mitigar e eliminar a dependência estrangeira. Destacamos a seguinte citação que une a END à Estratégia Nacional de Desenvolvimento:

> Estratégia acional de defesa é inseparável de estratégia nacional de desenvolvimento. Esta motiva aquela. Aquela fornece escudo para esta. Cada uma reforça as razões da outra. Em ambas, se desperta para a nacionalidade e constrói-se a Nação. Defendido, o Brasil terá como dizer não, quando tiver que dizer não. Terá capacidade para construir seu próprio modelo de desenvolvimento. [...]
>
> Projeto forte de defesa favorece projeto forte de desenvolvimento. Forte é o projeto de desenvolvimento que, sejam quais forem suas demais orientações, se guie pelos seguintes princípios:
>
> a) Independência nacional, efetivada pela mobilização de recursos físicos, econômicos e humanos, para o investimento no potencial produtivo do País. Aproveitar a poupança estrangeira, sem dela depender;
>
> b) Independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento [...]. (BRASIL, 2008b, p. 8-9)

A diretriz sobre dissuasão de forças hostis prevê a prontidão das FA, que tem a tecnologia como um instrumento de apoio ao combate (BRASIL, 2008b, p. 11).

Quanto à reorganização da Indústria de Defesa, a END estabelece as seguintes diretrizes:

> a. Dar prioridade ao desenvolvimento de capacitações tecnológicas independentes.
>
> Essa meta condicionará as parcerias com países e empresas estrangeiras ao desenvolvimento progressivo de pesquisa e de produção no País.

b. Subordinar as considerações comerciais aos imperativos estratégicos.
Isso importa em organizar o regime legal, regulatório e tributário da indústria nacional de material de defesa para que reflita tal subordinação.
c. Evitar que a indústria nacional de material de defesa polarize-se entre pesquisa avançada e produção rotineira.
Deve-se cuidar para que a pesquisa de vanguarda sirva à produção de vanguarda.
d. Usar o desenvolvimento de tecnologias de defesa como foco para o desenvolvimento de capacitações operacionais.
Isso implica buscar a modernização permanente das plataformas, seja pela reavaliação à luz da experiência operacional, seja pela incorporação de melhorias provindas do desenvolvimento tecnológico.
2. Estabelecer-se-á, para a indústria nacional de material de defesa, regime legal, regulatório e tributário especial.[...]
3. O componente estatal da indústria de material de defesa terá por vocação produzir o que o setor privado não possa projetar e fabricar, a curto e médio prazo, de maneira rentável. Atuará, portanto, no teto, e não no piso tecnológico. Manterá estreito vínculo com os centros avançados de pesquisa das próprias Forças Armadas e das instituições acadêmicas brasileiras.
4. O Estado ajudará a conquistar clientela estrangeira para a indústria nacional de material de defesa.[...]
9. Resguardados os interesses de segurança do Estado quanto ao acesso a informações, serão estimuladas iniciativas conjuntas entre organizações de pesquisa das Forças Armadas, instituições acadêmicas nacionais e empresas privadas brasileiras. O objetivo será fomentar o desenvolvimento de um complexo militar-universitário-empresarial capaz de atuar na fronteira de tecnologias que terão quase sempre utilidade dual, militar e civil. (BRASIL, 2008b, p. 34-37)

A END reconhece a existência de vulnerabilidades na estrutura de defesa do Brasil, tais como:

> - obsolescência da maioria dos equipamentos das Forças Armadas; elevado grau de dependência em relação a produtos de defesa estrangeiros; e ausência de direção unificada para aquisições de produtos de defesa;
> - limitados recursos aplicados em pesquisa científica e tecnológica para o desenvolvimento de material de emprego militar e produtos de defesa, associados ao incipiente nível de integração entre os órgãos militares de pesquisa, e entre estes e os institutos civis de pesquisa;
> - inexistência de planejamento nacional para desenvolvimento de produtos de elevado conteúdo tecnológico, com participação coordenada dos centros de pesquisa das universidades, das Forças Armadas e da indústria;
> - inexistência de regras claras de prioridade à indústria nacional, no caso de produtos de defesa fabricados no País;
> - bloqueios tecnológicos impostos por países desenvolvidos, retardando os projetos estratégicos de concepção brasileira. (BRASIL, 2008b, p. 42-43)

Do mesmo modo, a END aponta oportunidades, tais como:

> - otimização dos esforços em Ciência, Tecnologia e Inovação para a Defesa, por intermédio, dentre outras, das seguintes medidas:
> (a) maior integração entre as instituições científicas e tecnológicas, tanto militares como civis, e a indústria nacional de defesa;
> (b) definição de pesquisas de uso dual; e
> (c) fomento à pesquisa e ao desenvolvimento de produtos de interesse da defesa. [...]
> - maior integração entre as indústrias estatal e privada de material de defesa, com a definição de um modelo de participação na produção nacional de meios de defesa; [...]
> - integração e definição centralizada na aquisição de produtos de defesa de uso comum, compatíveis

> com as prioridades estabelecidas. (BRASIL, 2008b, p.44)

Política Nacional da Indústria de defesa (PNID – 2005)

A Política Nacional da Indústria de Defesa (PNID), foi aprovada pela Portaria Normativa Nº 899/2005, tem como objetivo geral o fortalecimento da BID, como também (BRASIL, 2005b):

> – Conscientização da sociedade em geral quanto à necessidade de o País dispor de uma forte BID.
> – Diminuição progressiva da dependência externa de produtos estratégicos de defesa, desenvolvendo-os e produzindo-os internamente.
> – Redução da carga tributária incidente sobre a BID, com especial atenção às distorções relativas aos produtos importados.
> – Ampliação da capacidade de aquisição de produtos estratégicos de defesa da indústria nacional pelas Forças Armadas.
> – Melhoria da qualidade tecnológica dos produtos estratégicos de defesa.
> – Aumento da competitividade da BID brasileira para expandir as exportações.
> – Melhoria da capacidade de mobilização industrial na BID (BRASIL, 2005b).

5.2.4 Agentes

Do setor Indústria

A Indústria de Defesa é responsável pela produção, que é fortemente afetada pelo orçamento de Defesa, que limita a demanda dos PRODE, e pelo nível da qualificação técnica exigida do seu pessoal, conforme citação:

> (...) para as empresas há escassez de dois recursos: de ordem financeira para a realização de investimentos e recursos humanos habilitados. O governo, representado principalmente pelo Ministério da Defesa − compreendendo as três Forças Armadas −, é o ator principal na provisão de recursos financeiros.

> As instituições de ensino superior, os centros de pesquisa e de desenvolvimento e as próprias organizações industriais são atores igualmente importantes para a qualificação de mão de obra para o setor. Assim, não há como compreender a dependência da indústria com relação às Forças Armadas sem o preciso entendimento de como a demanda por artigos, sistemas e serviços de defesa é constituída (MATHEUS, 2010, p.61).

Assim, a indústria trabalhar exclusivamente por demanda, ou seja, precisa "produzir para vender", conforme:

> O fato de que neste segmento, ao contrário de outros de bens de características tecnológicas semelhantes (o automobilístico, por exemplo), a lógica é "vender para produzir" e não "produzir para vender", é uma das razões que explicam esse comportamento. (DAGNINO e FILHO, 2009, p. 196)

Como forma de se manterem no mercado, um dos desafios está na permanência do quadro técnico especializado que é afetada pela carga de trabalho nas empresas, e que pode ser minimizada pelo emprego de tecnologias de uso dual (MATHEUS, 2010, p. 64)

As federações e associações do setor da indústria de Defesa atuam como representantes dos interesses e reinvindicações dos empresários do setor perante outros segmentos. Destacamos a Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE), fundada em 1985; o Departamento da Indústria de Defesa (Comdefesa), instituído em 2007 e pertencente à Federação das Indústrias do Estado de São Paulo (FIESP).

Do setor Governo

O Ministério da Defesa (MD), conforme a Lei Complementar Nº 97, de 9 de junho de 1999, tem a função de exercer a direção superior das Forças Armadas (FA). (BRASIL, 1999a)

O Art. 9º da Lei supracitada, é competência do Ministério da Defesa, dentre outras, as seguintes: Política de Defesa Nacional, Estratégia Nacional de Defesa e elaboração do Livro Branco de Defesa Nacional; Política de Ciência, Tecnologia e Inovação (C,T&I) de Defesa;

Política Nacional: de exportação de produtos de Defesa e fomento às atividades de pesquisa e desenvolvimento, produção e exportação em áreas de interesse da defesa e controle da exportação de produtos de defesa; de indústria de defesa; e de inteligência de Defesa; Projetos especiais de interesse da Defesa Nacional; Inteligência estratégica e operacional no interesse da Defesa; Relacionamento internacional de Defesa; Orçamento de Defesa; e Legislação de Defesa e militar; política de ensino de Defesa. (BRASIL, 1999a)

O MD tem papel importante na Defesa Nacional, conforme citação:

> (...) ator político responsável por fomentar a cooperação com os demais setores governamentais relacionados com a defesa do País, alinhando projetos de defesa com os programas desenvolvidos por outras áreas do governo (BRASIL, 2008b).

O Ministro de Defesa preside o Conselho Militar de Defesa (CMiD), que é composto pelos Comandantes de cada FA e Chefe do Estado-Maior Conjunto das Forças Armadas, cuja missão é assessorar o Presidente da República no emprego dos meios militares, e do próprio MD. (BRASIL, 2012, p. 55-56)

O Estado-Maior Conjunto das Forças Armadas (EMCFA) é um órgão de assessoramento, com a competência de elaborar o planejamento do emprego conjunto das Forças Armadas e assessorar o Ministro de Estado da Defesa na direção superior das FA e na condução dos exercícios conjuntos e quanto à atuação de forças brasileiras em operações de paz (BRASIL, 2013b)**.**

A Comissão Militar da Indústria de Defesa (CMID), que foi estabelecida pela Portaria nº 611/MD, de 12 de maio de 2005, CMID tem como atribuições (BRASIL, 2005 c):

> – Propor, coordenar e integrar atividades e estudos relativos ao fomento às atividades de pesquisa, de desenvolvimento, de produção e de exportação de produtos de defesa.
> – Estabelecer um fluxo adequado de informações entre o MD e as entidades civis e governamentais envolvidas.

> – Propor medidas com vistas a incentivar a capacitação dos recursos humanos necessários (BRASIL, 2005c).

Cabe à Secretaria de Produtos de Defesa (SEPROD) acompanhar a execução e assessorar na formulação e atualização da Política Nacional de Ciência, Tecnologia e Inovação de Defesa; da Política Nacional da Indústria de Defesa e da Política de Obtenção de Produtos de Defesa, assim como, normaliza e supervisiona as ações relativas ao controle das importações e exportações de produtos de defesa.

As Forças Armadas (FA) são constituídas por "instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República", são elas: Marinha, Exército e Aeronáutica, cuja missão compreende a "defesa da Pátria, a garantia dos poderes constitucionais e, da lei e da ordem", conforme estabelecido no Art, 12, da Constituição Federal do Brasil (BRASIL, 1988).

O Livro Branco de Defesa Nacional (LBDN) prevê o emprego da expressão militar fundamentado na capacidade das FA e no potencial dos recursos disponíveis (material e humano). Cabe ao MD a coordenação do esforço integrado de Defesa Nacional. (BRASIL, 2012c).

Do setor Academia

O MD possui dois centros de pesquisa: o Instituto Pandiá Calógenas (IPC) e a Escola Superior de Guerra (ESG).

O IPC tem a missão de contribuir para o pensamento sobre Segurança Internacional e Defesa Nacional no Brasil. Assiste o Ministro da Defesa com a produção de análises independentes sobre temas prioritários para a Defesa Nacional, com ênfase em três linhas de pesquisa: Entorno estratégico (América do Sul e Atlântico Sul); Economia da defesa e Cenários prospectivos e guerra do futuro. Também promove o diálogo com a academia e a sociedade civil (BRASIL, 2015c).

A ESG, criada em 1949, "é um instituto de altos estudos e pesquisas no campo da segurança e defesa nacional". Tem a missão de articular e consolidar conhecimentos voltados ao exercício das funções de assessoramento e planejamento da segurança nacional no âmbito do Ministério da Defesa (BRASIL, 2015c).

As instituições de ensino militares e civis atuam gerando conhecimentos e formando profissionais com qualificação específica para atuarem nos Centros de Pesquisa e na Indústria de Defesa. Destacamos a

Associação Brasileira de Estudos de Defesa, uma sociedade acadêmica civil fundada em 2005, que tem atuado promovendo encontros nacionais, estaduais e regionais para reunir pesquisadores e discutir os estudos de defesa.

5.3 CONCLUSÃO DO CAPÍTULO

Concluímos este capítulo apresentando a concepção do modelo Sociotécnico para a BID, destacando as inter-relações existentes entre os subsistemas e o ambiente externo, como apresentado na Figura 19.

Figura 19 – Sistema Sociotécnico para a BID

Fonte: Elaboração da autora, 2015

Conforme a Figura 19, o Ambiente Externo que contém o Ambiente da BID apresenta a origem, de onde são importados os insumos, e o destino, para onde são exportados os produtos. No ambiente externo se posicionam os agentes e as exigências de trabalho (requisitos), estes contidos em dispositivos legais e doutrinas. Os principais agentes citados foram o Governo, a academia, o MD e as Forças Armadas.

O modelo de Tavistock considera a organização como um Sistema Sociotécnico estruturado sobre dois subsistemas. Contidos no Ambiente da BID se encontra o Sistema Sociotécnico para a BID, constituído pelos Subsistemas Técnico e o Subsistema Social.

A Figura 19 representa também as relações e interações entre os Subsistemas, bem como as relações com o Ambiente Externo.

Subsistema Técnico é o responsável pela eficiência potencial e compreende as tarefas a serem desempenhadas, instalações e equipamentos. O Subsistema Social por sua vez compreende as pessoas, as relações sociais entre os indivíduos, e as exigências de trabalho.

Uma vez que os subsistemas estão interagindo e sendo mutuamente influenciados, ocorre, de forma contínua, a conversão dos insumos importados em produtos para serem exportados.

6 AMBIENTE DE INOVAÇÃO DA BID

O propósito deste capítulo é caracterizar o Ambiente de Inovação da BID, considerando a atuação dos agentes de C,T&I e os ciclos de vida dos produtos de Defesa de cada FA.

A gestão das inovações no setor de Defesa acontece por meio de vários sistemas sem interface e segregados (fragmentado e desarticulado) (FRANCO-AZEVEDO, 2013, p.21; CUNHA e AMARANTE, 2011, p.18).

O caminho percorrido para o desenvolvimento deste capítulo conta com a caracterização da estrutura BID; o levantamento dos projetos estratégicos que norteiam as ações de produção de Defesa; a identificação dos ambientes de CT&I e seus respectivos Ciclos de Vida dos Produtos, e por fim, representar o Sistema de Produção do Ambiente de Inovação da BID.

6.1 PROPÓSITO E REALIDADE DA BASE INDUSTRIAL DE DEFESA (BID)

O conceito Base Industrial de Defesa (*Defense Industrial Base* – DIB) é comumente encontrado na literatura sobre economia de gastos militares, porque a maioria das Nações tem uma BID. Uma nova visão foi proposta em 1995, onde a BID se representava por um setor ou grupo de indústrias que são dependentes em algum dos diversos níveis do orçamento de Defesa, e onde o Estado é tributário por demandar produtos necessários para a Defesa Nacional, assim a BID participa ativamente do orçamento da Defesa, e integra os interesses que compõem um Complexo Industrial de Defesa (DUNNE, 1995, p. 401). Esse estudo é considerado percursor e referência para definição da BID (MASSON, 2014, p. 147).

Dunne (1995, p. 399-429) propôs considerar a diversidade de produtos produzidos pela BID, porque as armas diferem desde a produção de armas de alta tecnologia e caros sistemas de armas até as inexpressivas pequenas armas. Assim, apresentou uma classificação em três grupos, considerando a relação dos produtos com ações militares ou de guerra, sendo:

1º. Sistemas de armas e equipamentos letais.
2º. Produtos não letais, mas estratégicos, por exemplo combustíveis e veículos.

3º. Demais produtos fornecidos para as Forças, por exemplo alimentos e fardamento. (DUNNE, 1995, p. 402 – tradução nossa)

Masson (2014) destaca que na França os estudos sobre a BID, ou sobre a base tecnológica e industrial de Defesa concentram-se no primeiro grupo proposto por Dunne (1995), porque consideram que:

> - Ele inclui as unidades que permitem, através dos programas de armamento, a autonomia estratégica;
> - Ele é diretamente afetado pelas escolhas dos equipamentos militares;
> - Ele representa o coração das habilidades da indústria de defesa e da pesquisa e desenvolvimento (MASSON, 2014, p. 148)

O autor enfatiza a existência de problemas de identificação e delimitação por parte do setor industrial de armamento francês, por ter dificuldade em distinguir o "caráter militar ou civil de certos materiais" da área eletrônica, e porque as empresas do setor também pertencem a outros setores industriais, e conclui que:

> Logo, a dificuldade em definir a base industrial de defesa tem, como consequência direta, a dificuldade de mensurar o peso desta indústria, ou seja, constituir os agregados e indicadores estatísticos confiáveis e consolidados. Ajunta-se, igualmente, a **dificuldade de acesso a informação em razão da sensibilidade do setor** (caráter estratégico)
> Entretanto, qualquer que seja a definição, certas características do mercado de defesa o diferenciam da maior parte dos outros mercados. Ele possui papel central no Estado (MASSON, 2014, p. 148 - grifo nosso).

Brick (2011) nos apresenta a abordagem da Base Logística de Defesa (BLD) para designar uma visão mais abrangente do conceito de BID empregado pelo MD. Segundo o autor, a BLD "é constituída por uma infraestrutura centrada em uma capacidade educacional, científico-tecnológica e industrial, capaz de gerar inovações e suprir as demandas de recursos de toda ordem para o sistema de defesa". Ele representa a BLD composta por sete componentes distintos e de intensa interação entre eles, apresentados no Quadro 18.

Quadro 18 - Componentes da Base Logística de Defesa

Componentes da Base Logística de Defesa	
1.	Infraestrutura Industrial da Defesa: empresas e organizações envolvidas no desenvolvimento e fabricação de produtos de defesa (a BID propriamente dita).
2.	Infraestrutura Científico-tecnológica da Defesa: universidades, centros de pesquisa e empresas envolvidos na criação de conhecimentos científicos e tecnologias inovadoras com aplicação em produtos de defesa.
3.	Infraestrutura de inteligência da defesa: instituições e pessoas envolvidas na coleta e análise de informações existentes no exterior sobre conhecimentos científicos e inovações tecnológicas com aplicação no desenvolvimento de produtos de defesa e em prospecção tecnológica com impacto em defesa.
4.	Infraestrutura de financiamento da defesa: instituições e recursos financeiros dedicados ao financiamento de pesquisa científica e tecnológica e ao desenvolvimento de produtos inovadores com aplicação em defesa e, também, ao financiamento de vendas externas de produtos de defesa.
5.	Infraestrutura de apoio logístico: para garantir o aprestamento dos sistemas e produtos de defesa durante sua vida útil.
6.	Infraestrutura para o planejamento e a mobilização e os recursos empregados em atividades civis para a defesa.
7.	Arcabouço regulatório da BLD.

Fonte: Brick (2011, p. 7-8).

Os autores Cunha e Amarante (2011, p. 15-16) representaram teoricamente a complexidade da BID nas figuras da "Pirâmide da Defesa" e "Iceberg da BID", para ilustrar e facilitar o entendimento sobre a relação entre as instituições responsáveis pela Defesa Nacional.

A Pirâmide de Defesa, representada na Figura 20, possui quatro blocos distintos:

- Base Nacional – sustenta "toda a estrutura de defesa, provedora dos recursos básicos, tanto humanos como tecnológicos e industriais de base".
- BID Base Científica, Tecnológica, Industrial e Logística - provê o suporte das forças combatentes em termos de conhecimentos, sistemas, equipamentos, materiais, serviços e tecnologia.

- Forças Armadas – representa o braço armado da defesa, que é regido pelas políticas e a estratégias militares; “as hipóteses de emprego, quando da efetiva eclosão de crises e guerras, e o trato dos assuntos relacionados às operações e à logística das operações militares estão aqui representados”.
- Defesa – “refere-se à consciência sobre a necessidade de defesa do Estado, sendo ocupado pelos setores responsáveis pela definição da política e da estratégia nacionais de defesa”.

Figura 20 - Pirâmide de Defesa

Fonte: Cunha e Amarante (2011, p. 16).

Na teoria, a Pirâmide de Defesa deve funcionar harmonicamente e coesa, ou seja, “devem trabalhar em conjunto e harmonia, de forma interdependente, e num ambiente em que as necessidades de cada setor sejam consideradas pelos demais para orientar suas próprias atividades” (CUNHA e AMARANTE, 2011, p. 17).

A outra representação apresentada na Figura 21, é chamada por Cunha e Amarante (2011) de “Iceberg da BID”, e recebeu o nome de “Iceberg Científico de Defesa” no LBDN. A única diferença entre as representações do iceberg está na faixa “Empresa de Engenharia” na qual Cunha e Amarante (2011) destacam a Infraestrutura.

Neste trabalho entendemos mais apropriado o termo “Iceberg da BID” por não restringir o termo somente a parte científica, visto que, a representação considera todas as fases do ciclo de vida do produto.

Figura 21 - Iceberg da Defesa

Fonte: adaptado de Brasil (2012) e Cunha e Amarante (2011, p. 19).

Podemos observar que a faixa “Universidades” representa a base da estrutura, onde “está o setor de geração, de manutenção e de transmissão do conhecimento acumulado por todas as gerações no mundo”. A atividade de “Ensino e Pesquisa” é também exercida pelos Institutos Militares. Acima, temos os “Centros de Pesquisa e Desenvolvimento” para exercer as atividades de “Pesquisa e Desenvolvimento”, ou seja, a pesquisa aplicada e o desenvolvimento experimental, com base nos conhecimentos adquiridos nas universidades.

Sobreposto, estão as “Empresas de Engenharia” que realizam os “Projetos”, e constroem as infraestruturas, utilizando os conhecimentos já disponibilizados para construir a base para o funcionamento das empresas industriais.

Acima, temos as “Empresas Industriais” responsáveis pela “Produção”, ou seja, a fabricam os produtos, sistemas, meios, equipamentos e materiais de defesa. Subindo, temos as “Empresas de Serviços” responsável pela “Logística”, ou seja, cuida da distribuição, da utilização, e da manutenção dos produtos, utilizando o conhecimento tecnológico para garantir o funcionamento dos produtos de defesa.

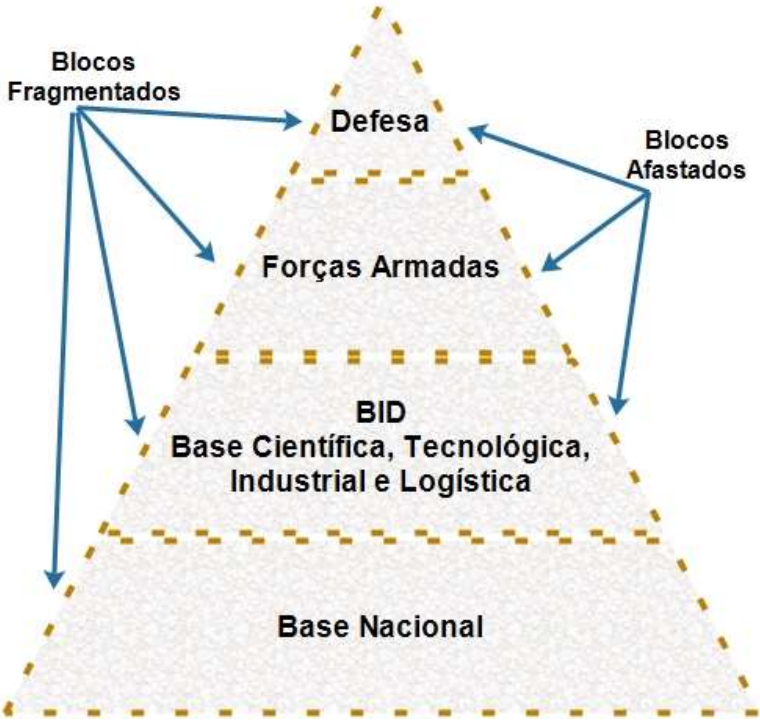
Ainda com relação à figura 21 destacamos a citação de Cunha e Amarante (2011):

> Observando o iceberg, acima da linha d’água está o que é visível para os usuários leigos, isto é, os produtos e serviços tecnológicos disponibilizados para a Defesa. Abaixo da linha d’água está a BID, representada pelas instituições e empresas que a integram. Quanto mais próximo da base estiver a instituição participante, maior o conteúdo científico do seu trabalho. E quanto mais próximo ao usuário, maior o conteúdo tecnológico de suas atividades. (CUNHA e AMARANTE, 2011, p. 20).

No Brasil, nos anos 80 a indústria de defesa desempenhou um importante papel no desenvolvimento brasileiro, depois caiu no “vale da morte” com a redução de encomendas militares, o que levou várias indústrias à falência, aumento do desemprego, estagnação da tecnologia militar, perda de competitividade no mercado, etc.

Conforme Cunha e Amarante (2011) na prática, verifica-se o afastamento e fragmentação dos blocos da Pirâmide de Defesa, como representado na Figura 22.

Figura 22 - Pirâmide de Defesa com Blocos Afastados e Fragmentados



Fonte: Cunha e Amarante, (2011, p. 16).

