**AVALIAÇÃO DA POLÍTICA CIBERNÉTICA DE DEFESA: APLICAÇÕES A TEORIA DO PROGRAMA**

A teoria do programa é uma importante ferramenta para avaliação de políticas públicas, pois permite delinear a cadeia causal entre a oferta da política pública e a mudança que ela causa no público alvo. Isto é, torna possível identificar de maneira sistemática para qual finalidade a política pública foi criada, qual o caminho que ela traça para atingir tal objetivo, e como os clientes usufruem e interagem com o serviço ofertado. O presente ensaio busca construir uma sólida estrutura, através de contribuições teóricas para uma posterior avaliação da Política Cibernética de Defesa.

**David Chaves**

1. **O que é a teoria do programa?**

Cassiolato e Gueresi (2010 *apud* DOMINGOS; SILVA, 2017) apontam duas principais contribuições dessa abordagem: (1) um recurso para melhor planejar a política pública em sua formulação; e, (2) identificação de possíveis falhas que possam afetar no sucesso da política. Dessa forma, essa ferramenta é crucial para avaliação de políticas públicas, haja visto que fornece insumos para avaliação da implementação e mensuração de impacto.

Além do mais, a teoria do programa consiste em uma forma de aumentar a accountability na formulação e implementação das políticas públicas (NEWCOMER et al, 2015 *apud* DOMINGOS; SILVA, 2015). Ao se tratar da Política de Defesa Cibernética, o aumento de transparência poderia encurtar a enorme distância que existe entre os oficiais das Forças Armadas e a sociedade civil brasileira.

Uma vez compreendida a relevância da teoria do programa, passamos a compreensão do que ela se trata. Essa etapa explica como a estratégia de atuação da política pública atua e como isso permite atingir os resultados esperados (ROSSI, FREEMAN e LIPSEY, 2003).

Em meados de 1970, Carol Weiss e Joseph Wholey foram um dos precursores desse instrumento teórico, desde então ele vem sendo adaptado e aperfeiçoado para otimizar o processo. Em razão disso, existe mais de um modelo de teoria do programa, porém aqui tratarei, em maior profundidade, do modelo lógico, o qual me parece mais intuitivo e eficaz para esboçar como a Política Cibernética de Defesa pretende alcançar resultados.

A Agência Americana para o Desenvolvimento Internacional (originalmente United States Agency for International Development- USAID) sistematizou o modelo lógico em um esquema que possibilita a clara visualização entre causa e efeito da política pública (FREITAS e SILVEIRA, 2015, DELGADO, 2010 *apud* DOMINGOS; SILVA, 2017, pág. 09), composto por 05 elementos de análise, a saber (ROSSI *et al,* 2003, *apud* DOMINGOS; SILVA, 2017):

1. Insumos: são os recursos financeiros e humanos destinados a execução das atividades da política pública, tais como, orçamento, equipe de agentes públicos, local de execução, etc.;
2. Atividades: quais procedimentos serão realizados para atingir os produtos, para ofertar os serviços ao público-alvo;
3. Produtos: o que é ofertado ao público alvo, isto é, o produto da “operacionalização” de insumos em resultados;
4. Resultados: serviços que os clientes da política pública vão consumir, os produtos, dos quais, o público-alvo usufruirá;
5. Impacto: os objetivos últimos, as mudanças de características do status-quodos clientes.

É interessante notar como cada elemento está interligado ao componente seguinte, constituindo o caminho causal da política pública, ao passo que entre o objetivo da política pública e o resultado esperado existe um caminho a ser trilhado. É preciso saber como alcançar aquele resultado, quais insumos serão mobilizados para realizar as atividades necessárias para produzir os serviços que serão usufruídos pelo público-alvo, e consonante a isso, é necessário pensar como os clientes irão reagir  aos serviços recebidos, e como esses últimos alterarão o status quo dos primeiros. Não basta apenas mensurar o impacto da política pública, mas saber como ela produziu esse efeito. Para melhor ilustrar, a seguir apresenta-se a figura:

Figura 01. Modelo Lógico da Teoria do Programa

Fonte: Elaboração própria de acordo com Domingos e Silva (2017)

A partir dessa breve apresentação da teoria do programa, traremos à continuidade um esboço de como se daria sua aplicação na Política Cibernética de Defesa, lei de autoria do Ministério da Defesa brasileiro, sob o comando do ministro Celso Amorim, datada de 27 de setembro de 2012, instituída através da portaria normativa No 3.389 /MD "Política Cibernética de Defesa" (BRASIL, 2012).

1. **Teoria do Programa Aplicada a Política Cibernética de Defesa**
* Insumos

De acordo com a leitura do texto rígido da lei, foram identificados quatro principais insumos: 1- a política deve ser revisada e atualizada periodicamente pelo Ministério da Defesa, por intermédio do EMCFA (Estado-Maior Conjunto das Forças Armadas), por iniciativa própria ou por proposta de uma das armas das Forças Armadas; 2- o Estado-Maior Conjunto das Forças Armadas é o órgão responsável por assessorar o Ministro da Defesa na implementação e gestão do Sistema Militar de Defesa Cibernética (SMDC); 3- as ações da polítca dependem, fundamentalmente, da atuação coletiva da sociedade, incluindo o Ministério da Defesa, a comunidade acadêmica, os setores públicos e privados e a base industrial de defesa; e 4- a capacitação tecnológica do setor cibernético deve ser atingida de maneira harmônica com a Política de Ciência, Tecnologia e Inovação para a defesa nacional.

* Atividades

Em relação às atividades contatou-se que a legislação prevê atividades distintas a depender de sua seara. Sendo divididas em: StCiber; Inteligência; SIC;Ministério de Ciência, Tecnologia e Inovação (MCTI); Legislação; mobilização social e militar; e, segurança dos ativos de informação da Administração Pública Federal (APF). Nesse ensaio, com finalidade ilustrativa, nos aprofundaremos nas atividades relacionadas ao StCiber e à Legislação.