Ambiciona-se que o Brasil tenha projeções internacionais, mas a realidade é que seus blocos são pouco expressivos quando comparados às necessidades, porque poucas instituições discutem o tema da Defesa Nacional, e o orçamento é descontínuo e insuficiente. O afastamento dos blocos retrata a dificuldade de interação entre eles. A fragmentação dos blocos se deve a "falta de conjunto", as distintas visões sobre Defesa, a independência dos órgãos das FA, e pouco entendimento entre alguns elementos da BID. (CUNHA E AMARANTE, 2011)

As Indústrias de Defesa diferem das demais indústrias ao considerarmos algumas características relacionadas ao produto, tecnologias, atividades funcionais, continuidade, competência, comercialização e mobilização industrial. Por exemplo, os produtos não podem apresentar falhas, seu desenvolvimento, normalmente, é realizado

em longos ciclos, sob demanda e com custo pago pelo cliente, e exige conhecimentos multidisciplinares e especialistas. É um desafio e necessidade conquistar autonomia tecnológica nos setores estratégicos da END (espacial, cibernético e nuclear); para realizar as atividades funcionais são necessários materiais e serviços modernos e uma formação técnica especializada; e a descontinuidade dos programas de defesa desencadeia uma série de prejuízos para as indústrias. (CUNHA E AMARANTE, 2011)

Nos últimos anos, observamos a publicação de estratégias, políticas, e normativos legais voltados à reestruturação do setor e à revitalização da BID, que compreende um conjunto de empresas estatais e privadas que participam de uma ou mais das etapas do ciclo de vida dos produtos de defesa.

O MD atua como promotor das condições necessárias para: alavancar a BID, capacitar a conquista da autonomia em tecnologias estratégicas para o Brasil, e instituir o marco regulatório para o setor. Para isso, conta com o PAED e a Lei nº 12.598/2012 (Lei de fomento à BID).

O PAED atua como um instrumento do Estado para "garantir o fornecimento dos meios que as FA necessitam, bem como a infraestrutura que irá provê-los", e para planejar e executar as compras relacionadas aos projetos estratégicos de defesa.

A Lei de fomento à BID "é um desdobramento do Plano Brasil Maior, criado para aumentar a competitividade da indústria nacional, a partir do incentivo à inovação tecnológica", além de instituir um regime especial de tributação (o RETID), diminuir o custo de produção de companhias legalmente classificadas como estratégicas, e estabelecer incentivos ao desenvolvimento de tecnologias indispensáveis ao Brasil.

A BID atua como geradora e difusora de novas tecnologias e está ligada à excelência tecnológica, e encontra essa natureza conforme citação:

> A BITD é importante geradora e difusora de novas tecnologias dentro da estrutura produtiva de uma nação. A indústria de defesa está intimamente ligada à excelência tecnológica. Ao atender à demanda do setor militar por equipamentos cada vez mais sofisticados, é importante fonte de inovação. Grande parte das inovações apresenta uso dual. [...]
> A busca da vantagem estratégica ou tática, pela superioridade tecnológica, gera um esforço científico e técnico constante, que, pelas leis do

> mercado, dificilmente ocorreria. A P&D militar foge do constrangimento da rentabilidade de curto prazo, abrindo novos domínios, sem obrigações com resultados. Com efeito, as necessidades de defesa permitem financiar P&D que as firmas não poderiam realizar, em função do custo e do longo prazo de maturação. (MELO, 2015, p. 44-45)

A razão de ser da BID é atuar no preparo do Poder Nacional para defesa do país. O seu fortalecimento e reestruturação visam a nacionalização tecnológica de Defesa, bem como minimizar dependência tecnológica internacional. Caso seja necessário adquirir tecnologia externa, deve ser utilizada a cláusula de compensação comercial, industrial e tecnológica (*off-set)* (contrapartidas). Neste contexto, destaca-se a citação do LBDN:

> No tocante ao mercado interno, a BID tem conseguido atender de forma crescente às demandas das Forças Armadas brasileiras, o que tem mantido as importações desse tipo de produto em níveis reduzidos.
> A recuperação e o fortalecimento da Base Industrial de Defesa são metas delineadas na Estratégia Nacional de Defesa. Além da finalidade de prover artigos e sistemas necessários às Forças Armadas, funcionará como indutora de inovações tecnológicas com aplicações civis, dado o caráter dual dos desenvolvimentos. (BRASIL, 2012c, p. 215)

6.2 PROJETOS ESTRATÉGICOS DE INTERESSES DA BID

6.2.1 Administração Central do Ministério da Defesa

Conforme consta no PAED a Administração Central do MD gerencia diretamente seis projetos, sendo quatro no Estado-Maior Conjunto das Forças Armadas e dois no Centro Gestor e Operacional do Sistema de Proteção da Amazônia (BRASIL, 2012c). São eles:

> – Sistema de Comunicações Militares por Satélite (SISCOMIS);
> – Sistema de Comunicações Militares Seguras (SISTED);

> – Desenvolvimento do Sistema de Logística e Mobilização de Defesa (SISLOGD);
> – Modernização da Defesa Antiaérea das Estruturas Estratégicas;
> – Modernização do Sistema de Proteção da Amazônia; e
> – Cartografia da Amazônia. (BRASIL, 2012c, p.207)

6.2.2 Marinha

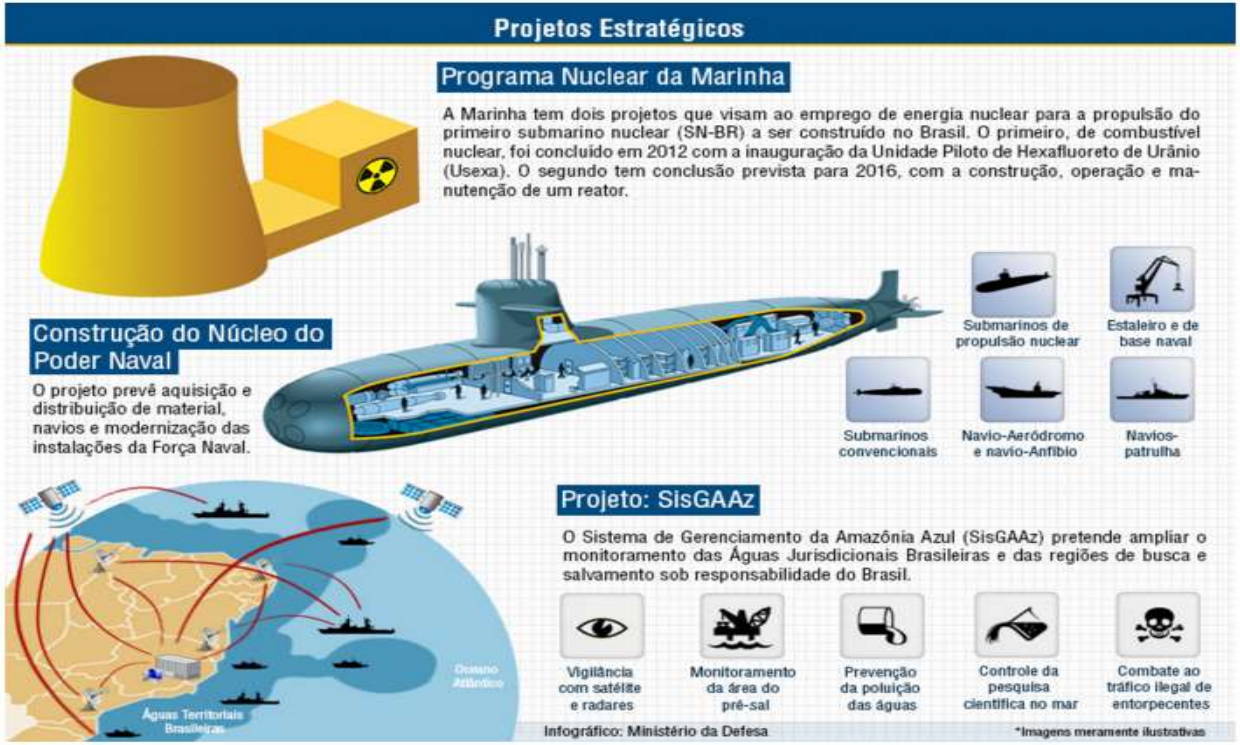
Dentre as atribuições da Marinha destacamos o preparo e emprego do Poder Naval, a fim de contribuir para a defesa da Pátria.

Conforme consta no PAED a Marinha possui 10 projetos prioritários dentre os quais citamos os três projetos considerados estratégicos:

- O Programa Nuclear – visa obter capacidade tecnológica para o projeto, construção, operação e manutenção de reator nuclear do tipo PWR *(Pressurized Water Reactor*) que será empregado na propulsão do primeiro Submarino Nuclear (SN-BR), atualmente em construção.
- A construção do núcleo do poder naval - se propõe a ampliar e modernizar a capacidade operacional da Marinha.
- O Sistema de Gerenciamento da Amazônia Azul (SisGAAz) – visa ampliar a capacidade de monitoramento e controle das águas jurisdicionais e das regiões de busca e salvamento sob responsabilidade do Brasil. (BRASIL, 2015c)

O infográfico apresentado na Figura 23 resume os projetos estratégicos da MB.

Figura 23 – Projetos Estratégicos de Defesa – Marinha do Brasil



Fonte: Brasil, 2015c.

6.2.3 Exército

É missão do Exército, entre outras, contribuir para a garantia da soberania nacional, dos poderes constitucionais, da lei e da ordem, salvaguardando os interesses nacionais e cooperando com o desenvolvimento nacional e o bem-estar social.

Conforme consta no PAED o Exército possui 14 projetos prioritários dentre os quais citamos os três projetos considerados estratégicos:

- O Sistema Integrado de Monitoramento de Fronteiras (Sisfron) – busca fortalecer as ações do Exército para reduzir as vulnerabilidades na região fronteiriça.
- O projeto Guarani - institui uma nova família de veículos blindados sobre rodas.
- Projeto Proteger – Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres. (BRASIL, 2015c)

A Figura 24 apresenta o infográfico dos projetos citados.

Figura 24 - Projetos Estratégicos de Defesa: Exército Brasileiro

Fonte: Brasil, 2015c.

6.2.4 Aeronáutica

A síntese da missão da Aeronáutica é “manter a soberania do espaço aéreo nacional com vistas à defesa da pátria".

Conforme consta no PAED a Aeronáutica possui 9 projetos prioritários dentre os quais citamos os três projetos considerados estratégicos:

- O Projeto KC-390 (cargueiro militar) - construção de uma aeronave de transporte militar e reabastecimento em voo, capaz de operar em pistas com pouco preparo.
- O Projeto AM-X - modernizar as aeronaves AM-X (avião de ataque ar-superfície usado nas missões de interdição, apoio aéreo e reconhecimento.
- O Projeto VANT-FAB – sistema completo de Veículos Aéreos Não Tripulados (Vants). (BRASIL, 2015c)

A Figura 25 ilustra os principais projetos da FAB.

Figura 25 – Projeto Estratégico de Defesa – Força Aérea Brasileira (FAB)

Fonte: Brasil, 2015c.

6.3 DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO AOS PRODUTOS DE DEFESA

No ambiente de Defesa, a Inovação se dá ao introduzir uma "novidade ou aperfeiçoamento no ambiente produtivo de PRODE", já o Desenvolvimento é definido como a "concepção ou projeto de novo PRODE ou seu aperfeiçoamento, incluindo, quando for o caso, produção de protótipo ou lote piloto" (BRASIL, 2012a).

O Ambiente de Inovação para a produção de PRODE pode ser visto sob o viés de Sistemas de Produtos Complexos (*Complex Product Systems* - CoPS). Para Davies e Hobday (2005, p.16 – tradução nossa), CoPS pode ser compreendido além de "conceitos e modelos convencionais, tais como descontinuidades tecnológicas e abordagens do ciclo de vida do produto". Por isso, identificamos os ciclo de vida dos PRODE de cada FA, porém não nos limitamos a eles para compreender este ambiente de inovação.

O PRODE são bens, produtos e serviços que envolvem alta tecnologia, alto custo, e capacitação específica. Porém, projetar e gerir tal sistema não requer somente as considerações sobre a complexidade da produção, são necessários outros instrumentos de gestão, como: a Gestão da Integração, a Gestão do relacionamento interinstitucional; e a Gestão da Inovação, como afirmam Freitas e Oliveira (2008):

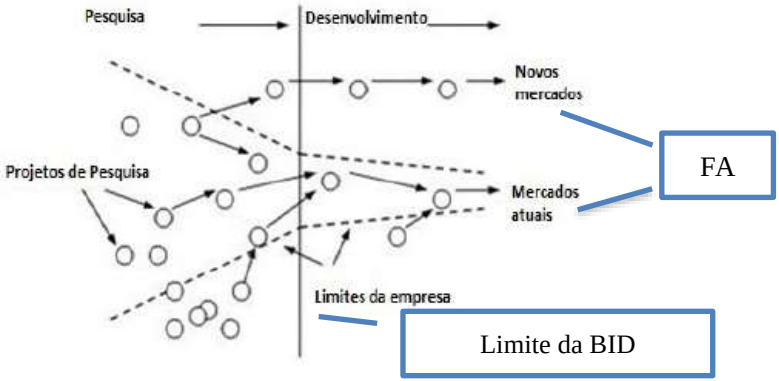
> A complexidade técnica dos produtos obtidos através destes arranjos - baseados na compatibilização de diferentes subsistemas e da estrutura de hardware e software - requer a integração de conhecimentos e competências extremamente diferenciados (HOBDAY, 2000; NIGHTINGALE, 2000; DAVIES & BRADY, 2000; GANN & SALER, 2000), o que pode ser considerado como uma atividade de Gestão da Integração. [...]
>
> A Gestão de CoPS extrapola a questão da complexidade do produto em si e passa a ser considerada também a complexidade das relações entre os atores participantes do processo. Deve ser lembrado ainda que, as relações de troca de informações entre atores endógenos, exógenos e institucionais visando o desenvolvimento do produto ou sistema, não se dá somente no âmbito do produto, mas também no âmbito do processo de

> produção, do desenvolvimento técnico e da própria administração. [...]
> A gestão da inovação é outro aspecto relevante em sistemas complexos. Autores como DAVIES (1998) sugerem que os CoPS possuem duas fases distintas quando analisado o processo de inovação. Na primeira, é priorizado o desenvolvimento de novos modelos de arquitetura. Nesta fase, a arquitetura do design é influenciada de maneira significativa pela rede de fornecedores. A segunda se relaciona à fase de geração de novos produtos e serviços, na qual a quantidade de inovação aumenta e ocorre a introdução sucessiva de novos produtos, serviços e componentes sem alterar fundamentalmente a arquitetura de design já estabelecida. (FREITAS e OLIVEIRA, 2008, p. 17-19)

Nesta pesquisa, adotamos o entendimento de que o ambiente de inovação da BID é um Ambiente de Inovação fechada, onde o ciclo de produção de PRODE, as pesquisas e a gestão do conhecimento precisam permanecer em sigilo e protegidos do conhecimento público, por serem de interesse de Defesa.

Assim, como apresentado na Figura 26 os projetos são desenvolvidos dentro dos limites da BID, sem interferência externa, até a entrega a Força que demandou o PRODE.

Figura 26 – Modelo de Inovação Fechada



Fonte: Chesbrough (2012) - Adaptado pela autora, 2015.

No ambiente de inovação proposto por Pimentel (2010c), apresentado na Figura 27, observa-se os seguintes componentes de um ambiente de inovação:

- Os agentes que são as partes interessadas tais como ICTs, fundação de apoio, o governo e órgãos de fomento.
- O problema a ser solucionado que pode ser qualificado através da descrição dos seus requisitos.
- A gestão compreendendo a alocação de recursos humanos e materiais.
- A formalização do projeto de pesquisa, de contratos com o demandante e com os recursos humanos contratados.
- As etapas de Pesquisa e Desenvolvimento (P&D) as quais efetivamente inovam ou criam o produto ou serviço solicitado.
- Proteção – sob este ponto de vista o modelo considera que a disponibilização do processo, produto ou serviço para o mercado seja com ou sem a proteção da propriedade intelectual. Caso o resultado da escolha seja proteger o processo, produto ou serviço poderá ser utilizado um dos seguintes instrumentos: patente, registro, certificado ou segredo.

Pimentel (2010a) esclarece que a caracterização da parceria de PD&I deve ser formalizada por contratos e acordos, além de estabelecer os termos de locação de bens tangíveis e intangíveis e seus contratos, conforme as citações:

> Recursos humanos e seus conhecimentos, inclusive a propriedade intelectual já existente – o capital intelectual (bens intangíveis); Recursos financeiros (outro bem intangível); Recursos materiais, como o laboratório, os equipamentos, os instrumentos e instalações necessárias para o serviço de P&D, seus testes e ensaios (bens tangíveis). (PIMENTEL, 2010a, p. 377)
>
> Acordo de parceria de PD&I; Contratos de prestação de serviços; Contrato de transferência de tecnologia (saber fazer); Contrato de licenciamento; Contrato de permissão de utilização de equipamentos, instrumentos, materiais, laboratórios e outras instalações; Contratos de compartilhamento de equipamentos, instrumentos,

> materiais, laboratórios e outras instalações; Contrato de cessão. (PIMENTEL, 2010a, p. 372)

O modelo considera também as possibilidades de inovação incremental e radical para o processo, produto ou serviço. Adicionalmente o modelo de Pimentel, apresentado na Figura 27, contempla a logística para o lançamento do invento no mercado.

Figura 27 - Ambiente de Inovação proposto por Pimentel (2010a)

Fonte: Pimentel (2010a).

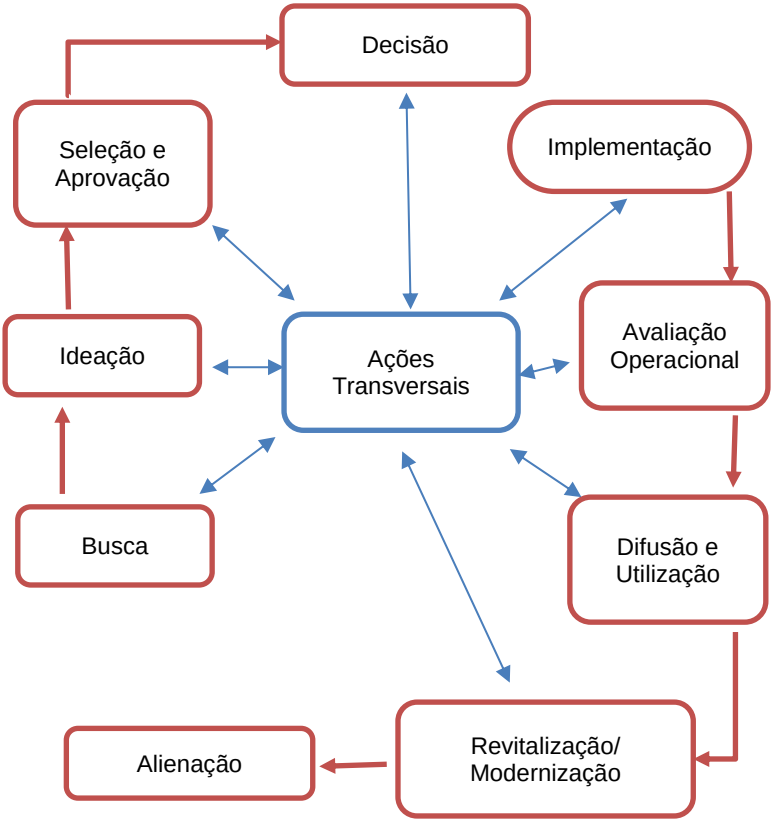
Deste modo, ao identificar os diversos agentes, Pimentel (2010a) ressalta a complexidade das relações entre os participantes do processo, cujas relações requerem a integração das diversas instituições, seus atores e recursos, de maneira harmônica e dinâmica, com a intensa troca de informação entre eles.

O instrumento de proteção é destacado em dois momentos: na fase do projeto quando se realiza o contrato e se estabelece a cláusula de confidencialidade; e no final do processo de Inovação, quando se decide

sobre a forma de proteção (patente, registro, certificado ou segredo) a ser adotada para o produto antes que entre no mercado.

Franco-Azevedo (2013) propôs um Modelo para Gestão das Inovações em Defesa, considerando as inovações tecnológicas e as não tecnológicas. Como esta tese trata das inovações tecnológicas, e não as doutrinárias, representamos na Figura 28 nossa leitura para as inovações tecnológicas no modelo proposto por Franco-Azevedo (2013):

Figura 28 - Gestão das Inovações em Defesa



Fonte: Franco-Azevedo (2013) - adaptado pela autora, 2015.

Neste contexto, a seguir, descrevemos o modelo de Franco-Azevedo (2013, p. 335-346):

- O modelo inicia com a fase de **Busca** pela inovação, provocada pela Prospecção Tecnológica ou pela Demanda das Forças. Quando provocada pela Prospecção Tecnológica, envolve as seguintes atividades: a) perceber os sinais dos ambientes interno (Núcleo de Inovação Tecnológica -NIT das FA) e externo (ICTs e Instituição de Ensino superior - IES); b) levantar as oportunidades tecnológicas (Parques Tecnológicos) e mercadológicas (núcleos de defesa da FIESP, FIRJAN e FINEP) junto a outros agentes (BID, Comércio Exterior, MRE e outros); c) analisar o banco de patentes do INPI e emitir o Relatório de Análise de Patentes (RAP) que constará do Relatório de Prospecção Tecnológica (REPROTEC); e d) prever que as atividades desta fase sejam coordenadas pela SEPROD/MD. Quando for por Demanda das Forças, significa as demandas advindas das atividades que aconteceram da observação sobre a obsolescência do PRODE ou das lições aprendidas nos exercícios e operações militares.
- A fase de **Ideação** representa a consolidação de todas as oportunidades para inovar, vindas do meio militar ou civil, formalizada no Relatório de Inovações Desejáveis (RID).
- A fase de **Seleção e Aprovação** contempla as atividades de estudo de viabilidade técnico-econômica, estudo de alternativas e alinhamento político-estratégico, para auxiliar no processo decisório.
- A fase de **Decisão** envolve a participação do nível político, ficando a cargo dos tomadores de decisão (Comandantes das Forças, Ministro da Defesa e Presidente da República) a opção por desenvolver uma tecnologia nacional, *off-set* ou comprar no exterior.
- A fase de **Implementação** envolve as medidas para a consecução dos projetos, por isso ocorre no nível estratégico-operacional. Envolve as atividades de P&D, capacitação, aquisição no exterior e/ou no país e infraestrutura. Aqui são estabelecidas as alianças para PD&I de produtos não sensíveis, ou acordos de cooperação para o desenvolvimento de parte do projeto de produto sensível. Ela finaliza com a apresentação de um protótipo ou lote-piloto.
- Na fase **Avaliação Operacional** é aferida a real capacidade do PRODE, sob a responsabilidade de execução das FA e coordenação do MD.
- A Fase **Difusão e Utilização** temos a atividade de fabricação em larga escala do PRODE e do emprego do PRODE, onde são avaliadas a necessidade de revitalização, modernização, melhora e desativação do PRODE.

- Na fase de **Revitalização / Modernização** são executadas modificações no PRODE devido à perda ou degradação de sua eficiência durante o uso, ou obsolescência e desatualização tecnológica.
- A última fase Alienação compreende as ações de planejamento e execução da retirada do PRODE com sua alienação ou inutilização, finalizando o ciclo de vida do produto. (FRANCO-AZEVEDO, 2013, p. 335-346).

As atividades transversais representam os estudos de viabilidade técnica e de alternativas; concepção preliminar do PRODE; elaboração e melhoria de requisitos de PRODE; estabelecimento de parcerias; proteção da propriedade intelectual; a capacitação de pessoal; a modernização organizacional; o acompanhamento do cronograma físico-financeiro; a fiscalização de contratos e outras tantas atividades (FRANCO-AZEVEDO, 2013).

Observamos que este Modelo considerou somente um instrumento de proteção – a Propriedade Intelectual – como uma das ações transversais.

Adotamos a definição de Brasil (2010a) para ciclo de vida como sendo:

> "Conjunto de procedimentos que vai desde a detecção da necessidade operacional, seu pleno atendimento por intermédio de um Sistema ou de um Material, a confrontação deste com os requisitos estabelecidos, o seu emprego, a avaliação operacional, a sua oportuna modernização ou revitalização até a sua desativação (BRASIL, 2010a, p. 10).

Assim, o entendimento sobre o ambiente de inovação da BID se faz não só a partir da contextualização dos ambientes envolvidos e das relações de seus principais atores e o ciclo de vida do PRODE em cada FA, mas também do ambiente de inovação proposto por Pimentel (2010c) e do Modelo para Gestão das Inovações em Defesa proposto por Franco-Azevedo (2013).

A seguir apresentamos os Ambientes de Inovação adotados pelo MD, Marinha, Exército, Aeronáutica e do ciclo de vida de PRODE em cada FA.

6.3.1 Ciência, Tecnologia e Inovação no Ministério da Defesa

Em 2002, fruto de trabalho conjunto que envolveu representantes do MD, Ministério da Ciência Tecnologia e Inovação (MCTI), Ministério do Desenvolvimento, Indústria e Comércio Exterior (MDIC), da academia e da indústria, o MD concebeu o Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa (SisCTID), que contempla as suas áreas e programas estratégicos. O SisCTID tem a missão de "viabilizar soluções científico-tecnológicas e inovações, para a satisfação das necessidades do país atinentes à Defesa Nacional e ao desenvolvimento nacional". A visão do sistema, para 2015, descrita no Quadro 19 era composta por quatro temas e vários objetivos estratégicos. (BRASIL, 2003, p. 18).

Quadro 19 – Visão 2015 do Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa

TEMA 1 – Domínio de tecnologias que atendam às necessidades da Defesa Nacional. 1. Ampliação do conteúdo tecnológico dos produtos e serviços de Defesa. 2. Elevação do nível de capacitação de recursos humanos. 3. Aprimoramento da infraestrutura de C&T de apoio a programas e projetos de interesse da Defesa Nacional.
TEMA 2 – Contribuição para o fortalecimento da indústria nacional 1. Criação de um ambiente favorável à inovação e à competitividade industrial. 2. Implantação de mecanismos de financiamento das atividades de C,T&I de interesse da Defesa Nacional.
TEMA 3 – Reconhecimento institucional, no Brasil e no exterior. 1. Ampliação do interesse dos diversos segmentos da sociedade pelas iniciativas nas áreas da C,T&I voltadas para a Defesa Nacional. 2. Aprimoramento da imagem de excelência institucional.

Continuação do Quadro 19

TEMA 4 – Gestão eficiente e eficaz
1. Integração das iniciativas de C.T&I de interesse de Defesa Nacional, conduzidas nas organizações militares de P&D, nos institutos, nas universidades civis e na indústria. 2. Estabelecimento de política para a valorização de recursos humanos, baseada em resultados. 3. Implantação de sistemática que integre o planejamento estratégico, o ciclo de desenvolvimento de produtos e serviços de Defesa e a avaliação de resultados.

Fonte: Brasil (2003, p. 18).

Para possuir as características de um sistema integrador, inovador e seguro, conceberam o SisCTID para operar em dois modos de acesso (BRASIL, 2003, p. 28):

> Controlado: onde se realizam o planejamento, a execução e o controle das ações, contém os projetos estratégicos e as informações sigilosas, por isso segue a conformidade da legislação sobre salvaguarda de assuntos sigilosos.
> Livre: funciona como uma rede de cooperação com múltiplas entradas de informações, para fomentar a inovação tecnológica e as parcerias vinculadas. (BRASIL, 2003, p. 28):

O SisCTID opera no nível estratégico, construindo indicadores de acompanhamento, uma base de dados para a GC e um modulo de Gestão estratégica., como apresentado na Figura 29.

Figura 29 – Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa

Fonte: Brasil (2003, p. 31).

A gestão do SisCTID é avaliada e otimizada pela Comissão Assessora de Ciência e Tecnologia para a Defesa (COMASSE), que atua por meio de sua Secretaria-Executiva, que segue a proposta de Fleisch & Österle (2002) prevendo as funções de gestão para cinco áreas de coordenação, são elas (BRASIL, 2003, p. 29-30):

- Gestão da Cadeia Produtiva: tem por objetivo conduzir o planejamento operacional e a execução dos processos, de forma eficiente.
- Gestão de Relacionamentos: tem por objetivo conquistar clientes e/ou fornecedores e ganhar lealdades.
- Inovação: tem por objetivo a criação rápida de novos produtos.
- Infraestrutura: trata das atividades de apoio.
- Desenvolvimento Organizacional: incentiva os colaboradores e os parceiros da cooperação. (BRASIL, 2003, p. 29-30):

Deste modo, a SisCTID prevê a consolidação e padronização de dados e informações sobre os assuntos CT&I das FA. Cabe destacar que o sistema não apresenta seu contato com os sistemas de C&T de cada FA.

Em Brasil (2003a) encontramos o detalhamento do Ciclo de vida dos produtos para o MD, que teve por guia a análise do Ciclo de Vida de Material de Emprego Militar do Exército, e do Ciclo de Vida de Sistemas e Materiais da Aeronáutica.

Brustolin (2014, p.8-9) ao comparar as práticas de inovação nos ambientes de defesa dos Estados Unidos da América (EUA) e do Brasil, apresenta uma importante diferenciação dos termos "modelo" e "sistemática".

O autor afirma que os EUA possuem um "modelo" de inovação de Defesa, onde "prioriza-se a utilização da infraestrutura própria na geração da ciência e tecnologia" e "interliga governo/militares as indústrias e academias". No caso do Brasil, existe uma infraestrutura de base, que não representa um modelo e sim uma sistemática, representada por uma série de práticas e de procedimentos para adquirir e gerar tecnologia de Defesa. A falta de um modelo "faz com que as interligações entre os agentes – governo/militares, indústrias e academias – fiquem aquém do seu potencial. Deixa-se assim, de aproveitar e desenvolver os recursos que o País dispõe, ao mesmo tempo em que este se torna dependente de soluções estrangeiras".

As próximas seções apresentam o Sistema de C&T de cada FA.

6.3.2 Ciência, Tecnologia e Inovação no âmbito da Marinha

O Sistema de Ciência, Tecnologia e Inovação da Marinha (SCTMB) possui um órgão central de gestão que é a Secretaria de Ciência, Tecnologia e Inovação da Marinha (SecCTM), que exerce o planejamento, a orientação, a coordenação e o controle das atividades científicas, tecnológicas e de inovação da Marinha.

Em 2004, cumprindo a Lei 10.973/2004[13], a Marinha criou o Núcleo de Inovação Tecnológica (NIT-MB) que tem a finalidade de gerir a política de inovação e é constituído por um Gerência de Inovação Tecnológica (GIT) e por Células de Inovação Tecnológicas (CIT) sediadas nas ICTs da Marinha.

As inovações tecnológicas na Marinha são originadas em uma Célula de Inovação Tecnológica (CIT) do Poder Naval. O modelo de

[13] Recentemente alterada pela Lei 13.243/2016.

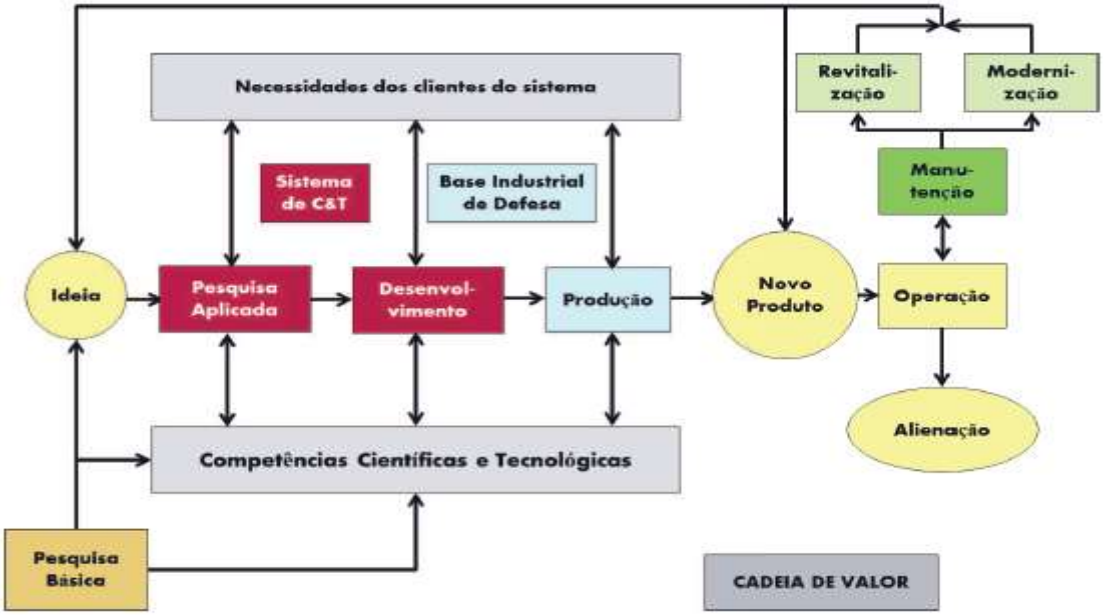
gestão destas inovações se dá por meio do Ciclo de Vida dos Materiais da Marinha, denominado por aquela Força de “Cadeia de Valor” apresentada na Figura 30. Pode-se dizer que, salvo algumas peculiaridades, o modelo é bem semelhante ao do MD e ao do Exército que será apresentado a seguir.

O Plano de Desenvolvimento Científico-Tecnológico e de Inovação da Marinha (PDCTM) está detalhado na publicação EMA 410. (BRASIL, 2009).

A Figura 30 descreve a produção científica, tecnológica e Industrial da Marinha como:

> (...) arranjos institucionais, considerando as competências científicas e tecnológicas (capacitação de pessoal e infraestrutura técnico-administrativa), bem como as necessidades dos clientes do sistema, que se articulam formando um processo cíclico referente à geração, à implementação e à difusão de funções, nos quais o valor é agregado a produtos e serviços, em prol da ciência, da tecnologia e da produção industrial decorrente. (BRASIL, 2009)

Figura 30 - Ciclo de Vida da Produção Científica, Tecnológica e Industrial da Marinha “Cadeia de Valor”



Fonte: Brasil (2009).

As fases do ciclo de vida dos produtos da Marinha foram retiradas da Figura 30, são elas: a) Fase 1 é composta pelas atividades de Pesquisa Básica, ideia e Pesquisa Aplicada; b) Fase 2 é comporta a atividade de desenvolvimento; c) Fase 3 compreende as atividades de Produção e Novo Produto; d) Fase 4 compreende as atividades de Operação, Manutenção, Revitalização e Modernização; e e) Fase 5 comporta a atividade de Alienação.

6.3.3 Ciência, Tecnologia e Inovação no âmbito do Exército

O Exército possui o Sistema de Ciência e Tecnologia (SCTEx) desde 1994, com a finalidade de planejar, orientar, coordenar, controlar e executar, no âmbito do Exército, as atividades científicas e tecnológicas relacionadas com o Material de Emprego Militar (MEM)[14] e suas influências nas áreas da Doutrina Militar Terrestre, da Logística e do Pessoal.

Encontra-se em curso a transformação do Sistema de Ciência e Tecnologia para o Sistema de Ciência Tecnologia e Inovação do Exército (SCTIEx).

O Núcleo de Inovação Tecnológica (NIT) encontra-se subordinado ao Departamento de Ciência e Tecnologia do Exército (DCT) que é o órgão central do SCTEx, a quem cabe elaborar o Plano Básico de Ciência e Tecnologia (PBCT), que é parte componente do Sistema de Planejamento do Exército (SIPLEx) (FRANCO-AZEVEDO, 2013, p. 95).

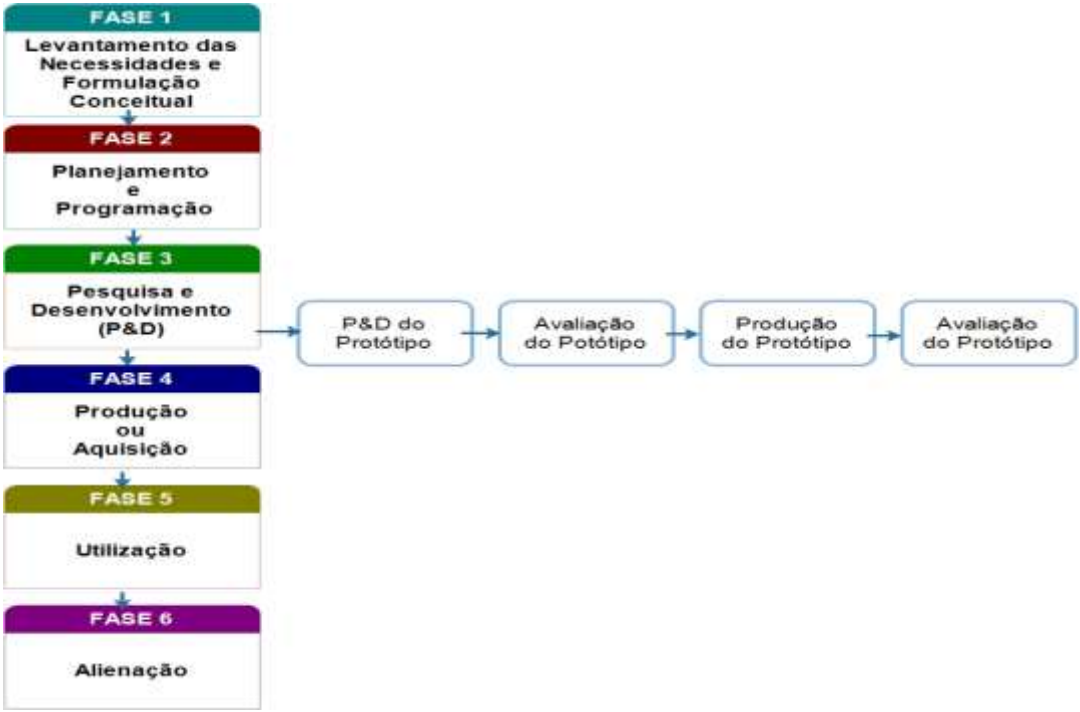
O Modelo do Ciclo de Vida dos Materiais de Emprego Militar tem a finalidade de ordenar e descrever as principais atividades e eventos que ocorrem durante o seu ciclo, e também define os órgãos do Exército responsáveis pela sua execução.

A Figura 31 representa o Ciclo de Vida do MEM, composto por seis fases que são executadas pelas diferentes organizações do SCTEx.

---

[14] Para esclarecimento, o Exército utiliza o termo Material de Emprego Militar (MEM) para se referir ao termo Produto de Defesa (PRODE) utilizado nas publicações atuais.

Figura 31 - – Ciclo de Vida do Material de Emprego Militar do Exército



Fonte: Elaboração da autora, baseado em CARRILHO (2014, p. 17-18).

As Fases são descritas por FRANCO-AZEVEDO (2013, p. 98), como:

a) Na Fase 1 - Levantamento das Necessidades e Formulação Conceitual, são identificadas as demandas do Exército, e elaborados documentos como: os Condicionantes Doutrinários Operacionais (CONDOP), os Requisitos Operacionais Básicos (ROB), os Requisitos Técnicos Básicos (RTB), e o Estudo de Viabilidade Técnico-econômica (EVTE).
b) Na Fase 2 - Planejamento e Programação, o MEM que necessita ser pesquisado, desenvolvido, modernizado, aperfeiçoado, nacionalizado ou adquirido é incluído no processo, para que o SIPLEx determine as prioridades de atendimento.
c) Na Fase 3 – Pesquisa e Desenvolvimento (P&D), são desenvolvidos um protótipo e um lote-piloto, com as características especificadas no ROB e RTB.
d) Na Fase 4 - Produção e Aquisição, o MEM é obtido, atendendo a quantidade e qualidade planejadas, e outras atividades são iniciadas, como: “manutenção, suprimento, instrução, quadros de organização, manual de campanha e manuais técnicos, concretizando a meta de que o MEM, ao ser entregue à tropa, o seja em condições de perfeita utilização e manutenção”.
e) Na Fase 5 - Utilização, o MEM passa a ser utilizado e possíveis deficiências são levantadas, o que significa uma futura revitalização, modernização ou melhoria.
f) A Fase 6 - Alienação, trata da desativação ou retirada do MEM de uso, significando o fim do ciclo do material (FRANCO-AZEVEDO, 2013, p. 98).

6.3.4 Ciência, Tecnologia e Inovação no âmbito da Aeronáutica

A Aeronáutica possui o Departamento de Ciência e Tecnologia Aeroespacial (DCTA) que tem as atribuições de planejar, gerenciar, realizar e controlar as atividades relacionadas com ciência, tecnologia e inovação, sendo, portanto, o gestor do Sistema de Ciência e Tecnologia da Aeronáutica (SCTA). (BRASIL, 2009).

Subordinados ao DCTA encontram-se os órgãos responsáveis pela pesquisa e desenvolvimento que são o Instituto de Aeronáutica e Espaço

(IAE), o Instituto de Estudos Avançados da Aeronáutica (IEAv), e o Instituto de Pesquisas e Ensaios em Voo (IPEV).

O NIT tem como missão principal “contribuir para o surgimento de inovações tecnológicas, por meio da Proteção da Propriedade Intelectual e da Transferência de Tecnologias geradas no COMAER”. Para isso:

- Busca fomentos e linhas de crédito para o desenvolvimento de invenções e descobertas oriundas das pesquisas realizadas nos institutos do DCTA, ocorrendo desta forma a proteção e o licenciamento da Propriedade Intelectual.
- Promove o desenvolvimento tecnológico da indústria aeroespacial brasileira por meio da proteção e do licenciamento da Propriedade Intelectual nacional.
- Apoia o processo de inovação tecnológica para o setor aeroespacial por meio da proteção e do licenciamento da Propriedade Intelectual oriunda do DCTA.

De modo similar ao do Exército, o modelo do ciclo de vida de sistemas e materiais empregados na Aeronáutica também é baseado nos fundamentos da Engenharia de Sistemas apresentados por Blanchard (1998), e é composto pelas fases: concepção; viabilidade; definição; desenvolvimento ou aquisição e produção (FRANCO-AZEVEDO, 2013), como apresentado na Figura 32.

Figura 32 – Ciclo de Vida de Sistemas e Materiais da Aeronáutica

Fonte: Elaboração da autora, 2015, baseado em Brasil (2010).

A seguir, as Fases são descritas de acordo com BRASIL (2010, p. 16-18):

a) Na Fase 1 – Concepção, é identificada a carência operacional ou oportunidade tecnológica / econômica para o sistema ou material.
b) Na Fase 2 – Viabilidade, com a colaboração dos órgãos intervenientes a viabilidade é verificada considerando a análise das capacidades, as alternativas, a avaliação dos riscos, dos prazos e do custo/benefício. Elabora-se o *Request for Information* (RFI) que é o primeiro contato formal com

empresas ou governos interessados. Também é realizado o planejamento sintético do ciclo de vida.

c) Na Fase 3 – Definição, elaboram-se o plano do projeto e o detalhamento das especificações e requisitos técnicos, logísticos e industriais (RTLI) do sistema ou material. Também são definidas condições como custo, qualidade e prazo. São selecionadas empresa(s) ou entidade(s) governamental(is) para o desenvolvimento (ou para a compra, no caso de produto já desenvolvido) e são elaboradas minutas de contratos.
d) Na Fase 4 – Desenvolvimento/Aquisição, em se tratando de desenvolvimento são elaborados e executados os planos de desenvolvimento, de nacionalização e transferência de tecnologia, de compensação comercial, de verificação, ensaios e certificação. No caso de aquisição são elaborados planos de nacionalização e de Compensação Comercial. São realizados testes e procedimentos para a homologação e certificação/aceitação do sistema ou material.
e) Na Fase 5 – Produção, quando se tratar de aquisição, no país ou exterior, esta fase tem início tão logo o sistema ou produto seja adquirido e os passos aplicáveis das fases de Definição e Desenvolvimento sejam realizados.
f) Na Fase 6 – Implantação, cumprem-se as atividades de preparo das organizações para o recebimento do sistema ou material, o cadastramento do sistema ou material, a distribuição, a ativação, o emprego operacional e inicia-se o suporte logístico contínuo.
g) Na Fase 7 – Utilização, desenvolvem-se as atividades de operação do sistema ou material, controle da garantia da qualidade, avaliação de desempenho operacional, relocação, padronização da operação, análise da expectativa de vida, manutenção e necessidade de revitalização ou modernização.
h) Na Fase 8 – Revitalização ou Modernização, ocorre o restabelecimento, incremento ou modificação das capacidades do sistema ou material.
i) Na Fase 9 – Desativação, realiza-se o planejamento e a execução da desativação do material ou serviço e sua posterior alienação ou inutilização encerrando o ciclo de vida. (BRASIL, 2010, p. 16-18).

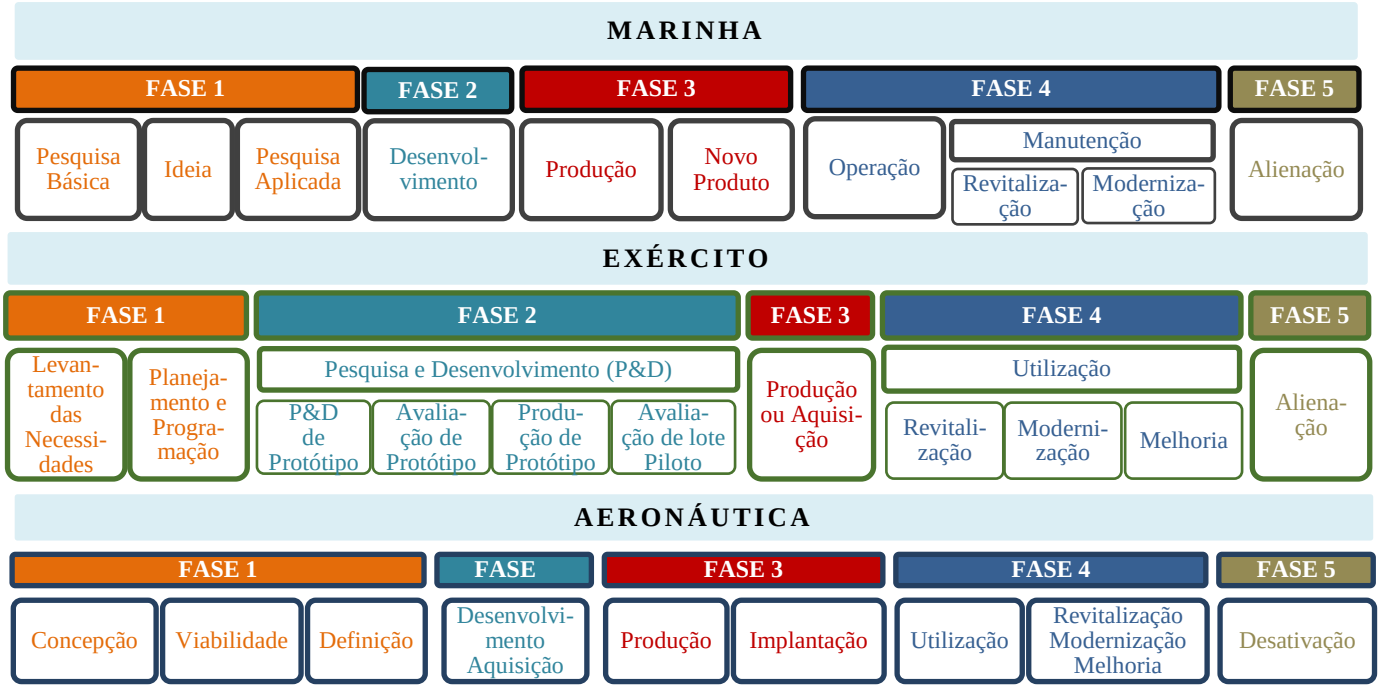
6.4 CONCLUSÃO DO CAPÍTULO

Esta seção conclui o capítulo apresentando o Modelo de Produção para o Ambiente de Inovação da BID, a partir do entendimento da atuação dos agentes de inovação e dos ciclos de vida dos produtos de Defesa de cada FA.

Realizamos uma análise dos ciclos de vida dos PRODE das FA para identificar as fases e a possibilidade de agrupamento de funções semelhantes, bem como ter uma visão ampla do processo produtivo dos PRODE das FA, o resultado está apresentado na Figura 33.

A análise dos ciclos de vida dos PRODE no âmbito das FA permitiu identificar fases que agrupam funções semelhantes, e ter uma visão consolidada do processo produtivo, como apresentado na Figura 33

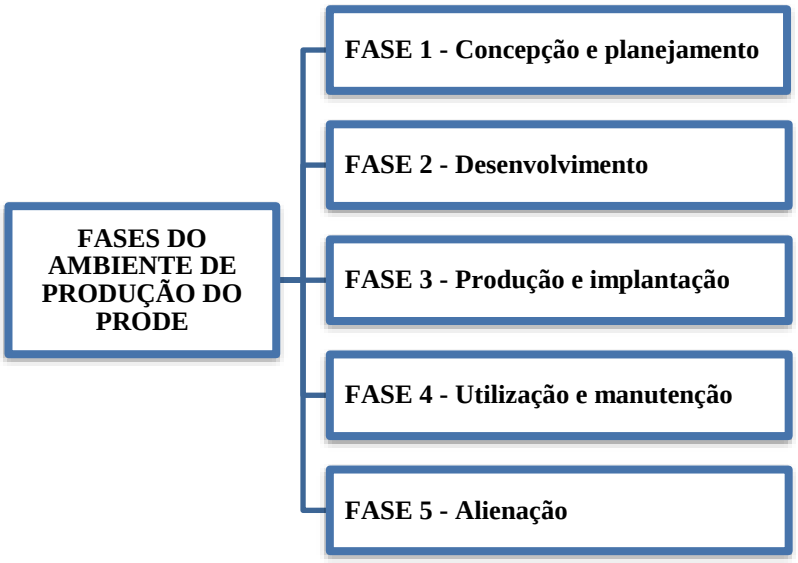
Figura 33 – Ciclo de Vida dos Produtos das FA agrupados por Fases



Fonte: Elaboração da autora, 2015.

Então, a partir da Figura 33 foi possível agrupar as fases de cada ciclo de vida de material adotado pelas FA em cinco fases que agrupam funções comuns no processo de produção do PRODE, conforme a Figura 34.

Figura 34 – Fases do Ambiente de Produção do PRODE



Fonte: Elaboração da autora, 2015, com base em Brasil (2009; 2010); Franco-Azevedo (2013); e Carrilho (2014).