Dessa maneira, no que tange a condução das atividades do StCiber no Ministério de Defesa, têm-se como atividades: 1-definir os perfis do pessoal necessário para a condução das atividades do StCiber; 2*-* criar cargos e funções específicos para pessoal especializado com o intuito de atender as necessidades do St Ciber; 3*-* estabelecer critérios e controlar a mobilização e desmobilização de pessoal para a atividade de Defesa Cibernética; 4- identificar, cadastrar e selecionar o pessoal com competências ou habilidades, existente nos ambientes interno e externo das Forças Armadas, para integrar o SMDC; 5*-* capacitar, de forma continuada, pessoal para atuar no StCiber, sob a orientação do órgão central do SMDC, aproveitando estruturas existentes; 6- viabilizar a participação de pessoal envolvido com o StCiber em cursos, estágios, congressos, seminários, simpósios e outras atividades similares relacionadas no Brasil e no exterior; 7*-* organizar eventos que possibilitem a apresentação e discussão de temas relevantes em áreas de interesse ao Setor Cibernético, e 8- incluir o conteúdo Defesa Cibernética nos currículos dos cursos, em todos os níveis de ensino do Ministério de Defesa.

Em relação à Legislação as atividades destacadas são: 1- colaborar com o órgão da Presidência da República encarregado pela elaboração da Política Nacional de Segurança Cibernética; 2*-* manter atualizada a Política Cibernética de Defesa em consonância com a Política Nacional de Segurança Cibernética; 3*-* definir atribuições e responsabilidades para o exercício das atividades relacionadas à Defesa Cibernética; 4- elaborar propostas de legislação federal, a fim de amparar as atividades de Defesa Cibernética; 5*-* propor criação de programa orçamentário para viabilizar as ações e atividades do StCiber; e, 6-propor a adequação da Lei de Mobilização Nacional e do Sistema Nacional de Mobilização (SINAMOB) para torná-los compatíveis com as necessidades do St Ciber.

* Produtos

São compreendidos como principais produtos da Política Cibernética de Defesa: 1-  Ampliação do quadro do sistema militar de defesa cibernético; 2- Integração do setor cibernético com o Ministério da Defesa; 3- Mapeamento das infraestruturas de informação; 4- Desenvolver projetos de segurança de redes; Organizar e alocar o pessoal e os cargos no setor cibernético; 5- Ampliar a participação dos empregados no setor cibernético em atividades como eventos e cursos; 6- Organização de eventos temáticos na área cibernética; 7- Inclusão da defesa cibernética nos cursos de ensino do Ministério da Defesa; 8- Inserção da fonte cibernética na integração de fontes de dados gerais; 9- Criação de estruturas de inteligência cibernética aplicando métodos científicos; 10- Integração do SMDC e os órgãos de Inteligência das Forças Armadas; 11- Implementação da Gestão de SIC na Defesa; 12- Realização de uma infraestrutura de chaves públicas da defesa; 13- Identificar padrões interoperáveis de criptografia de Defesa; 14- Integração das estruturas de Ciência, Tecnologia e Inovação (C,T&I) com o setor cibernético; 15- Fazer parcerias entre centros de pesquisa militares e civis; 16- Adequação do SINAMOB com o setor cibernético; 17- Criação de um banco de dados ativos sobre Defesa Cibernética; 18- Propor a campanha de educação sobre Defesa Cibernética, e 19- Colaborar com os órgãos da APF, compartilhando informações conjuntas.

* Resultados

Os resultados esperados são: 1- Capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (StCiber) no âmbito do Ministério de Defesa; 2- Assegurar, de forma conjunta, o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da Defesa Nacional; 3- Colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética; 4- Desenvolver e manter atualizada a doutrina de emprego do StCiber; 5- Implementar medidas que contribuam para a Gestão da SIC no âmbito do MD; 6- Adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do StCiber; 7- Definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no StCiber; 8- Cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do StCiber; e  9- Contribuir para a segurança dos ativos de informação da APF, no que se refere à Segurança Cibernética, situados fora do âmbito do Ministério da Defesa.

* Impacto

Identificados dois impactos na lei, eles são: 1- Aumentar a influência da Política Cibernética de Defesa na sociedade e a integração do espaço cibernético pelas Forças Armadas em alinhamento com os interesses nacionais, 2- Assegurar a Defesa Cibernética como um pilar importante no Ministério da Defesa, através da cooperação com o Ministério de Ciência, Tecnologia e Inovação e do estimulo ao ensino nacional.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

BRASIL, Ministério da Defesa. Política Cibernética de Defesa, MD31-P-02, 1ªed., Brasília, 2012, 24p.BRASIL, Minis

DOMINGOS, Amanda; SILVA, Lucas E. O.. TEORIA DO PROGRAMA: O que é, para que serve e quando fazer? **Congresso Alacip 2017.**Montevideo, p. 01-20. jul. 2017. Disponível em: <http://www.congresoalacip2017.org/arquivo/downloadpublic2?q=YToyOntzOjY6InBhcmFtcyI7czozNToiYToxOntzOjEwOiJJRF9BUlFVSVZPIjtzOjQ6IjIwMzMiO30iO3M6MToiaCI7czozMjoiNWZjZDkyYTUzOGY5MmFhNDk3YTlmMjUwMDIyMDcwYjYiO30%3D>. Acesso em: 02 jul. 2018.

ROSSI, Peter H.; LIPSEY, Mark W.; FREEMAN, Howard E. Evaluation: A systematic approach. Sagepublications, 2003.