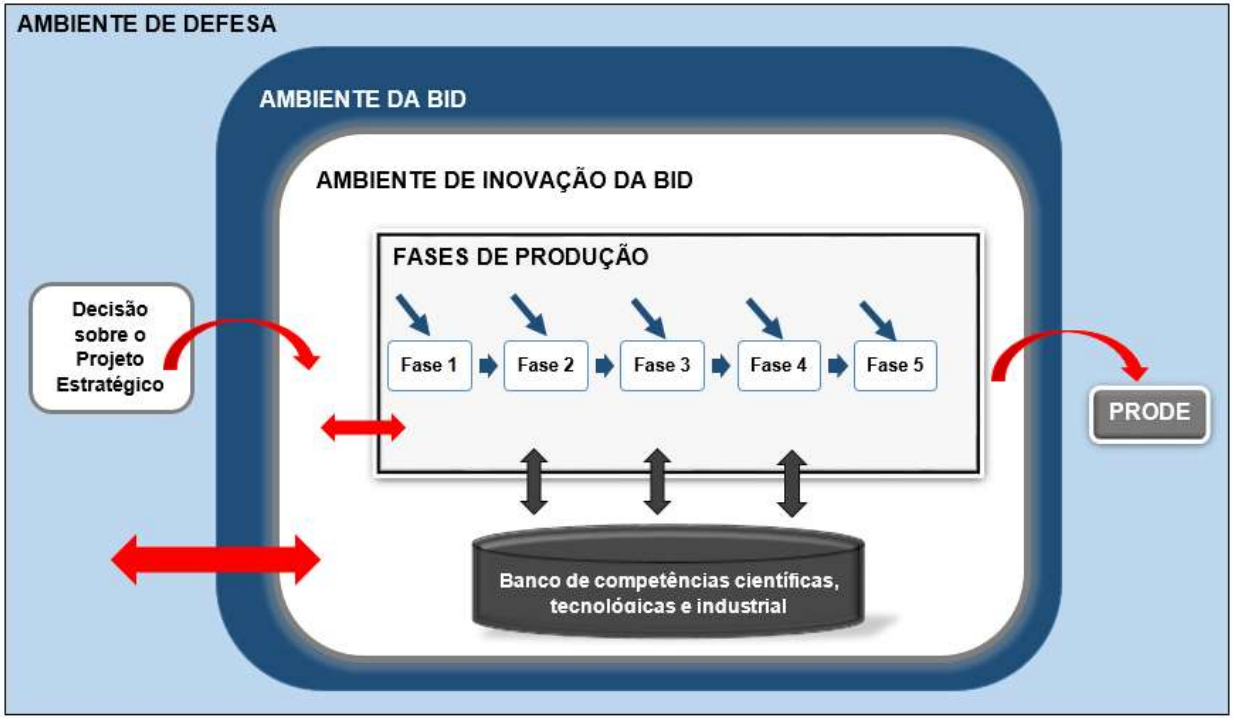
Deste modo, a seguir apresentamos a descrição das Fases do ambiente de produção do PRODE elaborada nesta pesquisa.

a) A Fase 1 – Concepção e Planejamento, envolve as atividades de levantamento da demanda (carência operacional) e da oportunidade tecnológica. Elabora-se o estudo de viabilidade, riscos, prazos, custos, requisitos operacionais e logísticos, e outros. Realiza-se o planejamento do que precisa ser feito quanto à demanda (desenvolvimento, modernização, aquisição e outros) e planeja as ações futuras, e elabora-se os contratos. Os envolvidos são selecionados, como as indústrias de defesa e órgãos governamentais.

b) A Fase 2 – Desenvolvimento, se for a opção o desenvolvimento do PRODE, então, compreende as atividades de planejamento e execução da P&D, nacionalização tecnológica e protótipo. Se for a opção de aquisição, serão elaborados e executados planos de nacionalização, *off-set*, e outros. Esta fase também prevê a realização de testes para homologação, certificação/aceitação do produto.
c) A Fase 3 – Produção e Implantação, compreende a obtenção do PRODE, seja por aquisição ou desenvolvimento de um novo produto, e os preparativos para ser entregue à Força demandante.
d) A Fase 4 – Utilização e Manutenção, destina-se as atividades de operação do PRODE, avaliação de desempenho operacional, análise de estimativa de vida, manutenção e necessidade de revitalização, melhorias e modernização. Assim, desta fase pode gerar novas demandas de produção.
e) A Fase 5 – Alienação, compreende o planejamento e a execução da desativação do PRODE.

Em seguida, apresentamos o Modelo de Produção para o Ambiente de Inovação da BID, na Figura 35, elaborado nesta tese, para representar as Fases do ambiente de produção do PRODE no seu ambiente de inovação, assim como as interações deste ambiente com os demais ambientes.

Figura 35 – Modelo de Produção para o Ambiente de Inovação da BID



Fonte: Elaboração da autora, 2015.

A aprovação de uma das ações previstas para o projeto estratégico da Força, no Ambiente de Defesa, serve de entrada para o Ambiente da BID. Este Ambiente, repassa em forma de Demanda para o Ambiente de Inovação da BID, que dispara a execução das Fases de Produção.

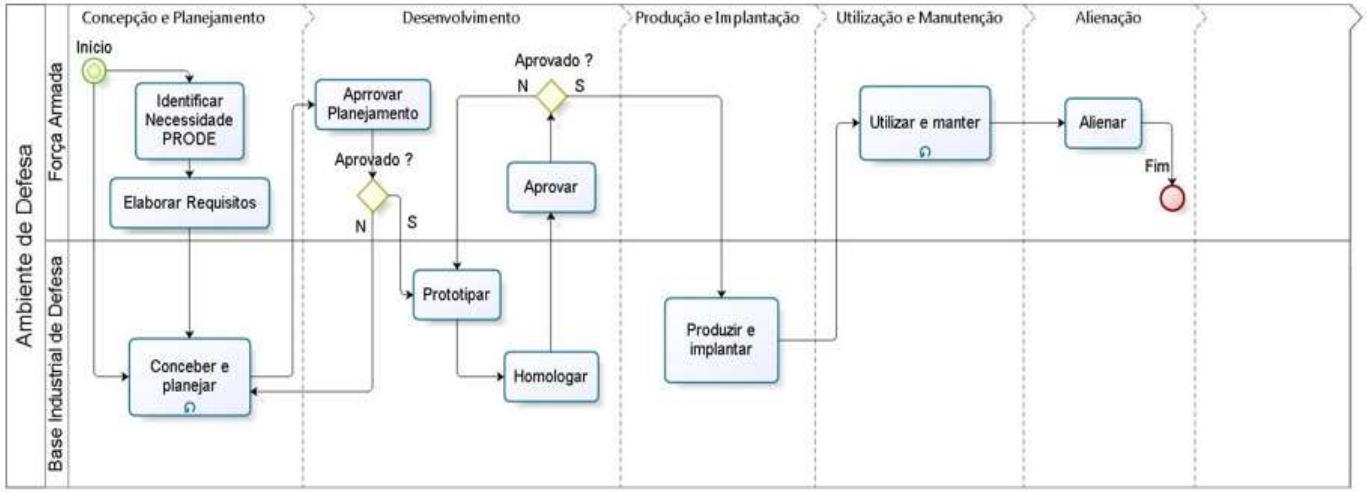
Observa-se que a execução das Fases acontece de forma sequencial, mas também pode ser iniciada a partir de qualquer uma delas, de acordo com o conteúdo da demanda recebida.

O resultado é a entrega do PRODE à Força demandante, que está no Ambiente de Defesa.

O Modelo prevê a existência do Banco de Competências científicas, tecnológicas e industriais formado e atualizado com o conhecimento adquirido na execução das Fases de Produção. Limitamos representá-lo na Figura 35, pois não é foco deste estudo.

A Figura 36 detalha o fluxo das principais ações previstas para as Fases de Produção do PRODE.

Figura 36 – Ações do Ambiente de Produção da BID



Fonte: Elaboração da autora, 2016.

7 PROPOSIÇÃO DO *FRAMEWORK* DE APLICAÇÃO DOS INSTRUMENTOS DE PROTEÇÃO DO SEGREDO NO AMBIENTE DE INOVAÇÃO DA BID

Constatada a ausência de um *framework* que represente a aplicação dos instrumentos de proteção do segredo no ambiente de inovação da BID, e em resposta a questão de pesquisa formulada para esta tese, *Como aplicar os instrumentos de proteção do segredo no ambiente de inovação da BID?, e*ntendemos que a forma que melhor atende a complexidade do quesito é elaborar o *Framework* de aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID.

O *framework* é um instrumento que suporta o entendimento e comunica os relacionamentos e interações das partes envolvidas para atender ao propósito estabelecido[15]. Adicionalmente, a representação gráfica das partes envolvidas tende a fazer com que o *framework* seja autoexplicativo, facilitando o seu entendimento e a sua utilização.

A terminologia *framework* é utilizada nas Ciências Sociais de forma abstrata, para representar e compreender um conjunto de conceitos sobre um assunto específico[16] (JULIANI, 2015)

O *Framework* de aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID, proposto nesta tese, representa as Macro Atividades (Controle, Monitoramento, Inteligência e Contra-Inteligência), e as principais dimensões de proteção do *segredo* (Pessoas, Processos, Tecnologia, Gestão Organizacional, Cultura e Artefatos de Conhecimento).

---

[15] Para Shehabudeen et al. (1999), o *Framework* suporta o entendimento e a comunicação da estrutura e o relacionamento dentro de um sistema com um determinado propósito – tradução do original: "*A framework supports understanding and communication of structure and relationship within a system for a defined purpose"* (SHEHABUDEEN et al. 1999, p. 9)

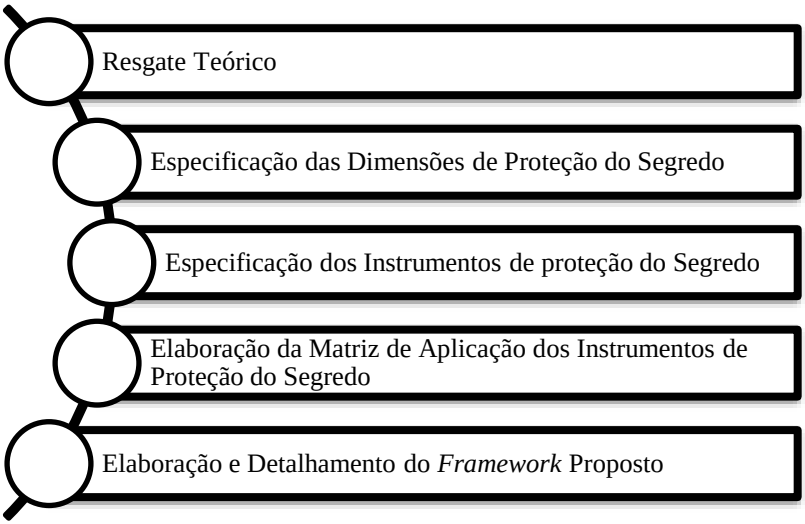
[16] Para Juliani (2015), *Nas ciências exatas, como as ciências da computação e engenharia do conhecimento, por exemplo, os frameworks têm uma conotação prática normalmente materializada por meio de artefatos aplicáveis em casos concretos, como é o caso de um framework para o desenvolvimento de softwares executáveis. Contudo, as ciências sociais utilizam essa mesma terminologia de forma mais abstrata para a representação e a compreensão de um conjunto de conceitos sobre um assunto específico* (JULIANI, 2015, p. 112-113)

Para a proposta do *Framework* de aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID foram seguidas as etapas apresentadas na Figura 37, descritas a seguir.

7.1 ETAPAS DE CONSTRUÇÃO DO *FRAMEWORK*

A Figura 37 apresenta as etapas que foram seguidas para a construção do *framework* proposto.

Figura 37 – Etapas de Construção do *Framework*



Fonte: Elaboração da autora, 2016.

7.2 RESGATE TEÓRICO PARA COMPOSIÇÃO DO *FRAMEWORK*

Para a concepção do *framework* aplicou-se a fundamentação construída ao longo dos capítulos anteriores. As principais peças são apresentadas a seguir.

No capítulo 2 prospectamos os fundamentos conceituais sobre informação e conhecimento nos ambientes acadêmico e de Defesa, aspectos de segurança e proteção da informação e conhecimento, inovação e segredo.

Foi de importância capital a harmonização dos definições e termos, pois proporcionou a caracterização do "segredo" no Ambiente de Inovação da BID, bem como elucidou a aplicabilidade dos diversos instrumentos para sua proteção.

Ainda concorreu, significativamente, para a elaboração do *framework* o Sistema Sociotécnico da BID, apresentado no Capítulo 4, e a caracterização do Ambiente de Inovação da BID, representado no Modelo de Produção para o ambiente de Inovação da BID, conforme o Capítulo 5.

Mostraram-se relevantes para a concepção deste *framework* as fundamentações apresentadas a seguir.

7.2.1 Informação, Conhecimento e Segredo no Ambiente de Inovação da BID

Ao fazer a harmonização, Capítulo 4, elaboramos conceitos e termos a partir de terminologias e definições de uso comum no ambiente da pesquisa, como apresentado a seguir.

A definição de *Informação de Defesa* foi construída a partir dos termos apresentados, anteriormente, na Figura 13.

Repetição da Figura 13 - Representação da Informação de Defesa

Fonte: Elaboração da autora, 2015.

O braço Inteligência provê insumos por intermédio dos diversos formatos que possuem características próprias na fase de elaboração. A outra fonte de insumos contém informações para negócios e informações de tecnologia que são provenientes da indústria, do meio acadêmico e do governo. A pertinência, a relevância e o valor dos insumos são verificados e analisados quanto ao Interesse de Defesa, possibilitando a partir destes filtros, a elaboração da Informação de Defesa.

Assim, definimos *Informação de Defesa*, como:

INFORMAÇÃO DE DEFESA: conjunto de dado e informação, processados ou não, de origem endógena e exógena que é de Interesse de Defesa.

A definição de *Conhecimento de Defesa* foi construída a partir dos termos apresentados, anteriormente, na Figura 14.

Repetição da Figura 14 – Representação do Conhecimento de Defesa

Fonte: Elaboração da autora, 2015.

Como representado na Figura 14, o *Conhecimento de Defesa* é bastante holístico e é produzido a partir informações imbricáveis, que vão da interpretação e da compreensão de *Informações de Defesa*, passa por conhecimentos produzidos pela inteligência e chega aos conhecimentos relacionados às diversas atividades estratégicas de defesa. Atributos como pertinência, relevância e valor das informações são verificados e analisadas quanto ao Interesse de Defesa, possibilitando a elaboração do Conhecimento de Defesa.

O Conhecimento de interesse da Defesa, foi chamado aqui de *Conhecimento de Defesa* e definido como:

CONHECIMENTO DE DEFESA: conhecimento de Interesse da Defesa obtido a partir da análise e interpretação de Informações de Defesa, Conhecimentos produzidos pela Inteligência, e outros Conhecimentos.

A definição de *Segredo* foi construída a partir dos termos apresentados, anteriormente, na Figura 15.

Repetição da Figura 15 – O Segredo no Ambiente de Inovação da BID

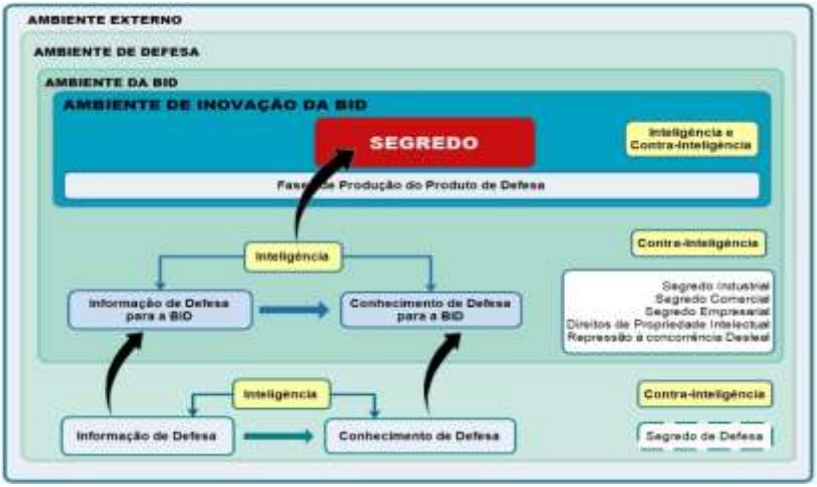
Fonte: Elaboração da autora, 2015.

Como representado na Figura 15, vários temos foram utilizados para formar a definição de *Segredo*, como:

SEGREDO: No Ambiente de Inovação da BID, é o conjunto de Informação de Defesa e de Conhecimento de Defesa, inclusive os artefatos de conhecimentos, que em função da criticidade, do valor que possui e da importância estratégica é classificado como sigiloso ou de acesso restrito, e que não pode ser de domínio público, pois envolve novidade, segredos e direitos de propriedade industrial da BID; e é passível de proteção, por instrumentos legais e administrativos e por atividades de Inteligência e Contra-Inteligência.

O Ambiente de Inovação da BID, para o qual foi apresentado a definição de *segredo* acima, encontra-se contextualizado na Figura 16, repetida a seguir:

Repetição da Figura 16 - Harmonização terminológica para o Ambiente de Inovação da BID



Fonte: Elaboração da autora, 2015.

A Figura 15 apresenta os ambientes considerados nesta tese. O Ambiente Externo acha-se circunscrito Ambiente de Defesa e este ao

Ambiente da BID. O Ambiente de Inovação da BID, mais segregado, está inscrito no Ambiente da BID.

A Figura 15 também apresenta os fluxos de Informações e Conhecimentos de Defesa bem como outros elementos relevantes nos ambientes. A representação gráfica do Ambiente de Inovação da BID comunica a ideia de restrição de acesso de pessoas ao ambiente bem como a relevância, o valor estratégico e a sensibilidade do *segredo*.

7.2.2 Sistema Sociotécnico para BID

No Capítulo 5 concebemos o Sistema Sociotécnico para a BID conforme foi apresentado na Figura 20.

O Sistema Sociotécnico representa as relações e interações entre o Subsistema Técnico e o Subsistema Social, bem como as relações com o ambiente externo.

O Subsistema Técnico que compreende as tarefas a serem desempenhadas, as instalações físicas, os equipamentos e instrumentos utilizados, as exigências da tarefa, as utilidades e técnicas operacionais, o ambiente físico, e a operação das tarefas. É o responsável pela eficiência potencial. O Subsistema Social compreende as pessoas, as relações sociais entre os indivíduos, e as exigências de trabalho. A repetição da Figura 19 representa esse entendimento para a tese.

Repetição da Figura 19– Sistema Sociotécnico para a BID

Fonte: Elaboração da autora, 2015

Observamos que o Ambiente Externo apresenta a origem, de onde são importados os insumos, e o destino para onde são exportados os produtos. Este ambiente contém o Ambiente da BID, os agentes e as exigências de trabalho (requisitos), estes contidos em dispositivos legais e doutrinas. Os principais agentes citados foram o Governo, a academia, o MD e as Forças Armadas.

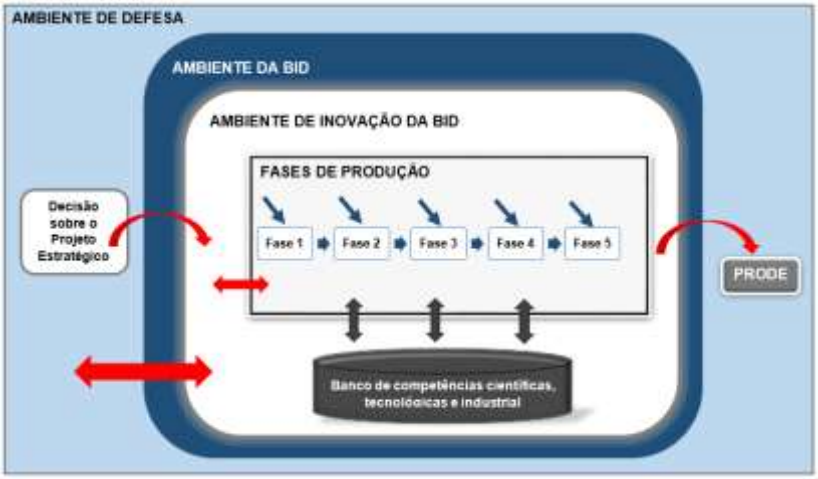
A estrutura do Sistema Sociotécnico para a BID comporta os subsistemas Técnico e Social com as respectivas relações e interações e também as relações com o Ambiente Externo.

Uma vez que os subsistemas estão interagindo e sendo mutuamente influenciados, ocorre, de forma contínua, a conversão dos insumos importados em produtos para serem exportados.

7.2.3 Modelo de Produção para o Ambiente de Inovação da BID

O Modelo de Produção para o Ambiente de Inovação da BID foi concebido no Capítulo 6 e reapresentado na Figura 35.

Repetição da Figura 35 – Modelo de Produção para o Ambiente de Inovação da BID



Fonte: Elaboração da autora, 2015.

O modelo apresenta o Ambiente de Inovação da BID inscrito no Ambiente da BID e este no Ambiente de Defesa. São apresentados também os insumos, resultados e as interfaces. Destaca-se no modelo a

representação das fases para a produção do PRODE, que foram elaboradas a partir da análise dos ciclos de vida dos PRODE de cada FA.

7.3 DIMENSÕES DE PROTEÇÃO DO SEGREDO

Heisig (2009) ao comparar 160 *frameworks* de GC, com o objetivo identificar semelhanças e diferenças entre *frameworks* e contribuir para a harmonização termos na GC, constatou que a maior frequência dos termos que foram considerados fatores críticos para o sucesso dos *frameworks* se encontrava nas dimensões do conhecimento Recursos Humanos, Organização (processos e estrutura organizacional), Tecnologia (infraestrutura e aplicativos) e Gestão Organizacional (estratégia e objetivos).

Para esta tese definimos Dimensões de Proteção do Segredo como:

DIMENÇÕES DE PROTEÇÃO DO SEGREDO: São dimensões de conhecimento, que representam áreas específicas dentro da organização, que requerem atenção quanto à proteção sob a ótica do segredo.

Para atender a complexidade inerente ao Ambiente de Inovação da BID, entendemos que as Dimensões de Proteção do Segredo devem considerar as dimensões apresentadas por Heisig (2009) e a especificidade exigida para a aplicação de instrumentos de proteção do segredo.

Assim, as Dimensões de Proteção do Segredo são: Pessoas, Processos, Tecnologia, Gestão Organizacional, Cultura e Artefatos do Conhecimento, apresentadas na Figura 38.

Figura 38 – Dimensões de Proteção do Segredo

Fonte: Elaboração da Autora, 2016.

As Dimensões de Proteção do Segredo propostas para o *framework* encontram-se descritas a seguir. Cabe ressaltar que elas abrangem, mas não esgotam, os tópicos relacionados em cada dimensão.

a) **Pessoas**: Esta dimensão contempla aspectos relacionados com o recrutamento, a seleção, o desenvolvimento, as competências individuais e coletivas, a formação, as experiências, os relacionamentos, a motivação, as qualificações, os princípios, a cultura geral, as habilidades e características pessoais, a capacidade de liderança, a facilidade para trabalhar em equipe, o sistema de reconhecimento, a facilidade para compartilhar conhecimento, o cumprimento de normas, aspirações, plano de carreira, salários. Contempla também empregados, pesquisadores, prestadores de serviço, colaboradores em geral.
b) **Processos**: Esta dimensão contempla aspectos relacionados com processos organizacionais, estrutura organizacional, infraestrutura, gestão dos processos, melhoria dos processos,

processos de pesquisa, testes, desenvolvimento de modelos e protótipos.

c) **Tecnologia**: Esta dimensão contempla aspectos relacionados à infraestrutura, sistemas e aplicações, segurança tecnológica, controle de acessos a sistemas, competências tecnológicas, atualização tecnológica, tecnologias de uso pessoal, tecnologias próprias, interações tecnológicas.
d) **Gestão Organizacional**: Esta dimensão contempla aspectos relacionados com o planejamento estratégico, a governança, a missão, os valores da organização, a liderança no setor de atuação, sistema de medição e indicadores de desempenho, a inteligência competitiva, o mercado, o regimento interno, aspectos legais.
e) **Cultura**: Esta dimensão contempla aspectos relacionados com programa de aprendizagem contínua, criação do conhecimento organizacional, gestão do conhecimento, proteção do conhecimento, gestão de riscos, valores.
f) **Artefatos de Conhecimento**: Esta dimensão contempla aspectos relacionados com os documentos, os projetos, os códigos de sistemas, circuitos, os planos de marketing, as comunicações, os contratos, as especificações, os requisitos.

7.4 INSTRUMENTOS DE PROTEÇÃO DO SEGREDO

A partir do entendimento que *proteção* é o conjunto de ações adotadas para a defesa do *segredo*, e que a *segurança* é o estabelecimento de condições que neutralizem potenciais ameaças ao *segredo*, inventariamos a partir das pesquisas documentais e bibliográficas realizadas nesta tese, os instrumentos de proteção aplicáveis ao Ambiente de Inovação da BID, e os apresentamos no Quadro 20, com as respectivas referências.

Quadro 20 – Instrumentos de Proteção Identificados na Literatura

	Instrumento de Proteção	Fonte
1.	Assinar acordos de não divulgação	NORMAN, 2001; BOCCHINO, 2012
2.	Atividades de Contra-Inteligência	NORMAN, 2001; BRASIL, 2005; DESOUZA, 2007; BRASIL, 2011; BOCCHINO, 2012; NBR ISO/IEC 27002, 2013b; NBR-16167, 2013a; MAIER, 2007; NBR-11515, 2007; JACINTO, 2008
	Atividades de Inteligência	BRASIL, 2005c
3.	Capacidade de Resposta imediata	DESOUZA, 2007
4.	Classificação e rotulação dos ativos	NBR-16167, 2013a
5.	Construção de Alianças baseadas na confiança	DESOUZA, 2007
6.	Construção de cenários alternativos	DESOUZA, 2007
7.	Consultar Especialistas	NORMAN, 2001; BOCCHINO, 2012
8.	Documentação do conhecimento	ILVONEN, 2013
9.	Estabelecer consequências para o descumprimento de regras de compartilhamento do conhecimento	NORMAN, 2001; BOCCHINO, 2012
10.	Firmar Contrato de parceria PD&I	PIMENTEL, 2010
11.	Firmar contrato de restrição de trabalhos futuros	NORMAN, 2001; BOCCHINO, 2012
12.	Firmar Contrato de sigilo	NORMAN, 2001; BOCCHINO, 2012; DE FARIA E SOFKA, 2010
13.	Formalizar a confidencialidade (acordos, cláusula, declaração e contrato)	NORMAN, 2001; BOCCHINO, 2012; PIMENTEL, 2010

(Continuação do Quadro 20)

	Instrumento de Proteção	Fonte
14.	Gestão de recursos humanos	BRASIL, 2000; GOLD et al, 2001; DESOUSA, 2007; NORMAN, 2001; NBR ISO/IEC 27002, 2013b; MAIER, 2007; NASCIMENTO, 2008; BOCCHINO, 2012; ILVONEN, 2013; OLANDER, VANHALA e HUMELINNA-LAUKKANEM, 2014
15.	Gestão de Riscos	NBR ISO 31000, 2009; JACINTO, 2008; BRASIL, 2005
16.	Contrato de *Know How*	WIPO,OMPI e INPI, 2015a
	Negar acesso as informações referentes a projetos de P&D sigilosos	BRASIL, 2011
17.	Negar acesso do parceiro às atividades, instalações restritas e pessoas for da parceria	NORMAN, 2001; BOCCHINO, 2012
18.	Nomear um gestor do conhecimento	NORMAN, 2001; BOCCHINO, 2012
19.	Planos de contingência	DESOUZA, 2007
20.	Políticas e procedimentos de segurança da informação e do conhecimento	NBR-16167, 2013a; MAIER, 2007; NBR ISO/IEC 27002, 2013b
21.	Procedimentos de segurança física para os Dados	NBR-11515, 2007
22.	Processo de proteção na GC	DAVENPORT et al, 1998; GOLD *et al*., 2001; LUCAS, 2010; MAIER, 2007; ROCHA et al.,[200?]
23.	Proteger os Direitos de Propriedade Intelectual (Propriedade Industrial e Direitos autorais)	WIPO, OMPI e INPI, 2015a; NORMAN, 2001; BOCCHINO, 2012; MAIER, 2007; OLANDER, VANHALA e HUMELINNA-LAUKKANEM, 2014; DE FARIA E SOFKA, 2010; GONZÁLEZ-ÁLVAREZ E NIETO-ANTOLÍN, 2007; JUNGMANN, 2010

(Continuação do Quadro 20)

	Instrumento de Proteção	Fonte
24.	Segredo de Negócio	WIPO, OMPI e INPI, 2015a; JUNGMANN, 2010; BRASIL, 1996
25.	Segurança no uso de tecnologias pervasivas	DESOUZA, 2007
26.	Segurança física das instalações	DESOUZA, 2007

Fonte: Elaboração da autora, 2016.

Destaca-se que esta seleção refletiu o estado da arte no momento da construção do referencial teórico desta tese, portanto não esgota as possibilidades de instrumentos de proteção aplicáveis ao *framework* proposto.

Os Instrumentos de Proteção do Segredo aplicáveis nas Dimensões apresentadas na seção 6.3, representam o conjunto instrumentos de natureza própria que têm por finalidade mitigar riscos ao Segredo do Ambiente de Inovação da BID.

Definimos Instrumento de Proteção do Segredo, como:

INSTRUMENTO DE PROTEÇÃO DO SEGREDO
Objeto que contém recomendações aplicáveis às Dimensões de Proteção do Segredo com a finalidade de salvaguardar o segredo

A Figura 39 representa a aplicação dos Instrumentos de Proteção do Segredo nas Dimensões de Proteção do Segredo (seção 6.3).

Figura 39 – Instrumentos de Proteção do Segredo

Fonte: Elaboração da autora, 2016.

A Figura 39 enfatiza a aplicação dos Instrumentos de Proteção do nas Dimensões de Proteção do Segredo com a finalidade de salvaguardar o segredo no Ambiente de Inovação da BID.

A seguir, apresentamos as diretrizes para a aplicação dos Instrumentos de Proteção do Segredo para o Ambiente de Inovação da BID, com a descrição sucinta elaborada a partir do Quadro 20. Estas descrições foram elaboradas com adaptações para atender a aplicação do instrumento no Ambiente de Inovação da BID.

1. Assinar acordos de não divulgação
   - Os acordos de não divulgação operam como instrumento capaz de garantir legalmente a proteção do *segredo* quanto à não exposição de seu conteúdo ao conhecimento público.
   - Convém que seja estabelecido critérios para avaliar a necessidade de aplicação deste instrumento no Ambiente de Inovação da BID.
2. Atividades de Contra-Inteligência
   - O Instrumento Contra-Inteligência, compreende as atividades que buscam detectar, identificar, neutralizar barreiras e prevenir operações de Inteligência adversa ou ações de qualquer natureza que ameacem o *segredo* e seus suportes, tais como: documentos, pessoas, material, áreas e instalações e nas tecnologias. Mantém um quadro de ameaças, riscos e vulnerabilidades, provenientes da Gestão de Riscos, para a salvaguarda do *segredo*. É subdividida em Segurança Orgânica e Segurança Ativa.
   - Cabe à Segurança Orgânica proteger o *segredo* sob os aspectos pessoal, documental, material, nos meios de TI e nas áreas e instalações. Para isso, executa as ações de controle de visitantes e funcionários; fornecimento de credenciais de segurança; restrição de acesso ao conhecimento somente para quem necessita conhecer (compartimentalização do conhecimento); implementação de mecanismos de proteção para as tecnologias; controle de pontos de entrada e saída de objetos; ações especializadas para iludir e confundir ações adversas, e outras.
   - Cabe à Segurança Ativa empreender ações contra as ações de influência psicológica, como por exemplo: propaganda adversa; e contra as ações de espionagem e Inteligência adversa. Monitora os comportamentos do pessoal interno e dos parceiros.
   - Convém que seja criado uma estrutura de inteligência para gerir as ações da Contra-Inteligência no Ambiente de Inovação da BID, e tomar as medidas de proteção tempestivamente.

3. Atividades de Inteligência
   - O exercício das Atividades de Inteligência representa aplicação do Instrumento capaz de produzir conhecimentos para a proteção do segredo, relatando na forma de Informes, Informação, Apreciação e Estimativa, os fatos e situações, atuais ou potenciais, que possam comprometer o segredo.
   - Convém que este Instrumento seja utilizado amplamente no Ambiente da BID.
4. Capacidade de resposta Imediata
   - Este instrumento mede o preparo da organização para enfrentar o momento de crise causado pela exposição, indevida, do *segredo* ao conhecimento público ou outro evento que traga instabilidade para a garantia de proteção do *segredo*, cabendo uma ação imediata para sanar a crise.
   - Convém que a aplicação deste Instrumento seja considerada uma ação proativa de proteção do *segredo*.
5. Classificação e rotulação dos ativos
   - Este instrumento refere-se a identificação e atribuição de classes de grau de sigilo aos dados, informações e conhecimentos.
   - Convém que, seja aplicado ao se criar um conhecimento ou informação, pois representa um instrumento essencial para a proteção do *segredo*.
6. Construção de alianças baseadas na confiança
   - Este Instrumento previne a ação com dolo e o vazamento de informações, de conhecimento por parte dos parceiros, o que afetaria a proteção do *segredo*.
   - Convém que a confiança deve ser estabelecida antes da parceria e monitorada por meio dos comportamentos dos parceiros da aliança.
7. Construção de cenários alternativos
   - Representa um instrumento de ação proativa que prepara o Ambiente de Inovação da BID para a adoção de medidas alternativas que garantam a proteção do *segredo* diante de uma possibilidade de crise (exposição indevida do segredo ao conhecimento público, ou outro evento que traga instabilidade para a garantia de proteção do segredo).

- Convém que seja utilizada técnicas de escalonamento de crises para verificar a aplicação do Instrumento no Ambiente de Inovação da BID.

8. Consultar especialistas
   - Representa a aplicação de Instrumento consultivo para o Ambiente de Inovação da BID.
   - É válido para obter instruções e conselhos de pessoas de notório saber em áreas, que embora não represente o *core business* da BID, sejam consideradas essenciais para melhorar o entendimento em determinado assunto.
   - Convém se que mantenha um cadastro de especialistas nas diversas áreas de interesse da BID.
9. Documentar o conhecimento
   - Este instrumento diz respeito à explicitação (codificação) do conhecimento em mídias de conhecimento apropriadas, que permitam a apropriação e sua proteção do conhecimento, e consequentemente, do *segredo*.
   - Convém que seja observada a classificação do grau de sigilo para não comprometer a proteção do *segredo*.
10. Estabelecer consequências para o descumprimento de regras de compartilhamento do conhecimento
    - Este instrumento tem o propósito de regular o tratamento dado ao conhecimento, alertar e estabelecer consequências para a imprudência e dolo nas ações praticadas no trato e compartilhamento do conhecimento.
    - Convém que seja observado a aplicação deste Instrumento para que não haja comprometimento da proteção do *segredo.*
11. Firmar Contrato de parceria PD&I
    - Refere-se ao Instrumento jurídico que atua como garantia da proteção do *segredo* ao caracterizar o conjunto de elementos intangíveis e tangíveis alocados pelas partes contratantes ou parceiras, e registrar a forma de como se dará a transferência dos resultados de PD&I.
    - Convém que este Instrumento seja aplicado com todo o rigor e abrangência jurídica para que haja a efetiva proteção do *segredo.*

12. Firmar *contrato de restrição de trabalhos futuros*
    - Este instrumento jurídico é aplicado para restringir, por tempo determinado, ações de apropriação de conhecimentos especializados por parte da concorrência, que ao contratar ex-funcionários que detenham conhecimentos estratégicos relativos à sua função anterior, possa representar conflito de interesse.
    - Convém que na contratação seja aplicado este Instrumento, conforme o caso.
13. Firmar Contrato de sigilo
    - Refere-se ao Instrumento jurídico que visa garantir que o conhecimento ou tecnologia compartilhada com o parceiro esteja protegida para não se tornar de domínio público.
    - Convém que este Instrumento seja aplicado em casos que envolvam segredo comercial e projetos de P&D.
14. Formalizar a confidencialidade (acordos, cláusula, declaração e contrato)
    - Trata-se de Instrumento jurídico que garante direitos de confidencialidade ao conhecimento ou à tecnologia que esteja sob sigilo ou restrição de acesso.
    - Convém que este Instrumento seja aplicado desde a concepção do projeto, e que seja considerado para todos os envolvidos no Ambiente de Inovação da BID.
15. Gestão de Recursos Humanos
    - Este Instrumento refere-se a parte mais frágil da proteção do *segredo* (“o elo mais fraco”) que é a pessoa, dotada de suas crenças e valores, e que atua no Ambiente de Inovação da BID.
    - Convém que este Instrumento de proteção seja implementado desde o ingresso do funcionário até seu desligamento. Compreende ações de recrutamento, ao verificar os antecedentes. Ações de monitoramento constantemente, para verificar a nível de confiança no funcionário, e verificar se os objetivos dele se alinham com os objetivos requeridos no Ambiente de Inovação da BID.
    - Convém que se estabeleça regras de conduta para os funcionários, e se mantenha o cadastro de dados funcionais atualizado.

- O Instrumento também compreende a retenção de talentos, que é vista como uma forma de proteger o *segredo*.
- Convém que seja promovida ações de incentivos e de recompensas para manter o funcionário na organização.
- A aplicação do Instrumento visa desenvolver e identificar capacidades essenciais.
- Convém que a educação seja vista como protagonista no desenvolvimento de competências essenciais e promotora da proteção do segredo ao capacitar o funcionário no desempenho de suas funções.
- O Instrumento é aplicado ao se conscientizar sobre a cultura de segurança e treinar sobre a confidencialidade.
- Convém que o Instrumento seja aplicado para mitigar a ação da Inteligência adversa que possa comprometer a proteção do segredo, e promover a retenção do conhecimento na organização.

16. Gestão de Riscos
    - A Gestão de Riscos é um Instrumento de proteção capaz de apresentar o retrato das ameaças, identificar deficiências e vulnerabilidades à salvaguarda do *segredo* no Ambiente de Inovação da BID.
    - Convém que a aplicação deste Instrumento seja conjugada com a aplicação do Instrumento de Contra-Inteligência para que não haja duplicidade de ações.
17. Contratos de *Know-how*
    - Refere-se ao Instrumento que protege juridicamente o *know-how*, como objeto do contrato que representa os conhecimentos técnicos e secretos de valor econômico no Ambiente de Inovação da BID.
    - Convém que este Instrumento seja aplicado ao segredo de negócio ou de fábrica.
18. Negar acesso as informações referentes a projetos de P&D sigilosos
    - Este Instrumento legal não dá acesso público as informações sobre os projetos de P&D de interesse de Defesa, por ser de natureza sigilosa.
    - Convém que este Instrumento seja aplicado para dar o tratamento previsto na LAI para as informações sigilosas, evitando que as informações de projetos de

P&D sigilosos sejam de domínio público, e consequentemente, protegendo o *segredo* no Ambiente de Inovação da BID.

19. Negar acesso do parceiro às atividades, instalações restritas e pessoas fora da parceria
    - Refere-se ao Instrumento que nega acesso dos terceiros às atividades e às áreas e instalações de acesso restrito que não estejam no âmbito de sua parceria.
    - Também não permite que os parceiros estabeleçam comunicação com pessoas de fora da parceria estabelecida.
    - Convém que estas regras de negação de acesso do parceiro estejam claramente estabelecidas e sejam de conhecimento dos parceiros e dos funcionários envolvidos na parceria, para que apliquem este Instrumento de proteção do *segredo* no Ambiente de Inovação da BID.
20. Nomear um gestor do conhecimento
    - Este Instrumento prevê que seja nomeado um gestor do conhecimento, com a missão de mitigar a negligencia nas ações de proteção ao conhecimento, bem como ser o responsável pela gestão de conhecimentos proprietários.
    - Convém que o gestor do conhecimento tenha dedicação exclusiva para desempenhar suas funções e fomentar a proteção do segredo no Ambiente de Inovação da BID.
21. Planos de contingência
    - Representa um Instrumento de natureza preventiva, preditiva e reativa que mitiga as consequências negativas para o caso de quebra da proteção do segredo, e permite a continuidade do processo e o controle dos danos.
    - Convém que o Instrumento seja aplicado como uma boa prática de sustentabilidade do Ambiente de Inovação da BID.
22. Políticas e procedimentos de segurança da informação e do conhecimento
    - Este instrumento assegura a confidencialidade, a integridade, a autenticidade, o não-repúdio, além de

prover e a disponibilidade dos dados, das informações e dos conhecimentos tratados, classificados e sensíveis.
- Estabelece normas jurídicas para a implementação da segurança, e as regras de Tratamento da informação classificada.
- Convém a aplicação deste Instrumento para a garantia da confidencialidade, da integridade, da autenticidade do segredo no Ambiente de Inovação da BID.

23. Procedimentos de segurança física para os Dados
    - Refere-se ao Instrumento que considera a proteção e segurança dos dados em seus ambientes operacionais, e mitiga os fatores que influenciam a segurança física dos dados, tais como: localização; construção; infraestrutura elétrica; climatização; móveis, utensílios e equipamentos; medidas, sistemas de controle de acesso e barreiras de segurança; sistemas de detecção e combate a incêndio, alagamento e outros sinistros; operações de manuseio (produção, manutenção e cópias de segurança); e redundância de dispositivos.
    - Convém que este Instrumento seja aplicado aos dados do Ambiente de Inovação da BID.
24. Processo de proteção na GC
    - Este Instrumento possibilita que a proteção seja vista como um dos processos da GC.
    - Convém a aplicação deste Instrumento para garantir a proteção do segredo por meio da GC.

25. Proteger os Direitos de Propriedade Intelectual
    - Instrumento legal que protege os bens intangíveis por meio de patentes e registros de propriedade industrial.
    - Convém que este Instrumento seja aplicado de acordo com a estratégia de negócio adotada no Ambiente e Inovação da BID.
26. Segredo de Negócio
    - Este instrumento refere-se à proteção dos métodos de contratação, comercialização e distribuição do produto, listas de fornecedores e clientes, e processos de produção.
    - As circunstâncias individuais determinam quais informações constituem um segredo comercial.

- Convém que a aplicação deste Instrumento aconteça em concordância com a estratégia de negócio adotada no Ambiente de Inovação da BID para proteger o *segredo* contra as práticas abusivas no domínio das informações secretas, que incluem a espionagem industrial ou comercial, quebra de contrato e violação de confiança.

27. Segurança no uso de tecnologias pervasivas
    - Este Instrumento destina-se a proteção dos dados, informações e conhecimento no uso das tecnologias móveis, de armazenamento e duplicação, e das aplicações tecnológicas.
    - Convém que este Instrumento seja aplicado como proteção do *segredo* durante o uso de tecnologias em viagens ou fora do ambiente da organização.
28. Segurança física das instalações
    - Refere-se ao Instrumento que prevê a proteção física das áreas e instalações da organização.
    - Convém que este Instrumento seja aplicado em conjunto com a Segurança Orgânica prevista no Instrumento Contra-Inteligência para mitigar o risco na proteção do *segredo* dentro do Ambiente de Inovação da BIID.

7.5 MATRIZ DE APLICAÇÃO DOS INSTRUMENTOS DE PROTEÇÃO DO SEGREDO

A Matriz de Aplicação dos Instrumentos de Proteção do Segredo, apresentada no Quadro 21, tem por objetivo apresentar os Instrumentos de Proteção do Segredo, descritos na seção 6.4, mais adequados para serem aplicados na Dimensão de Proteção do Segredo, descritas na seção 6.3.

Quadro 21 – Matriz de Aplicação dos Instrumentos de Proteção do Segredo

Instrumentos de Proteção	**Pessoas**	**Processos**	**Tecnologia**	**Gestão Organizacional**	**Cultura**	**Artefatos de Conhecimento**
Assinar acordos de não divulgação	**X**			**X**	**X**	**X**
Atividades de Contra-Inteligência	**X**	**X**	**X**	**X**	**X**	**X**
Atividades de Inteligência	**X**	**X**	**X**	**X**	**X**	**X**
Capacidade de resposta imediata	**X**			**X**	**X**	
Classificação e rotulação dos ativos				**X**	**X**	**X**
Construção de alianças baseadas na confiança	**X**			**X**	**X**	
Construção de cenários alternativos	**X**			**X**		
Consultar Especialistas	**X**			**X**	**X**	
Documentar o conhecimento				**X**	**X**	**X**
Estabelecer consequências para o descumprimento de regras de compartilhamento do conhecimento	**X**			**X**	**X**	
Firmar Contrato de parceria PD&I				**X**		
Firmar contrato de restrição de trabalhos futuros	**X**			**X**		
Firmar Contrato de sigilo	**X**			**X**	**X**	
Formalizar a confidencialidade (acordos, cláusula, declaração e contrato)				**X**	**X**	
Gestão de Recursos Humanos	**X**			**X**	**X**	
Gestão de Riscos	**X**	**X**	**X**	**X**	**X**	**X**
Contrato de *Know How*		**X**		**X**	**X**	
Negar acesso as informações referentes a projetos de P&D sigilosos	**X**			**X**	**X**	
Negar acesso do parceiro às atividades, instalações restritas e pessoas for da parceria	**X**			**X**	**X**	
Nomear um gestor do conhecimento				**X**	**X**	
Planos de contingência				**X**	**X**	

(Continuação do Quadro 21)

Instrumentos de Proteção	Pessoas	Processos	Tecnologia	Gestão Organizacional	Cultura	Artefatos de Conhecimento
Políticas e procedimentos de segurança da informação e do conhecimento	X	X	X		X	X
Procedimentos de segurança física para os Dados	X				X	X
Processo de proteção na GC	X	X	X	X	X	X
Proteger os Direitos de Propriedade Intelectual		X	X		X	X
Segredo de Negócio	X	X	X	X	X	X
Segurança no uso de tecnologias pervasivas	X	X	X		X	X
Segurança física das instalações	X				X	

Fonte: Elaboração da autora, 2016.

O Quadro 21 foi elaborado a partir da observação das diretrizes para a aplicação dos Instrumentos de Proteção do Segredo no contexto de cada Dimensão de Proteção do Segredo.

A distribuição dos Instrumentos de Proteção do Segredo nas Dimensões de Proteção do Segredo é apresentada pelo Gráfico 2.

Gráfico 2 – Aplicabilidade dos Instrumentos de Proteção do Segredo

Fonte: Elaboração da autora, 2016.

Observa-se no Gráfico 2 que houve maior concentração dos Instrumentos de Proteção do Segredo nas dimensões Cultura, Gestão Organizacional e Pessoas, e poucos Instrumentos aplicáveis às dimensões Artefatos de Conhecimento, Processos e Tecnologia.

Enfatizando que a dimensão *Cultura* contempla aspectos relacionados com programa de aprendizagem contínua, criação do conhecimento organizacional, gestão do conhecimento, proteção do conhecimento, gestão de riscos, valores; a dimensão *Gestão Organizacional* contempla aspectos relacionados com o planejamento estratégico, a governança, a missão, os valores da organização, a liderança no setor de atuação, sistema de medição e indicadores de desempenho, a inteligência competitiva, o mercado, o regimento interno, aspectos legais; e a dimensão *Pessoas* contempla aspectos relacionados com o recrutamento, a seleção, o desenvolvimento, as competências individuais e coletivas, a formação, as experiências, os relacionamentos, a motivação, as qualificações, os princípios, a cultura geral, as habilidades e características pessoais, a capacidade de liderança, a facilidade para trabalhar em equipe, o sistema de reconhecimento, a facilidade para compartilhar conhecimento, o cumprimento de normas, aspirações, plano de carreira, salários. Contempla também empregados, pesquisadores, prestadores de serviço, colaboradores em geral.

Em adição, a dimensão *Artefatos de Conhecimento* contempla aspectos relacionados com os documentos, os projetos, os códigos de sistemas, circuitos, os planos de marketing, as comunicações, os contratos, as especificações, os requisitos; a dimensão *Processos* contempla aspectos relacionados com processos organizacionais,

estrutura organizacional, infraestrutura, gestão dos processos, melhoria dos processos, processos de pesquisa, testes, desenvolvimento de modelos e protótipos; e a dimensão *Tecnologia* contempla aspectos relacionados à infraestrutura, sistemas e aplicações, segurança tecnológica, controle de acessos a sistemas, competências tecnológicas, atualização tecnológica, tecnologias de uso pessoal, tecnologias próprias, interações tecnológicas.

7.6 ELABORAÇÃO E DETALHAMENTO DO *FRAMEWORK* DE APLICAÇÃO DOS INSTRUMENTOS DE PROTEÇÃO DO SEGREDO NO AMBIENTE DE INOVAÇÃO DA BID

A partir dos resultados obtidos nas etapas de resgate teórico (seção 6.2), das Dimensões de Proteção do Segredo (seção 6.3), dos Instrumentos de Proteção do Segredo (seção 6,4), da Matriz de Aplicação dos Instrumentos de Proteção do Segredo (seção 6.5), e da experiência da pesquisadora, detectou-se a necessidade de acrescentar artefatos para exercerem atividades que identifiquem e neutralizem potenciais ameaças ao segredo. Tal necessidade foi suprida com a inclusão das Macro Atividades: *Controle*, *Monitoramento*, *Inteligência* e *Contra-Inteligência*, descritas a seguir.

7.6.1 Macro Atividade *Controle*

Considerando que o *Controle* inclui qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco (NBR ISO 31000, 2009), a Macro Atividade *Controle* atua em benefício da proteção do segredo assegurando que os Instrumentos de Proteção do Segredo adequados sejam aplicados às Dimensões de Proteção do Segredo, e que o conjunto de medidas adotado seja suficiente para mitigar riscos ao segredo.

7.6.2 Macro Atividade *Monitoramento*

A Macro Atividade *Monitoramento* executa, continuamente, as atividades de verificação, supervisão e observação crítica, a fim de identificar as mudanças no ambiente das Dimensões de Proteção do Segredo onde foram aplicados os Instrumentos de Proteção do Segredo, assegurando a mitigação de riscos ao segredo.

Atenção especial deve ser dedicada à gestão de mudanças, pois novas vulnerabilidades podem surgir e afetar a segurança do segredo.

Outro ponto de atenção é a obsolescência dos ativos de informação e conhecimento, pois possuem ciclo de vida curto.

7.6.3 Macro Atividade Inteligência e Contra-Inteligência

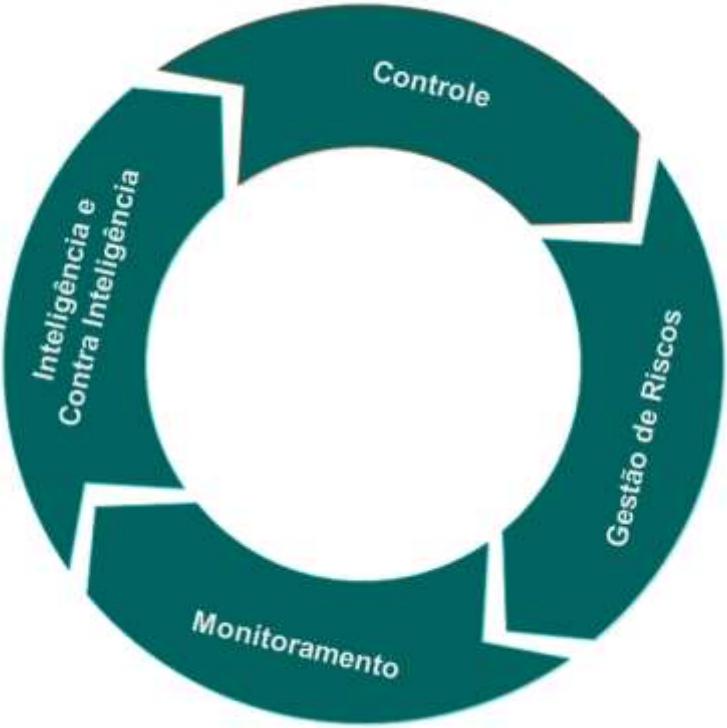
Esta Macro Atividade comporta duas atividades que trabalham juntas. A Macro Atividade *Inteligência* atua em benefício da segurança do segredo produzindo informações e conhecimentos sobre fatos e situações, atuais ou potenciais, internas e externas, que possam comprometer a segurança do segredo. A Macro Atividade *Contra-Inteligência* atua em benefício da segurança do segredo conduzindo atividades que buscam prevenir, detectar, e neutralizar ações de qualquer natureza e origem que ameacem a segurança do segredo.

7.6.4 Macro Atividade Gestão de Riscos

A Macro Atividade *Gestão de Riscos* compreende a prática dos princípios e processos da Gestão de Riscos prevista na NBR-ISO-31000 (2009) para que sejam conhecidas as ameaças, as probabilidades de virem a ocorrer, e os impactos que poderão causar à segurança do segredo. As documentações são utilizadas na escolha dos Instrumentos de Proteção do Segredo mais adequados para aplicação na Dimensão de Proteção do Segredo.

A Figura 40 apresenta as Macro Atividades descritas.

Figura 40- As Macro Atividades



Fonte: Elaboração da autora, 2016.

Uma vez descritas as Macro Atividades, elaborou-se o *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID, orquestrando as principais estruturas envolvidas que são: as Macro Atividades *Controle*, *Monitoramento*, *Inteligência e Contra-Inteligência*; e as Dimensões de Proteção do Segredo *Pessoas*, *Processos*, *Tecnologia*, *Gestão Organizacional*, *Cultura* e *Artefatos de Conhecimento*.

Ao elaborar o *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID primou-se pela simplicidade da sua forma ao conjugar estruturas, conceitos e atividades inerentes ao seu propósito, como apresentado na Figura 41.

Figura 41 - *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID

Fonte: Elaboração da autora, 2016.

O *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID se apresenta delimitado com um anel composto pelas Macro Atividades que atuam na perspectiva agregadora de ações que visam a segurança do segredo. São elas: Monitoramento, Controle, Contra-Inteligência e Inteligência. Como representado, estas Macro Atividades são dinâmicas, interagem entre si e envolvem o hexágono formado pelas Dimensões de Proteção do Segredo.

Na estrutura formada pelas Dimensões de Proteção do Segredo *Pessoas*, *Processos*, *Tecnologia*, *Gestão Organizacional*, *Cultura* e

Artefatos de Conhecimento são aplicados os Instrumentos de Proteção do Segredo.

Ainda mais segregado e encapsulado no hexágono formado pelas Dimensões de Proteção do Segredo, isto é, no núcleo do *framework*, encontra-se o *Segredo*, cuja segurança é a razão deste *framework*.

As Dimensões de Proteção do Segredo, descritas na seção 6.3, abrangem aspectos fundamentais de uma organização que, se não geridos adequadamente, podem possibilitar que a segurança do segredo seja comprometida.

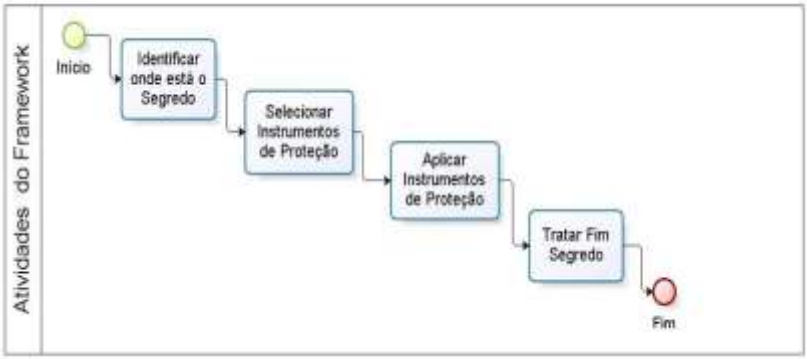
A seleção dos Instrumentos de Proteção do Segredo ocorre de forma específica para cada Dimensão de Proteção do Segredo, porém um mesmo instrumento pode ser aplicado em mais de uma dimensão, conforme a Matriz de Aplicação dos Instrumentos de Proteção do Segredo (Seção 6.5).

A aplicação dos Instrumentos de Proteção do Segredo nas Dimensões de Segurança do Segredo poderá causar efeito sinérgico e resultar no fortalecimento da segurança do segredo.

7.6.5 Sequência das Atividades do *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID

O *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID é coeso e abstrai atividades importantes para a sua utilização. As atividades, bem como a sequência para a execução são apresentadas na Figura 42.

Figura 42 – Atividades do *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID



Fonte: Elaboração da autora, 2016.

A primeira atividade - *Identificar onde está o Segredo* representa ações de Inteligência e Contra-Inteligência que devem ser conduzidas, com a devida discrição, para produzir informações e conhecimentos sobre o segredo, tais como: localização; fonte; tipo de armazenamento; pessoas envolvidas; possíveis ações para dificultar engenharia reversa e espionagem industrial; estratégias e iniciativas de inteligência competitiva de concorrentes; e outras.

No seio destas ações, especial atenção deve ser dada aos recursos humanos. Segundo Nascimento (2008) os recursos humanos são considerados o elo mais frágil da corrente, em função de características de subjetividade, como sentimentos; necessidades; motivações; expectativas; e diferenças individuais.

As ações de Inteligência e Contra-Inteligência, entre outras atribuições, monitoram os ambientes interno e externo, as relações formais e informais com outras organizações, eventos e congressos, evoluções tecnológicas, novas tecnologias e diretrizes do MD.

Nesta atividade, para as ações de GR são considerados os ambientes externo à BID e o ambiente interno, delimitado pela abrangência das Dimensões de Proteção do Segredo. Convém que as ações de GR empreguem, para cada *Dimensão* de *Proteção* do *Segredo*, os princípios e processos descritos na NBR-ISO-31000 (2009) para identificar os fatores de riscos; identificar, analisar e avaliar os riscos; estimar as probabilidades dos riscos se concretizarem, bem como os impactos que poderão causar.

Ao seu final, esta atividade deve emitir relatório contendo a identificação do segredo a ser protegido, contendo os riscos identificados em cada Dimensão de Proteção do Segredo, a probabilidade da ameaça se concretizar e o impacto que poderá causar ao segredo. Os riscos deverão ser apresentados em ordem prioridade, que pode ser obtida pela ponderação da probabilidade e do impacto.

De forma sintética o Quadro 22 exemplifica parte do relatório produzido ao final da execução da atividade *Identificar onde está o Segredo*. Estas informações constituem o insumo para a atividade *Selecionar Instrumentos de Proteção*.

Quadro 22 – Exemplo do Relatório da Atividade *Identificar onde está o Segredo*

Relatório de Identificação do Segredo				
Descrição do segredo:				
Dimensão de Proteção do Segredo	**Riscos**	**Probabilidade**	**Impacto**	**Prioridade**
Dimensão 1	Risco a	30%	Alto	1
Dimensão 1	Risco b	50%	Médio	2
Dimensão n	Risco n	N%	Baixo	N

Fonte: Elaborado pela autora, 2016.

Na segunda atividade - *Selecionar Instrumentos de Proteção* são identificados os Instrumentos de Proteção do Segredo mais adequados para serem aplicados nas Dimensões de Proteção do Segredo.

Para que a escolha dos Instrumentos de Proteção do Segredo seja assertiva, devem ser seguidos os passos:

- Analisar as informações produzidas pela primeira atividade - *Identificar onde está o Segredo*.
- Consultar a descrição dos Instrumentos de Proteção do Segredo (seção 6.4)
- Consultar a Matriz de Aplicação dos Instrumentos de Proteção do Segredo (seção 6.5).

Durante esta atividade devem ser observadas características de pertinência, validade, abrangência e complementariedade dos Instrumentos de Proteção do Segredo.

Após a escolha dos Instrumentos de Proteção do Segredo mais adequados, devem ser elaboradas e emitidas recomendações pertinentes à aplicação dos Instrumentos de Proteção do Segredo nas Dimensões de Proteção do Segredo.

Na terceira atividade - *Aplicar Instrumentos de Proteção*, para cada Dimensão de Proteção do Segredo e cada Instrumento de Proteção do Segredo escolhido na atividade anterior, são adotadas as providências e ações necessárias para que o instrumento exerça a efetiva proteção do segredo.

Podemos assim dizer que o término da atividade - *Aplicar Instrumentos de Proteção* caracteriza o início o tratamento do(s) risco(s) identificado(s) na atividade - *Identificar onde está o Segredo*.

Recomendamos que, para facilitar as Macro Atividades Controle e Monitoramento sejam registrados em sistema de informação informações dos Instrumentos de Proteção do Segredo aplicados, tais como: identificação; data de aplicação; Dimensão de Proteção do Segredo onde foi aplicado; local da aplicação do instrumento; responsável pela aplicação do instrumento; validade da aplicação do instrumento; e outros.

A última atividade - *Tratar fim do Segredo* representa as ações adotadas quando do término do período de vigência dos Instrumentos de Proteção do Segredo adotados.

8 CONCLUSÕES

Neste trabalho, o levantamento bibliográfico realizado nas buscas das bases de teses e dissertações da CAPES e do IBICT revelou o ineditismo do tema de pesquisa e do desenvolvimento de uma pesquisa em um programa Interdisciplinar, além do pouco envolvimento da academia nos estudos de Defesa e a pouca massa crítica para os assuntos de Defesa e BID.

Tais revelações foram comprovadas ao realizar a busca com os argumentos de pesquisa *Segurança do Segredo*, pois a busca não encontrou registro nas bases. Na busca com os argumentos *Defesa Nacional, Indústria de Defesa, Base Logística de Defesa e Base Industrial de Defesa* que revelou a concentração das discussões na área da Ciência Política e no tema Defesa Nacional. Na busca realizada com os argumentos *Indústria de Defesa, Base Logística de Defesa e Base Industrial de Defesa*, retornou oito registros, sendo uma tese e sete dissertações, porém, nenhum dos trabalhos publicados abordou a proteção do Conhecimento ou instrumentos de proteção, ou melhor, nenhum conceito próximo à proteção do segredo, como proteção do conhecimento, segurança do conhecimento, proteção da informação ou segurança da informação.

A escolha do tema se deu ao considerarmos uma série de fatores, tais como: Primeiro, entender a necessidade de fortalecimento da BID com as condições seguras para inovar em seu ambiente de produção e atender as demandas das FA, a precariedade dos equipamentos das FA e a necessidade de modernização dos equipamentos e produtos utilizados pelas FA, a capacidade de ter produtos de defesa adequados para fazer frente às ameaças aos interesses de Defesa Nacional, o que despertou o interesse no Ambiente de Inovação da BID.

Segundo o entendimento de que o Desenvolvimento da BID promove o desenvolvimento econômico do país e a diminuição da dependência tecnológica estrangeira.

Desafiados a adentrar na complexidade que envolve a BID e seu ambiente de inovação, o que despertou a necessidade de contribuir para os conhecimentos realizando a pesquisa no ambiente de inovação BID, e aproveitar a experiência da pesquisadora para pesquisar como os instrumentos de proteção poderiam proteger o segredo nesse ambiente, garantindo a novidade para a Inovação.

Os achados desta pesquisa se deram ao longo do percurso percorrido para alcançar o objetivo geral de propor o *Framework* de

Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID, e os objetivos específicos são descritos a seguir.

No capítulo 4, para alcançar o objetivo específico de *Apresentar um conjunto de termos e definições e harmonizá-los para a definição do termo "segredo" no Ambiente de Inovação da BID*, se fez necessário elaborar um conjunto de terminologias próprias para esta tese, que considerou três ambientes específicos onde os termos informação e conhecimento ganharam especificidades próprias para atender a terminologia requerida em cada ambiente. A fundamentação teoria elaborada para esta tese, foi essencial para identificar na literatura os instrumentos de proteção para o segredo.

As principais contribuições da tese vinculadas ao alcance deste objetivo foram a definição de novos termos, devidamente caracterizados por meio de representações gráficas que descreveram a transformação dos termos básicos e seus relacionamentos em novos termos específicos para este estudo, são eles: INFORMAÇÃO DE DEFESA, CONHECIMENTO DE DEFESA e SEGREDO.

Para a definição dos novos termos, apresentamos o Ambiente Externo, que envolve o Ambiente de Defesa e representa tudo que está fora das fronteiras do Ambiente de Defesa. No ambiente externo se localizam outros órgãos da APF, empresas, universidades, a sociedade e as nações. As relações e interações entre os ambientes representados não foram alvo desta pesquisa. A ênfase recaiu sobre o fluxo de informação e conhecimento.

No domínio do Ambiente de Defesa se localizam *stakeholders* como o MD e as FA bem como as políticas e estratégias de defesa. Se destacou neste ambiente a atividade de Inteligência que produz Informações e Conhecimentos de Defesa a partir de insumos internos e externos ao Ambiente de Defesa, a atividade de Contra-Inteligência que empreende ações que visam salvaguardar o conhecimento de qualquer ameaça externa e o Segredo.

Se delimitou dentro do Ambiente de Defesa o Ambiente da BID, onde se encontram as Indústrias de Defesa, setores do MD e os ICT das FA. A atividade de Inteligência no Ambiente da BID recebe insumos da atividade de Inteligência do Ambiente de Defesa. No domínio da BID também são representados os segredos que lhe são inerentes e a atividade de Contra-Inteligência.

O Ambiente de Inovação da BID se encontra mais segregado no interior do Ambiente da BID. O fluxo de Informações e Conhecimentos de Defesa para a BID juntamente com o *Know How* e conhecimentos

protegidos da indústria originam o segredo no Ambiente de Inovação da BID.

Cabe destacar que, ao trazer as atividades de Inteligência e Contra-Inteligência, oriundas da Doutrina de Inteligência de Defesa, para estudos acadêmicos fora da academia militar abrem novas linha de pesquisa e espaço de discussão, além do desenvolvimento de pesquisas que contribuam para o avanço do conhecimento e formação de massa crítica e de pesquisadores especialistas.

O capítulo 5 visou alcançar o objetivo específico de *Apresentar o Sistema Sociotécnico para a BID para entender as influências entre subsistema técnico e o subsistema social, bem como as relações com o ambiente externo*. O modelo Sociotécnico de Tavistock fundamentou a concepção do Sistema Sociotécnico para a BID. Foram concebidos os dois subsistemas, o Técnico e o Social, que estruturam o modelo.

O subsistema técnico que compreende as tarefas a serem desempenhadas; as instalações físicas; os equipamentos e instrumentos utilizados; as exigências da tarefa; as utilidades e técnicas operacionais; o ambiente físico; e a operação das tarefas, é o responsável pela eficiência potencial. Assim, identificamos como estrutura do subsistema o Ministério da Defesa, as Indústrias de Defesa; as Instituições de Ciência e Tecnologia das Forças Armadas; a academia; e o Plano de Articulação e Equipamento de Defesa.

O subsistema social que compreende as pessoas, as relações sociais entre os indivíduos, e as exigências de trabalho. cabendo a ele a transformação da eficiência potencial em eficiência real. Os principais agentes e as exigências de trabalho, contidas em dispositivos legais e doutrinas,

Uma vez que os subsistemas estão interagindo e sendo mutuamente influenciados, ocorre, de forma contínua, a conversão dos insumos importados em produtos para serem exportados. Assim, foi elaborado o SISTEMA SOCIOTÉCNICO PARA A BID, que representa as relações e interações entre o subsistema técnico e o subsistema social, bem como as relações com o ambiente externo.

No Capítulo 6 alcançamos o objetivo específico de *Caracterizar o Ambiente de Inovação da BID, considerando a atuação dos agentes de C,T&I e os ciclos de vida dos produtos de Defesa de cada FA.*

O caminho percorrido para o desenvolvimento deste capítulo contou com a caracterização da estrutura da BID; o levantamento dos projetos estratégicos de cada FA, que norteiam as ações de produção de Defesa; a identificação dos ambientes de CT&I e seus respectivos Ciclos de Vida dos Produtos. Como achados desta fase da pesquisa elencamos a

CONSOLIDAÇÃO DOS CICLOS DE VIDA DOS PRODUTOS DAS FA AGRUPADOS POR FASE; a elaboração e detalhamento das FASES DO AMBIENTE DE PRODUÇÃO DO PRODE; e a elaboração do MODELO DE PRODUÇÃO PARA O AMBIENTE DE INOVAÇÃO DA BID.

Como descrito no capítulo, gerir a inovação no setor de Defesa significa conjugar vários sistemas sem interface e segregados (fragmentado e desarticulado). O que foi constatado desde o momento da coleta de dados bibliográficos e documental, quando encontramos as informações dispersas e proprietárias nos diversos órgãos pesquisados.

A observação do Ambiente de Inovação da BID sob a ótica dos Sistemas de Produtos Complexos permitiu perceber como os bens, os produtos e os serviços que compõem o PRODE envolvem alta tecnologia, alto custo, e capacitação específica.

A favor do interesse de Defesa, o sigilo envolve as Fases de Produção e as pesquisas desenvolvidas, e caracteriza o Ambiente de Inovação da BID como Ambiente de Inovação Fechada.

A falta de harmonização de termos e definições para descrever as fases de produção do ciclo de vida dos PRODE das FA, nos levou a análise de cada ciclo. Foi possível, então, identificar as fases comuns e agrupá-las por atividades semelhantes. O resultado forneceu uma visão ampla e única para as Fases de Produção do PRODE.

Assim, concebemos o Modelo de Produção para o Ambiente de Inovação da BID que caracterizou o Ambiente de Inovação da BID representando as relações e interações do Ambiente de Defesa e do Ambiente de Inovação da BID, onde se executam as Fases de Produção do PRODE.

O Capítulo 7 visou atender o objetivo específico de *Elaborar um framework que represente a aplicação dos instrumentos de proteção do segredo no Ambiente de Inovação a BID*.

Para elaborar do *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID foi necessário definir novos termos e conceitos para atender a complexidade inerente ao Ambiente de Inovação da BID, são eles: Os INSTRUMENTOS DE PROTEÇÃO DO SEGREDO, as DIMENSÕES DE PROTEÇÃO DO SEGREDO; assim como construir a MATRIZ DE APLICAÇÃO DOS INSTRUMENTOS DE PROTEÇÃO DO SEGREDO.

Foi essencial o entendimento de que a *proteção* compreende o conjunto de ações adotadas para a defesa do *segredo*, e que a *segurança* representa o estabelecimento de condições que neutralizem potenciais ameaças ao *segredo*.

Os Instrumentos de Produção do Segredo foram selecionados a partir das pesquisas documentais e bibliográficas realizadas nesta tese. Eles representam o conjunto de instrumentos de natureza própria que têm por finalidade mitigar riscos ao Segredo do Ambiente de Inovação da BID e são aplicáveis nas Dimensões de Proteção do Segredo. Então, definimos Instrumento de Proteção do Segredo, como *objeto que contém recomendações aplicáveis às Dimensões de Proteção do Segredo com a finalidade de salvaguardar o segredo*.

Definimos Dimensões de Proteção do Segredo as dimensões do conhecimento, que representam *áreas específicas dentro da organização, que requerem atenção quanto à proteção sob a ótica do segredo*. Foram consideradas as dimensões da GC referenciadas no trabalho e a especificidade exigida para a aplicação de Instrumentos de Proteção do Segredo, e adotados como as Dimensões de Proteção do Segredo: Pessoas, Processos, Tecnologia, Gestão Organizacional, Cultura e Artefatos do Conhecimento.

De posse dos dois elementos mencionados acima, foi elaborada a Matriz de Aplicação dos Instrumentos de Proteção do Segredo com o objetivo de apresentar os Instrumentos de Proteção do Segredo considerados os mais adequados para serem aplicados na Dimensão de Proteção do Segredo.

Neste ponto, a experiência da pesquisadora foi necessária para detectar a necessidade de outros elementos para exercerem atividades de identificação e neutralização das potenciais ameaças ao segredo, e garantir a segurança para o Ambiente de Inovação da BID. Foram definidas as Macro Atividades de *Controle; de Monitoramento; de Inteligência e Contra-Inteligência*; e *Gestão de Riscos.*

Por fim, alcançamos o objetivo geral desta tese, qual seja, propor o *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID. Primou-se pela simplicidade da sua forma ao conjugar estruturas, conceitos e atividades inerentes ao seu propósito.

O *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID está delimitado com um anel composto pelas Macro Atividades que atuam na perspectiva agregadora de ações que visam a segurança do segredo. Este anel envolve o hexágono formado pelas Dimensões de Proteção do Segredo, onde são aplicados os Instrumentos de Proteção do Segredo.

Ainda mais segregado e encapsulado no hexágono formado pelas Dimensões de Proteção do Segredo, isto é, no núcleo do *framework*, encontra-se o *Segredo*, definido como: *o conjunto de Informação de*

Defesa e de Conhecimento de Defesa, inclusive os artefatos de conhecimentos, que em função da criticidade, do valor que possui e da importância estratégica é classificado como sigiloso ou de acesso restrito, e que não pode ser de domínio público, pois envolve novidade, segredos e direitos de propriedade industrial da BID; e é passível de proteção, por instrumentos legais e administrativos e por atividades de Inteligência e Contra-Inteligência.

Ainda como considerações, cabe destacar que no escopo desta pesquisa o sigilo inerente aos assuntos de interesse de Defesa limitou a identificação dos instrumentos de proteção do segredo adotados no Ambiente da BID nacional; o sigilo que envolve os negócios e a produção dos PRODE impediu a divulgação de informações e conhecimentos, e restringiu a realização de entrevistas. Os encontros realizados com consultores da área de Defesa, não foram formalizados nem gravados a pedido dos mesmos, mas foram importantes para nortear as decisões tomadas durante a pesquisa. Os livros publicados sobre Indústria de Defesa são de origem estrangeira e retrata a realidade de outros países, que diferem da realidade da BID nacional.

Outras considerações importantes sobre a pesquisa foram a revisão que está ocorrendo nas políticas e estratégias que norteiam as atividades da BID; a rara literatura sobre a proteção do conhecimento no âmbito da GC; o aspecto cultural de tratar de forma reservada dos assuntos inerentes a Defesa; as estruturas de Defesa são desconexas e atuam de forma isolada; pouca participação da academia nos assuntos de Defesa; a inexistência de modelo de ciclo de vida de PRODE comum ao ambiente da BID.

Concluindo, a Tese apresentou como aplicar os Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID, propondo o *Framework* de Aplicação dos Instrumentos de Proteção do Segredo no Ambiente de Inovação da BID.

Nas áreas de Estudos de Defesa e Gestão do Conhecimento, esta tese representa uma pesquisa inédita realizada em um Programa Interdisciplinar, e contribui para o avanço do conhecimento. Desenvolver a tese na linha de pesquisa Teoria e Prática de GC permitiu a introdução de um novo ambiente de discussão para os estudos de GC no PPGEGC/UFSC.

Esta tese não esgota a intensão de produzir novos conhecimentos sobre a segurança do segredo no ambiente de inovação da BID e na área de GC.

Portanto, sugerimos como pesquisas futuras a atualização dos Instrumentos de Proteção do Segredo e da Matriz de Aplicação; bem

como a revisão das Dimensões de Proteção do Segredo, enriquecendo o acervo de Instrumentos de Proteção do Segredo e das diretrizes.

Considerar outras áreas das Ciências Sociais e de outras Ciências, como as Ciências Extadas, representa uma oportunidade de trabalhos futuros para pesquisadores de outros progamas. Sugere-se incluir no acervo de Instrumentos de Proteção do Segredo os instrumentos da ciberdefesa e da certificação digital.

Outra recomendação, recai na GC, que tem acentuada em sua natureza o compartilhamento do conhecimento, e amadurecer o processo de proteção do conhecimento.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. Programa Nacional de Proteção ao Conhecimento. **O que é o PNPC**. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/?tac=229>. Acesso em: 20 setembro 2015.

ALVARENGA NETO, R. C. D. de. **Gestão do conhecimento em organizações: proposta de mapeamento conceitual integrativo**. São Paulo: Saraiva, 2005.

AMARAL, Sérgio Ferreira do; PRETTO, Nelson de Luca (Orgs). **Ética, hacker e educação.** Campinas/SP. FE/UNICAMP, 2009

ARAÚJO, Wagner Junqueira de. **A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento.** 2009. Tese (Doutorado) - Universidade de Brasília - Departamento de Ciência da Informação e Documentação, Brasília, 2013.

ARÍS, Enrique Paniagua (ORG.) ***La Gestión Tecnológica del Conocimento***. Universidad de Murcia – Espanha: Editora Editum, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 13789**: Terminologia – Princípios e métodos – Elaboração e apresentação de normas de terminologia. ABNT: Rio de Janeiro, 1997.

_____. **ABNT NBR 11515**: Guia de práticas para segurança física relativas ao armazenamento de dados. ABNT: Rio de Janeiro, 2007.

_____. **ABNT ISO 31000**: Gestão de riscos – Princípios e diretrizes. ABNT: Rio de Janeiro, 2009.

_____. **ABNT NBR ISO/IEC 27005**: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. ABNT: Rio de Janeiro, 2011.

_____. **ABNT NBR 16167**: Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação. ABNT: Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27002**: Tecnologia da informação – Técnicas de segurança - Código de prática para controles de segurança da informação. ABNT: Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DAS INDÚSTRIAS DE MATERIAIS DE DEFESA E SEGURANÇA (ABIMDE); FUNDAÇÃO INSTITUTO DE PESQUISAS ECONÔMICAS (FIPE). **Cadeia de valor e importância socioeconômica da indústria de defesa e segurança no Brasil.** São Paulo, 2015. Disponível em: < http://www.abimde.org.br/index.php/downloads/files/40>. Acesso em: 3.jun.2015.

AWAD, E. & GHAZIRI, H. . ***Knowledge Management***. *Prentice Hall, Upper Saddle River, New Jersey,* 2004.

BARBOSA, Denis Borges. **Uma introdução à propriedade intelectual**. 2. ed. Rio de Janeiro: Lúmen Júris, 2003., 2008. 2008.

BARONE, Daniela Marcos. **A proteção internacional do segredo industrial**. 2009. 134f. Dissertação (Mestrado em Direito) – Faculdade de Direito – Universidade de São Paulo. São Paulo, SP, 2009.

BARRAL, Welber; PIMENTEL, Luiz Otávio (Orgs.). **Propriedade intelectual e desenvolvimento**. Florianópolis: Fundação Boiteux, 2005.

BEM, Roberta Moraes. JUNIOR, Divino Inácio Ribeiro. **A gestão do conhecimento dentro das organizações: a participação do bibliotecário.** Revista ACB: Biblioteconomia em Santa Catarina, (Brasil) - ISSN 1414-0594. *v. 11, n. 1 (2006), p. 75-82. ISSN 1414-0594* Florianópolis/SC. Disponível em: <http://revista.acbsc.org.br/racb/article/view/468>. Acesso em: 8 abril 2015.

BEM, Roberta Moraes de . ***Framework*** **de gestão do conhecimento para bibliotecas universitárias**. 2015. 344 f.. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis, SC, 2015.

BOCCHINO, L. de O.; OLIVEIRA, M. C. C. de; MAIA, M. S.; PARMA, Nilto; JELITA, R. R. R. Von; MACHADO, R. F.; PENA, R.

M. V. Propriedade Intelectual Conceitos e Procedimentos, **Publicações da Escola da AGU**, Brasília, ano 2, n. 06, 2010.

BOCCHINO, Leslie de Oliveira Bocchino. **Proteção legal do conhecimento organizacional: uma abordagem de padrões de projeto**. 2012. 232f. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis, SC, 2012.

BOLISANI, E. ; PAIOLA, M. ; SCARSO, E. . ***Knowledge protection in knowledge-intensive business services.*** Journal of Intellectual Capital, 14 (2), pp. 192-211. 2013.

BORGES, M. E. N.; CAMPELLO, B. S. **A organização da informação para negócios no Brasil**. Perspectivas da Ciência da Informação, v. 2, n. 2, p. 149-161, 1997.

BOTELHO, L. L. R.; CUNHA, C. C. A.; MACEDO, M. **O método da revisão integrativa nos estudos organizacionais**. Gestão e Sociedade**,** v. 5, n. 11, p. 121-136, 2011.

BRASIL Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Disponível em: 168 Acesso em: 15 mai. 2014.

_____. Governo Federal. **Lei n. 9.279, de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF, 1996.

_____. _____. **Lei nº 9.456, de 25 de abril de 1997**. Institui a Lei de Proteção de Cultivares e dá outras providências. Brasília, DF, 1997.

_____. _____. **Lei nº 9.610 de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF, 1998 a.

_____. _____. **Lei nº 9.609 de 19 de fevereiro de 1998**. Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país e dá outras providências. Brasília, DF, 1998b.

_____. _____. **Decreto Nº 2.553, de 16 de abril de 1998**. Regulamenta os arts. 75 e 88 a 93 da Lei nº 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativos à propriedade industrial. Brasília, DF, 1998c.

_____. _____. **Lei Complementar No. 97, de 9 de junho de 1999.** Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, DF, 1999a.

_____. _____. **Lei nº 9.883, de 7 de dezembro de 1999**, estabelece a competência da ABIN. Brasília, DF. 1999b.

_____. _____. **Decreto-lei Nº 3.505, de 13 de junho de 2000.** Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Diário Oficial República Federativa do Brasil, Brasília, DF, 24 jun. 2000.

_____. Ministério da Defesa. **Portaria Normativa Nº 764/MD, de 27 de dezembro de 2002**. Aprova a Política e as Diretrizes de Compensação Comercial, Industrial e Tecnológica do Ministério da Defesa. Brasília, DF, 2002.

_____. Ministério da Ciência e Tecnologia. **Concepção Estratégica: Ciência, Tecnologia e Inovação de Interesse da Defesa Nacional**. Brasília, DF, 2003a.

_____. _____. **Gerenciando projetos no Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa Nacional**. Brasília, DF, 2003b.

_____. Ministério da Defesa. **Portaria Normativa Nº 1.317/MD, de 4 de novembro de 2004**. Aprova a Política de Ciência, Tecnologia e Inovação (C,T & I) para a Defesa Nacional. Brasília, DF, 2004a.

_____. Governo Federal. **Lei nº 10.973, publicada em 2 de dezembro de 2004**. Lei da Inovação. Brasília, DF, 2004b.

_____. _____. Decreto nº 5.484, de 30 de junho de 2005. **Política de Defesa Nacional (PDN).** Brasília, DF, 2005a.

_____. Ministério da Defesa. Portaria Normativa nº 899/MD, de 19 de julho de 2005. **Política Nacional da Indústria de Defesa (PNID**). Brasília, DF, 2005b.

_____. _____. **Portaria Nº 611/MD, de 12 de maio de 2005**. Instituiu a Comissão Militar da Indústria de Defesa – CMID. Brasília, DF, 2005c.

_____. Governo Federal. **Lei, nº 11.484, de 31 de maio de 2007**. Dispõe sobre os incentivos às indústrias de equipamentos para TV Digital e de componentes eletrônicos semicondutores e sobre a proteção à propriedade intelectual das topografias de circuitos integrados, instituindo o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores – PADIS e o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Equipamentos para a TV Digital – PATVD; altera a Lei no 8.666, de 21 de junho de 1993; e revoga o art. 26 da Lei no 11.196, de 21 de novembro de 2005. Brasília, DF, 2007a .

_____. Ministério da Defesa**. Portaria Normativa Nº 777/MD, de 31 de maio de 2007**. Institui a Comissão de Implantação do Sistema de Certificação, Metrologia, Normalização e Fomento Industrial das Forças Armadas e dá outras providências. Brasília, DF, 2007b.

_____. Ministério do Desenvolvimento, Indústria e Comércio Exterior. 12 de maio de 2008. **Política de Desenvolvimento Produtivo (PDP)**. Brasília, DF, 2008a.

_____. Governo Federal. **Decreto Nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, DF, 2008b.

_____. Estado-Maior da Armada. EMA-410 – **Plano de desenvolvimento Científico-tecnológico e de Inovação da Marinha** (PDCTM). Brasília, DF, 2009.

_____. Ministério da Defesa. Comando da Aeronáutica. **ICA 400-31 – Logística. Gerenciamento do ciclo de vida de sistemas e materiais do SISCEAB**. 2010a.

_____. _____. **Portaria Normativa Nº 1797, de 25 de novembro de 2010**. Estabelece a Missão e Visão do Ministério da Defesa. Brasília, DF, 2010b.

_____. Governo Federal. **Lei n. 12.527, de 18 de novembro de 2011**. Lei de acesso à informação. Brasília, DF, 2011.

_____. _____. Lei nº 12.598, de 22 de março de 2012. **Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa [...] (RETID),** Brasília, DF, 2012a.

_____. _____. **Decreto-lei Nº 7.845, de 14 de novembro de 2012.** Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Diário Oficial República Federativa do Brasil, Brasília, DF, 16 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>. Acesso em: 8 fev.2014.

_____. _____. **Livro Branco de Defesa Nacional**. Brasília, DF, 2012c.

_____. _____. **Decreto Nº 7.970, de 28 de março de 2013**. Regulamenta dispositivos da Lei nº 12.598, de 22 de março de 2012, que estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e sistemas de defesa, e dá outras providências. Brasília, DF, 2013a.

_____. _____. **Decreto nº 7.974, de 1o de abril de 2013**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Defesa. Brasília, DF, 2013b.

_____. _____. **Decreto Nº 8.122, de 16 de outubro de 2013**. Regulamenta o Regime Especial Tributário para a Indústria de Defesa - Retid, instituído pela Lei nº 12.598, de 22 de março de 2012. Brasília, DF, 2013c.

_____. Ministério da Defesa. **Portaria Normativa Nº 3.214, de 26 de novembro de 2013.** Dispõe sobre a organização e o funcionamento da

Comissão Mista da Indústria de Defesa, criada pelo Decreto nº 7.970, de 28 de março de 2013c.

_____. Receita Federal, RFB. **Instrução Normativa RFB Nº 1.454, de 25 de fevereiro de 2014.** Dispõe sobre a aplicação do Regime Especial Tributário para a Indústria de Defesa (Retid). Brasília, DF, 2014.

_____. Ministério da Defesa. **Relação Geral das Empresas Cadastradas como ED & EED**. Atualizado em: 31/07/2015. Disponível em: <http://www.defesa.gov.br/arquivos/industria_de_defesa/cmid/publicacoes_dos_credenciamentos_no_dou.pdf>. Acesso em: 10 março 2015a.

_____. Senado Federal. **Ata da 33ª Reunião da Comissão de Relações Exteriores e Defesa Nacional**, Ordinária, da 1ª Sessão Legislativa Ordinária, da 55ª Legislatura, realizada em 17 de setembro de 2015. Brasília, DF, 2015b.

_____. Ministério da Defesa. Disponível em: < http://www.defesa.gov.br/ >. Acesso em: 7.jan.2015c.

_____. Governo Federal. **Lei nº 13.243, de 11 de janeiro de 2016**. Dispõe sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação e altera a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 6.815, de 19 de agosto de 1980, a Lei nº 8.666, de 21 de junho de 1993, a Lei nº 12.462, de 4 de agosto de 2011, a Lei nº 8.745, de 9 de dezembro de 1993, a Lei nº 8.958, de 20 de dezembro de 1994, a Lei nº 8.010, de 29 de março de 1990, a Lei nº 8.032, de 12 de abril de 1990, e a Lei nº 12.772, de 28 de dezembro de 2012, nos termos da Emenda Constitucional no 85, de 26 de fevereiro de 2015.

BRICK, E.S. **Base Logística de Defesa**. In: Anais do V Encontro Nacional da Associação Brasileira de Estudos de Defesa. Fortaleza. ago. 2011.

BUKOWITZ, W.R.; WILLIAMS, R.L. **Manual de Gestão do Conhecimento.**Tradução Carlos Alberto Silveira Netto Soares. Porto Alegre. 2002.

BRUSTOLIN, Vitelio Marcos. **Inovação e desenvolvimento via Defesa Nacional nos EUA e no Brasil.** 2014. 169f. Tese (Doutorado em Ciências) - Instituto de Economia da Universidade Federal do Rio de Janeiro, com estágio doutoral na Universidade Harvard. Rio de Janeiro, RJ. 2014.

CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. **Documento de Área – Ano 2013**. Disponível em:<http://capes.gov.br/images/stories/download/avaliacaotrienal/Docs_de_area/Interdisciplinar_doc_area_e_comiss%C3%A3o_block.pdf> . Acesso em: 20ago. 2014.

CAPURRO, Rafael; HJORLAND, Birger. **O Conceito da Informação**. Perspectivas em Ciência da Informação, v.12, n.1, p. 148-207, jan/abr. 2007. Disponível em: < http://bogliolo.eci.ufmg.br/downloads/CAPURRO.pdf>. Acessado em: 22/abril/2015.

CARDORI, Aluízia Aparecida**. A gestão do conhecimento aplicada ao processo de transferência de resultados de pesquisa de instituições federais de ciência e tecnologia para o setor produtivo: processo mediado pelo núcleo de inovação tecnológica**. 2013. 465 f.. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis. 2013.

CARDOSO, Ana Maria Pereira. P**ós-modernidade e informação: conceitos complementares?**. Perspectiva em Ciência da Informação. Belo Horizonte, v. 1, n.1, p. 63-79, jan/jun. 1996.

CARVALHO, Isami Machado de. **A dinâmica dos mecanismos de proteção e compartilhamento de conhecimento, no processo de desenvolvimento de software, em uma empresa pública de Tecnologia da Informação (TI)**. 2014, 288f. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis. 2014.

CASTRO AA, Saconato H, Guidugli F, Clark OAC. **Curso de revisão sistemática e metanálise** [Online]. São Paulo: LED-DIS/UNIFESP;

2002. Disponível em:
URL: http://www.virtual.epm.br/cursos/metanalise.

CEPIK, Marcos. **Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência**. Rio de Janeiro: Fundação Getúlio Vargas. 2003.

CHECKLAND, P. **Systems thinking.** In: CURRIE, W. L.; GALLIERS, B. (Eds.). *Rethinking management information systems: an interdisciplinary perspective*. New York: Oxford University Press, p. 45-56, 1999.

CHESBROUGH, H. **Inovação aberta: como criar e lucrar com a tecnologia.** Porto Alegre: Bookman, 2012.

CHIAVENATO, Idalberto, **Introdução à teoria geral da administração: uma visão abrangente da moderna administração das organizações** / Idalberto Chiavenato - 7. ed. rev. e atual. - Rio de Janeiro: Elsevier, 2003 - 6' reimpressão

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

COOPER, H. M. ***The integrative research review: a systematic approach***. *Beverly Hills* (CA): *Sage Publications*, 1984.

CRESWELL, J. W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 3.ed. Porto Alegre: Artmed/Bookman, 2010.

CUNHA, M. B.; AMARANTE, J. C. A. **O livro branco e a base científica, tecnológica, industrial e logística de defesa**. Revista da Escola de Guerra Naval, Rio de Janeiro, v.17, n.1, p. 11-32, jan./jun. 2011.

DAGNINO, Renato Peixoto; FILHO, Luiz Alberto Nascimento Campos. **Análise sobre a viabilidade de revitalização da indústria de defesa brasileira**. BBR - Brazilian Business Review. Vol 4, No. 3, set/dez.2007. pp – 191-207. FUCAPE *Business School*. Vitória-ES, 2007.

DALKIR, Z. ***Knowledge Managemet in theory and practice***. 2 nd. MIT Press: Cambridge, 2011.

DAVENPORT, Thomas H. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação**. São Paulo: Futura, 1998.

DAVENPORT; PRUSAK, P. **Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual.** Rio de Janeiro: Elsevier, 2003.

DE ANDRADE MARCONI, Marina; LAKATOS, Eva Maria. **Metodologia do trabalho científico: procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos científicos**. Atlas, 2007.

DE FARIA, P. A; SOFKA, W. B. ***Knowledge protection strategies of multinational firms-A cross-country comparison.*** *Research Policy*, 39 (7), pp. 956-968. 2010.

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

DESOUZA, Kevin C. ***Managing knowledge security****, Strategies for protecting your company´s intellectual assets. London: Kogan*, 2007.

DESOUZA, Kevin C.; PAQUETTE, Scott. ***Knowledge management: An introduction***. *Neal-Schuman Publishers*, 2011.

DICIONÁRIO DO AURÉLIO ONLINE. Disponível em: < https://dicionariodoaurelio.com/>. Acesso em: 03.fev. 2015.

DING, X., LIU, H. e SONG, Y. ***Are internal knowledge transfer strategies doubleedged swords*?**. *Journal of Knowledge Management*. vol. 17, no. 1. pp. 69-86. 2013

DONATE, M.J.; e CANALES, J.I. ***A new approach to the concept of knowledge strategy.*** *Journal of Knowledge Managemen*t. vol. 16, no. 1. p. 22-44, 2012.

DRUCKER, Peter F. **Sociedade pós capitalita**. 2a. ed. São Paulo, Pioneira, 1994.

DUNNE, J.P. *The Defence Industrial Base*. pp. 399-429 in K. Hartley and T. Sandler (eds.) ***Handbook of Defence Economics***. *Amsterdam*: Elsevier, 1995.

EDVINSSON, Leif; MALONE, Michael S. **Capital intelectual: descobrindo o valor real de sua empresa pela identificação de seus valores internos**. 1998.

ESCOLA SUPERIOR DE GUERRA, ESG. **Doutrina de Inteligência de Defesa (DID) – MD52-N-01**. Brasília, DF, 2005.

_____. **Manual Básico: Elementos Fundamentais**. Volume 1, ano 2009. Reimpr. rev. Rio de Janeiro, 2011.

FIGUEIREDO, Saulo Porfírio. **Gestão do Conhecimento**: estratégias competitivas para a criação e mobilização do conhecimento na empresa. Rio de Janeiro: Quality Mark, 2005.

FILHO, Sergio, L. S. C.; BARROS, Daniel C.; CASTRO, B. H. R.; FONSECA, Paulus V. R.; GORNSZTEJN, Jaime. **Panorama sobre a indústria de defesa no Brasil**. In BNDES Setorial n. 38, p. 373-408.

FLORES, Milton César da Silva. **Da Cláusula de Sigilo nos Contratos Internacionais de Transferência de Tecnologia – Know-How**. 2006. 342p. Tese (Doutorado em Direito). Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas. Florianópolis, SC. 2006.

FONTANELA, Cristiani; DOS SANTOS, Maria Isabel A. S. **Habitats de Inovação Aberta: A Gestão do Conhecimento nos Parques Científicos e Tecnológicos**. CONPEDI, 2015.

FRANCELIN, M.M. **A epistemologia da complexidade e a Ciência da Informação.** Ciência da Informação, Brasília, v. 32, n. 2, 64-68. 2004.

FRANCO-AZEVEDO, Carlos Eduardo**. Gestão de Defesa: o sistema de inovação no segmento de não-guerra.** 2013. 423 f.. Tese (Doutorado em Administração) – Escola Brasileira de Administração Pública e de Empresas, Fundação Getúlio Vargas, Rio de Janeiro.

FREIRE, Patricia de Sá. **Engenharia da integração do capital intelectual nas organizações intensivas em conhecimento participantes de fusões e aquisições.** 2012. 354 f.. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis, 2012.

FREITAS, José Eduardo de Figueiredo; OLIVEIRA, Luiz Guilherme de. **A engenharia de sistemas e a gestão de CoPS como ferramentas da gestão de projetos complexos na área de TI**. JISTEM J.Inf.Syst. Technol. Manag. (Online), São Paulo , v. 5, n. 1, p. 15-36, 2008 . Available from <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752008000100003&lng=en&nrm=iso>. access on 10 Jan. 2016.

GALVÃO-NETTO, Argemiro. **Gestão de Ciência, Tecnologia e Inovação no Exército Brasileiro no contexto da Lei de Inovação**. 2011. 158f. Dissertação (Mestrado em Política Científica e Tecnológica) – Instituto de Geociências, Universidade Estadual de Campinas, Campinas, SP, 2011.

GANONG, L. ***Integrative Reviews of Nursing Research***. *Research in Nursing and Health*, 10. 1987: 1-11.

GIL, A.C. **Como Elaborar Projetos de Pesquisa**. 3. ed. São Paulo: Atlas, 1999.

GODOY, A. S. **Introdução à pesquisa qualitativa e suas possibilidades**. Revista de Administração de Empresas, Rio de Janeiro, v. 35, n. 2, p. 57-63, mar./abr., 1995.

GOLD, A.H.; MALHOTRA, A; SEGARS, A. 2001. ***Knowledge Management: An Organizational Capabilities Perspective***. *Journal of Management Information Systems.* vol. 18, no. 1. pp. 185-214.

GONÇALVES, Adriana Aguillera. **A proteção do conhecimento e a inovação na Universidade Estadual de Londrina**. 2012. 178f. Dissertação(Mestrado em Gestão da Informação) – Universidade Estadual de Londrina, 2012.

GONZÁLEZ-ÁLVAREZ, N.; NIETO-ANTOLÍN, M. ***Appropriability of innovation results: An empirical study in Spanish manufacturing firms.*** *Technovation*, 27 (5), pp. 280-295. 2007.

GOVERNO ELETRÔNICO, GOV.BR. Disponível em: < https://www.governoeletronico.gov.br/>. Acesso em: jan. 2015.

HEISIG , P. ***Harmonisation of knowledge management – comparing 160 KM frameworks around the globe***. *Journal of Knowledge Management*, vol 13, nº 4, pp. 4-31. 2008.

HELOU, Angela Regina Heinzen Amin. **Avaliação da maturidade da gestão do conhecimento na administração pública.** 2015. 391 f.. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis. 2015.

HISLOP, D. ***Knowledge Management in Organizations - a critical introduction***. *Oxford University Press,* New York, 2005.

DAVIES, Andrew; HOBDAY, Michael. ***The business of projects: managing innovation in complex products and systems****. Cambridge University Press: United Kingdom.* 2005.

HOLSAPPLE, Clyde. ***Handbook on Knowledge Management 1****: Knowledge Matters. In: International Handbooks on Information Systems.* USA: Springer, 2003.

ILVONEN, Ilona. ***Knowledge Security – A conceptual Analysis.*** *Department of Information Management and Logistics, Thesis for Degree of Doctor of Science in Technology.* Tampere *University of Technology* – Tampere, 2013.

ISACA. **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**. ISACA, 2012.

ITSMF. *Information Technology Service Management Forum.* ***An introductory overview of*** **ITIL V3**. UK: ITSMF, 2007.

JACINTO, AMÉRICO B. M. **Gestão do Conhecimento: diretrizes organizacionais para a proteção do conhecimento**. 2008. 177f.

Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) - Universidade Católica de Brasília, Brasília, 2008.

JAPIASSU, Hilton. **Interdisciplinaridade e patologia do saber**. Rio de Janeiro, Imago, 1976.

JENNEX, M. ***Knowledge Management and Security: A Call for Research*****.** *International Journal of Knowledge Management*, Vol. 3(1), i-iv., 2007.

JULIANI, Douglas Paulesky. ***Framework*** **da cultura organizacional nas universidades para a inovação social.** 2015. 213 f.. Tese (Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina, Florianópolis, 2015.

JUNGMANN, Diana de Mello **Inovação e propriedade intelectual: guia para o docente** / Diana de Mello Jungmann, Esther Aquemi Bonetti. – Brasília: SENAI, 2010. 93 p.: il. Disponível em: <http://www.protec.ufam.edu.br/attachments/006_guia_docente_completo_indexado.pdf>. Acessado em: 4/10/2015.

JUNGMANN, Diana de Mello. **A caminho da inovação: proteção e negócios com bens de propriedade intelectual: guia para o empresário** /Diana de Mello Jungmann, Esther Aquemi Bonetti. – Brasília: IEL, 2010 125 p.: il. ISBN 978-85-87257-49-9

KELLI, A.; METS, T.; PISUKE, H.; VASAMÄE, E.; VÄRV, A. ***Trade Secrets in the Intellectual Property Strategies of Entrepreneurs: The Estonian Experience***. *Review of Central and East European Law*, 35, 315−339. 2010.

LAKATOS, E. M.; MARCONI, M. de A**. Fundamentos de metodologia científica**. 6. Ed. 5. Reimp. São Paulo: Atlas, 2007.

LASTRES, Helena Maria Martins; ALBAGLI, Sarita. **Informação e Globalização na era do conhecimento** (organizadoras) Rio de Janeiro: Campus, 1999. Disponível em: <http://www.liinc.ufrj.br/fr/attachments/055_saritalivro.pdf>. Acesso em: Jul.2014.

LIEBESKIN, Julia Porter. ***Knowledge and the Firm*** *Strategic Management Journal*, Vol. 17, *Special Issue*: (Winter, 1996), pp. 93-107.

LINDEGAARD, S. (2011). ***A revolução da inovação aberta: princípios básicos, obstáculos e habilidades de liderança.*** São Paulo: Évora.

LUCAS, L.M. *The evolution of organizations and the development of appropriate knowledge structures*. ***Journal of Knowledge Management***. vol. 14, no. 2. pp. 190201, 2010.

MAIER, R. ***Knowledge Management Systems***. 3ed. Springer-Verlag, Berlin., 2007.

MARCONI, M. de A.; LAKATOS, E. M. **Metodologia do trabalho científico:** procedimentos básicos de pesquisa bibliográfica, projeto e relatório; publicações e trabalhos científicos. 7. ed. São Paulo: Atlas, 2009. 225 p.

MASSON, Hélène. Indústrias de defesa na França e na Europa: emergência, mutação, perspectivas de evolução. Tradução do original em francês de Lis Barreto. **Revista Brasileira de Estudos de Defesa**, v. 1, n. 1, p. 147-161.2014.

MATÉ, J. L.; SILVA, A. ***Requeriments engineering for sociotechnical systems***. *London: Information Science Publishing*, 2005.

MATHEUS, Alexandre Soares**. Indústria de Defesa: uma análise da rede nacional a partir da teoria da dependência de recursos**. 2010. 121f. Dissertação (mestrado) - Escola Brasileira de Administração Pública e de Empresas, Centro de Formação Acadêmica e Pesquisa. Rio de Janeiro, RJ, 2010.

MATURANA, H. R. & VARELA, F. J. **A Árvore do Conhecimento: as bases biológicas da compreensão humana**. São Paulo: Pala Athenas, 2001

MELO, Regine de. **Indústria de Defesa e desenvolvimento estratégico: estudo comparado França-Brasil**. Fundação Alexandre de Gusmão – FUNAG, Ministério das Relações Exteriores. Brasília, DF. 2015.

MERRIAM, S. B. ***Qualitative research and case study applications in education***. *San Francisco: Jossey-Bass*. 1992.

MIRANDA, R.C. da R. O uso da informação na formulação de ações estratégicas pelas empresas. **Ciência da Informação,** Brasília, v. 28, n. 3, p. 286-292, set./dez. 1999.

MONTALLI, Katia Maria Lemos; CAMPELLO, Bernardete dos Santos. Fontes de informação sobre companhias e produtos industriais: uma revisão de literatura. **Ci. Inf.**, Brasilia , v. 26, n. 3, p. , Sept. 1997 . Available from <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19651997000300014&lng=en&nrm=iso>. access on 30 Mar. 2017. http://dx.doi.org/10.1590/S0100-19651997000300014..

MOTA, Jéssica Romeiro. **A proteção do conhecimento resultante da parceria de Pesquisa, Desenvolvimento & Inovação originado da realção universidade e empresa**. 2011. 145f. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) – Departamento de Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina,. Florianópolis/SC. 2011.

MUTA, Tarcísio Takashi. Conhecimento: intangível essencial e estratégico para o país. In **INFORME** – Revista oficial da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança. Setembro, 2014 – Edição 05, p. 38.

NASCIMENTO, Marta Sianes Oliveira do. **Proteção ao conhecimento: uma proposta de fundamentação** teórica. 2008. 181 f.. Dissertação (Mestre em Ciência da Informação) - Departamento de Ciência da Informação, Universidade de Brasília. Brasília, 2008.

NOHARA, Jouliana Jordan; ACEVEDO, Claudia Rosa. **Monografia no curso de administração:** guia completo de conteúdo e forma. 3.ed. São Paulo: Huminuras/FAPESP, 2011.

NOLD, H.A. ***Linking knowledge processes with firm performance****: organizational culture. Journal of Intellectual Capital*. Vol.13, no. 1, p.16-38, 2012.

NONAKA, I.; TAKEUCHI, H. **Criação de conhecimento na empresa: como as empresas japonesas geram a dinâmica da inovação**. Rio de janeiro: Campus, 1997.

NONAKA, Ikujiri, TAKEUCHI, H. Hirotaka. **Criação de Conhecimento na empresa. Como as empresas japonesas geram a dinâmica da inovação**. Rio de Janeiro: Editora Campus, 1995.

NONAKA, Ikujiro. ***A dynamic theory of organizational knowledge creation***. *Organization science,* v. 5, n. 1, p. 14-37, 1994.

NONAKA, Ikujiro; TOYAMA, Ryoko; NAGATA, Akiya. ***A firm as a knowledge-creating entity****: a new perspective on the theory of the firm. Industrial and corporate change,* v. 9, n. 1, p. 1-20, 2000.

NORTH, Klaus. **Gestão do conhecimento: um guia prático rumo a empresa inteligente. Rio de Janeiro: Qualitymark**, 2010.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO, OCDE. **Manual de Oslo: Proposta de Diretrizes para Coleta e Interpretação de Dados sobre Inovação Tecnológica** – com base na segunda edição de 1997. 3. ed. Rio de Janeiro: FINEP (2005).

_____. **Manual De Frascati: Metodologia proposta para definição da pesquisa e desenvolvimento experimental**. Portugal. F-Iniciativas. 2013.

OLANDER, H.; HURMELINNA-LAUKKANEN, P.; HEILMANN, P. . ***Do SMEs benefit from HRM-related knowledge protection in innovation management?.*** *International Journal of Innovation Management,* 15 (3), pp. 593-616. 2011.

PPEGC, Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento**.** Disponível em: http://egc.ufsc.br/>. Acesso em: 7 mai. 2016.

PACHECO, Roberto C. S. **EGC/UFSC: Passado, Presente e Futuro**. CIKI – IV Congresso Internacional de Conhecimento e Inovação. LOJA/Equador, 2014a.

_____. **Gestão do Conhecimento: Teoria e Prática.** Instituto de Engenharia Nuclear, Rio de Janeiro, 2014b.

PIMENTEL, Luiz Otávio. **Proteção jurídica da tecnologia e as funções do direito de patentes**. 1999. Tese (Doutorado em Direito) - Faculdade de Direito e Ciências Sociais, Universidade Nacional de Assunção, Assunção, Paraguai, 1999.

_____. **Propriedade Intelectual e Universidade: Aspectos legais**. Florianópolis: Fundação Boiteux, 2005.

_____. A propriedade intelectual como instrumento de proteção jurídica dos resultados de I+D e da inovação no agronegócio. In: FERNANDÉZ ARROYO, Diego P.; DREYZIN DE KLOR, Adriana (Dirs.). ***De CITA 10: Derecho del comercio internacional: propriedad intelectual***. Asunción: CEDEP, 2009a.

_____. Contratos: introdução aos contratos de prestação de serviços de pesquisa, parceria de pesquisa e desenvolvimento, comercialização de tecnologia e propriedade intelectual de instituições científicas e tecnológicas. In: SANTOS, Marli Elizabeth Ritter dos. et al. (Orgs.). **Transferência de tecnologia: estratégias para a estruturação e gestão de núcleos de inovação tecnológica**. Campinas, SP: Komedi, 2009b.

_____. (Org.). **Curso de propriedade intelectual & inovação no agronegócio.** 2. ed. Brasília: MAPA; Florianópolis: SEaD/UFSC/Fapeu, 2010a.

_____. (Org.). **Manual básico de acordos de parceria de PD&I.** Porto Alegre: Fortec/EdiPUCRS, 2010b.

PROBST, G.; RAUB, S.; ROMHARDT, K. **Gestão do Conhecimento: os elementos construtivos do sucesso.** Porto Alegre: Bookman, 2002.

REIS, D. R. **Gestão da inovação tecnológica**. 2ª ed. São Paulo: Manole, 2008.

RICKSON, R. E. ***Knowledge Management in Industrial Society and Environment Quality***, *in: Human Organization*, Vol 35, Nº 3, 1976, p. 239-251.

ROCHA, Adilson; BIAZZI, Fábio; TERRA, José Cláudio; SCHOUERI, Ricardo. **Proteção do Conhecimento: elemento crítico em estratégias de Gestão do Conhecimento.** [200?]. Disponível em: <http://biblioteca.terraforum.com.br/BibliotecaArtigo/libdoc00000073v002Protecao%20do%20Conhecimento-Consultores.pdf>. Acesso em: 10 set. 2014.

ROMAN, Arlete Regina; FRIEDLANDER, Maria Romana. **Revisão integrativa de pesquisa aplicada à enfermagem**. Cogitare enferm, v. 3, n. 2, p. 109-112, 1998.

ROSSI, Juliano Scherner. Proteção do know-how nos contratos de transferência de Tecnologia de defesa. **Propriedade intelectual, transferência de tecnologia e inovação** [Recurso eletrônico on-line] organização CONPEDI/UFSC; coordenadores: João Marcelo de Lima Assafim, Salete Oro Boff, Luiz Otavio Pimentel. – Florianópolis: CONPEDI, 2014. Disponível em: http://www.publicadireito.com.br/artigos/?cod=60b8b65c7b7342a9. Acesso em: 20 out. 2014.

RYAN, Julie J. C. H. ***Managing knowledge security***. *The journal of information and knowledge management systems. USA*, v. 36, n.2, p. 143-145, 2006.

SAMPIERI, Roberto Hernández et al. **Metodologia de pesquisa**. 2006.

SANDHAWALIA, B.S. & DALCHER, D. ***Developing knowledge management capabilities: a structured approach***. *Journal of Knowledge Management*. vol. 15, no. 2. pp. 313-328, 2011

SANTOS, Flávio Marcelo Risuenho; SOUZA, Richard Perassi Luiz. **O conhecimento no campo da engenharia e gestão do conhecimento.** *Perspectivas em Ciência da Informação*. v. 15, n. 1, p. 259-281, jan/abr 2010.

SCHNEIDER, U. **Management in der wissensbasierten Unternehmung.** Das Wissensnetz in und zwischen Unternehmen knüpfen, in: Schneider, U. (ed.): Wissensmanagement. Die Aktivierung des intellektuellen Kapitals, Frankfurt/Main 1996, 13-48

SERVIN, Geraud. ***ABC of Knowledge Management,*** *Freely extracted from the NHS National Library for Health at . Disponível em: http://www.library.nhs.uk/knowledgemanagement/ by Géraud Servin. Creator: NHS National Library for Health: Knowledge Management Specialist LibraryContributor: Caroline De BrúnPublication Date: July* 2005.

SHEDDEN, Piya et al. *Incorporating a knowledge perspective into security risk assessments.* ***Vine****,* v. 41, n. 2, p. 152-166, 2011.

SHEHABUDDEEN, Noordin; PROBERT, David; PHAAL, Rob; PLATTS, Ken. ***Representing and Approaching Complex Management Issues: Part 1 - Role and Definition.*** Centre for Technology Management (CTM). 1999. Publicação - *Working Paper*, No. 2000/03.

SILVEIRA, Newton. **Contrato de Transferência de Tecnologia**. São Paulo: Cadernos FUNDAP, 1985.

SINGH SANDHAWALIA, Birinder; DALCHER, Darren. ***Developing knowledge management capabilities: a structured approach.*** *Journal of Knowledge Management*, v. 15, n. 2, p. 313-328, 2011.

SIRIHAL, Adriana Bogliolo; LOURENÇO, Cíntia de Azevedo. **Informação e Conhecimento: aspectos filosóficos e informacionais.** Informação & Sociedade: estudos. João Pessoa, v. 12, n. 1, p.67-92, 2002. Disponível em: <http://www.ies.ufpb.br/ojs/index.php/ies/article/viewFile/154/148>. Acessado em:

SMITH, S.; WINCHESTER, D.; BUNKER, D. e JAMIESON, R. ***Circuits of Power: a Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization***. *MIS Quarterly.* vol. 34, no. 3. pp. 463-486. 2010.

STEIL, A. V. **Estado da arte das definições de gestão do conhecimento e seus subsistemas**. Florianópolis: Instituto Stela, 2007.Technical Report.

STETLER, C. B et al. ***Utilization-focused integrative reviews in a nursing service***. ***Appl. Nurs. Res.***, v. 11(4), pp. 195-206, 1998.

SVEIBY, Karl-Erik**.** ***A knowledge-based theory of the firm to guide in strategy formulation***. *Journal of intellectual capital*, v. 2, n. 4, p. 344-358, 2001.

SVEIBY, Karl-Erik; LLOYD, T. ***Managing Knowhow***, *London 1987.*

SVEIBY, Karl-Erik**.** *GlobalBrands - Sveiby* Associados, 2001.

TEIXEIRA, Tarcísio. **Direito empresarial sistematizado: doutrina e prática**. 2ª edição. São Paulo: Saraiva, 2013.

THIERAUF, Robert J.. ***Effective Business Intelligence Systems***. Quorum Books, Westport, 2001.

THIERAUF, Robert J.; HOCTOR James *J.* ***Smart business systems for the optimized organization***. Londres: Editora Praeger, 2003.

TIDD, J.; BESSANT, J.; PAVITT, K. **Gestão da inovação.** Porto Alegre: Bookman, 2008.

TOFFLER, Alvin**. Powershift. As mudanças do poder**. Rio de Janeiro: Editora Record, 2 edição, 1990.

UNESCO, *The United Nations Educational, Scientific and Cultural Organization. Knowledge versus information societies:* ***UNESCO report takes stock of the difference.*** *UNESCOPRES, 2005. Disponível em: <http://portal.unesco,org/en/ev.phpURL_ID=30586&URL_DO=DO_TOPIC&URL_SECTION=201.HTML>. Acesso em: 15jan.2014.*

UNIVERSIDADE DE BRAÍLIA, UnB. **Glossário da Faculdade de Ciência da Informação, da Universidade de Brasília.** Disponível em: http://www.fci.unb.br/index.php/glossario.html. Acesso em: 17.mai.2015.

VASCONCELOS, M.C.R.L.; JAMIL, G.L. **Knowledge protection: An analysis of positive and negative impacts due to knowledge leakage in Brazilian and United Kingdom enterprises [Proteção ao conhecimento: Análise dos impactos positivos e negativos do vazamento de conhecimento em empresas no Brasil e no Reino**

Unido]. Perspectivas em Ciencia da Informacao, 13 (3), pp. 96-115. 2008.

VELLOSO, João Paulo dos Reis. **O Brasil e a economia do conhecimento**, (coordenador); CARDOSO, Fernando Henrique... [et al]. Rio de Janeiro: José Olympio, 2002.

VERGARA, Sylvia Constant. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2005.

VERNON, K. D. C. (Ed.). ***Information sources in management and business.*** *London: Butterworths, 1*984. 346p.

von KROGH, G. ***Individualist and collectivist perspectives on knowledge in organizations:*** *implications for information systems research. Journal of Strategic Information Systems*. Vol. 18, p. 119-129.

_____. ***How does social software change knowledge management? Toward a strategic research agenda.*** *Journal of Strategic Information Systems,* 21 (2), pp. 154-164. 2012.

WEBER, Alan M. ***What´s So New About the New Economy?*** *Harvard Business Review*: Jan. Fev. 1993.

WIENER, N. **Cibernética**. São Paulo: EDUSP: Polígono, 1970.

WIIG, K. M. ***Management of Knowledge: Perspectives of a new Opportunity****, in: Bernold, T. (ed.): User Interfaces: Gateway or Bottleneck?, Proceedings of the Technology Assessment and Mnagement Conference of the Gottlieb Duttweiler Institute Rüschlikon/Zurich (CH), 20 – 21 October, 1986, Amsterdam 1988, 101-116.*

WORLD INTELLECTUAL PROPERTY ORGANIZATION, WIPO. **What is a trade Secret?**. Disponível em: < http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm >. Acesso em: 16. Jan.2014.

_____. Organização Mundial de Propriedade Intelectual no Brasil OMPI; Instituto Nacional de Propriedade Industrial, INPI. **DL101PBR – DL-101 Curso Geral de Propriedade Intelectual**. 2015.

ZAND, D. E. ***Managing the Knowledge Organization***, *in*: Drucker, P. (ed.): *Preparing Tomorrow´s Business Leaders Today*, USA: Englewood Cliffs (NJ), 1969, p. 112-136.

ZIBETTI, Fabíola Wüst. **A titularidade de direitos de propriedade intelectual.** In: Eliza Coral; Valéria Arriero Pereira; Carlos Eduardo N. Bizzotto. (Org.). PLATIC - Arranjo produtivo catarinense: Tecnologia da informação e comunicação. Florianópolis: Instituto Euvaldo Lodi-SC [2008].

ANEXO – EXTRATO DA DOUTRINA DE INTELIGÊNCIA DE DEFESA

As informações deste anexo foram extraídas da Doutrina de Inteligência de Defesa (BRASIL, 2005, p. 23-24)

CARACTERÍSTICAS DA DID

Termo / Conceito	Definição
Adogmática	Significa que seus preceitos são derivados de fundamentos racionais e realísticos.
Assessorial	Orientação para o exercício de uma atividade de assessoria na condução do processo decisório.
Básica	Significa que seu conteúdo enuncia princípios fundamentais e conceitos doutrinários básicos.
Dinâmica	A razão do caráter evolutivo de seus fundamentos.
Objetiva	O propósito deve ser orientado para o preparo e o emprego das Forças Armadas brasileiras.
Normativa	O conteúdo exprime preceitos orientadores do exercício da Atividade de Inteligência.
Unitária	Os preceitos determinam a unidade de pensamento e de linguagem entre os integrantes do SINDE.

CONCEITOS BÁSICOS

Termo / Conceito	Definição
Acesso	É a possibilidade ou oportunidade de uma pessoa obter conhecimento ou dado classificado. Depende, necessariamente, de uma autorização oficial emanada de autoridade competente, materializada por uma credencial de segurança, ou da superação das medidas de salvaguarda.
Autenticidade	Certificação de que o dado ou conhecimento é verdadeiro e fidedigno, tanto na origem quanto no destino.
Classificação	Atribuição, pela autoridade competente, de grau de sigilo a dado, conhecimento, documento, material, área ou instalação.
Compartimentação	Restrição do acesso com base na necessidade de conhecer.

(Continuação)

Termo / Conceito	Definição
Comprometimento	É a perda de segurança resultante do acesso não autorizado.
Conhecimento	Representação de um fato ou de uma situação, real ou hipotética, de interesse para a Atividade de Inteligência, produzido mediante a aplicação de metodologia própria.
Credencial de segurança	É o certificado concedido por autoridade competente e que habilita uma pessoa a ter acesso a assunto sigiloso, de acordo com o seu grau de necessidade de conhecimento. É o certificado que materializa o Credenciamento.
Credenciamento	Autorização oficial, concedida pela autoridade competente que habilita determinada pessoa a ter acesso a dados ou conhecimentos, nos diferentes graus de sigilo, desde que esteja caracterizada a necessidade de conhecer.
Dado	Representação de fato ou situação por meio de documento, fotografia, gravação, relato, carta topográfica e outros meios, ainda não submetido à metodologia para a produção do conhecimento.
Desclassificação	É o cancelamento, pela autoridade competente ou pelo transcurso de prazo, de classificação, tornando ostensivos dados ou conhecimentos.
Desinformação	Técnica especializada utilizada para iludir ou confundir um centro decisor, por meio da manipulação planejada de informações falsas e/ou verdadeiras, visando, intencionalmente, a induzi-lo a erro de avaliação.
Disponibilidade	É a facilidade de recuperação ou acesso a dados e a conhecimentos.
Espionagem	Ação realizada por pessoal adverso, vinculado ou não a serviço de Inteligência, visando à obtenção de conhecimento, dado sigiloso, documento ou material para beneficiar Estados, grupos de países, organizações, facções, empresas, personalidades ou indivíduos.

(Continuação)

Termo / Conceito	Definição
Fonte	É qualquer pessoa, imagem, sinal ou outro meio do qual o dado pode ser obtido.
Grau de sigilo	Gradação atribuída a dados, conhecimentos, áreas ou instalações consideradas sigilosas em decorrência de sua natureza ou conteúdo;
Integridade	Incolumidade de dados ou conhecimentos na origem, no trânsito ou no destino.
Investigação para Credenciamento	É a averiguação sobre a existência dos requisitos indispensáveis para a concessão de credencial de segurança.
Necessidade de conhecer	Condição indispensável, inerente ao exercício funcional, para que uma pessoa, possuidora de credencial de segurança, tenha acesso a conhecimento ou dado sigiloso específico, compatível com o seu credenciamento. Dessa maneira, a necessidade de conhecer constitui fator restritivo do acesso, independentemente do grau hierárquico ou do nível da função exercida pela pessoa.
Órgão de Inteligência	Organismo da estrutura de Inteligência das FA e do Ministério da Defesa.
Ostensivo	É o documento sem classificação, cujo acesso pode ser franqueado, pois não há restrição.
Propaganda Adversa	Manipulação planejada de informações, ideias ou doutrinas para influenciar grupos e indivíduos, com vistas a obter comportamentos pré-determinados que resultem em benefício ao seu patrocinador.
Reclassificação	Alteração do grau de sigilo atribuído a dado, conhecimento, documento, material, área ou instalação.

(Continuação)

Termo / Conceito	Definição
Sabotagem	Ato deliberado, de efeito físico e psicológico, executado por agentes adversos, vinculados ou não a serviço de Inteligência, com o objetivo de inutilizar ou de adulterar conhecimento, dado, material, equipamento e instalação. A sabotagem pode ser, ainda, empregada para a destruição de ideias ou da reputação de instituições e de pessoas.
Sigilo	É a qualidade de restrição de acesso atribuída a um conhecimento classificado.
Terrorismo	Caracteriza-se pela ameaça ou emprego da violência física ou psicológica, de forma premeditada, por indivíduos ou grupos adversos, apoiados ou não por Estados. É motivado por razões políticas, ideológicas, econômicas, ambientais, religiosas ou psicossociais, e objetiva coagir ou intimidar autoridades ou parte da população, subjugar pessoas ou alcançar determinado fim ou propósito.
Vazamento	Divulgação não autorizada de conhecimento ou dado classificado.

TÉCNICA DE AVALIAÇÃO DE DADOS

A. Julgamento da fonte

- Sob o aspecto da autenticidade, procura-se verificar se o dado provém realmente da fonte presumida. Esse trabalho é desenvolvido por meio do estudo das particularidades e dos eventuais indicativos que permitam caracterizar a fonte. Cuidados especiais são observados para distinguir fonte de canal de transmissão, já que muitas vezes surge entre a fonte e o avaliador a figura do intermediário do dado. Esse intermediário é considerado canal de transmissão e não deve ser confundido com a fonte do dado.
- Sob o aspecto da confiança, são considerados básicos os seguintes indicadores que a ela se relacionam:

        - antecedentes (criminal, político, de lealdade, de honestidade, etc.);
        - padrão de vida (compatível ou não com o seu poder aquisitivo);
        - contribuição já prestada ao SISTEMA (precisão de dados, etc.); e
        - motivação (pagamento, patriotismo, interesse pessoal, vingança, etc.).
- Sob o aspecto da competência, a fonte é julgada levando-se em conta, essencialmente, os seguintes indicadores:
    - Habilitação: atributos pessoais da fonte presumida para perceber, memorizar e descrever especificamente o fato ou situação objeto do dado. A fonte é, portanto, julgada com base no estudo da sua capacidade pessoal para perceber o fato ou a situação; e
    - Localização: possibilidade de a fonte (por si mesma), em razão da sua localização física, perceber o fato ou a situação que descreve.

Após a análise da fonte é atribuído o Grau de Idoneidade, conforme o julgamento da fonte:

JULGAMENTO DA FONTE			
LETRA	**GRAU DE IDONEIDADE**	**SIGNIFICADO**	**REQUISITOS**
A	Idônea	É aquela que, ao longo do tempo em que vem sendo utilizada, atendeu sempre aos parâmetros considerados.	Atende positivamente aos parâmetros AUTENTICIDADE, CONFIANÇA e COMPETÊNCIA. Caracteriza-se pela precisão e comprovação posterior dos dados que disponibiliza
B	Regularmente idônea	Na maioria das ocasiões se conduziu positivamente em relação às avaliações.	Atende aos parâmetros AUTENTICIDADE e COMPETÊNCIA, mas não plenamente ao parâmetro CONFIANÇA. Caracteriza-se por disponibilizar dados que normalmente se comprovam.
C	Regularmente inidônea	Na maioria das ocasiões se conduziu negativamente em relação às avaliações.	Pode atender ou não aos parâmetros AUTENTICIDADE e COMPETÊNCIA. Apresenta pouco grau de CONFIANÇA. Caracteriza-se por disponibilizar dado que normalmente não se comprova.
D	Não avaliada	A fonte era desconhecida até o momento.	Fonte desconhecida até então.

B. Julgamento do Conteúdo

Visa a determinar o grau de veracidade do conteúdo. No julgamento, o conteúdo do dado é considerado sob os aspectos de semelhança, coerência e compatibilidade.

- A semelhança consiste em verificar se há outro dado, oriundo de fonte diferente, cujo conteúdo esteja conforme o dado em julgamento.
- A coerência consiste em determinar se o dado em julgamento não apresenta contradições em seu conteúdo; busca-se, assim, verificar a harmonia interna do dado, o seu encadeamento lógico.
- A compatibilidade é aferida estabelecendo-se o relacionamento do dado com o que se sabe sobre o fato ou a situação que é objeto do mesmo procura-se, desse modo, examinar o grau de harmonia com que o dado se relaciona com os outros conhecidos anteriormente.

Após a análise do conteúdo, é atribuído o grau de confirmado, provavelmente verdadeiro, duvidoso ou não avaliado, conforme o o julgamento do conteúdo:

JULGAMENTO DO CONTEÚDO		
NÚMERO	**CONTEÚDO**	**SIGNIFICADO**
1	Idônea	Foi disponibilizado por outra(s) fonte(s) e apresenta um conteúdo coerente e compatível.
2	Regularmente idônea	Embora não tenha sido confirmado por outra(s) fonte(s), apresenta coerência e compatibilidade
3	Regularmente inidônea	Embora coerente, não pôde ser confirmado e é pouco compatível com o que já se conhece sobre o fato ou situações considerados.
4	Não avaliada	Não se pôde avaliar o conteúdo com relação aos parâmetros SEMELHANÇA e COMPATIBILIDADE.