

Política Cibernética de Defesa

PORTARIA NORMATIVA No- 3.389/MD, DE 21 DE DEZEMBRO DE 2012

Dispõe sobre a Política Cibernética de Defesa. O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe conferem o inciso II do parágrafo único do art. 87 da Constituição, e observado o disposto nos incisos III, VI e IX do art. 1º e inciso VII do art. 16 do Anexo I do Decreto nº 7.364, de 23 de novembro de 2010, e no Decreto no 6.703, de 18 de dezembro de 2008, resolve:

Art. 1º Aprovar a Política Cibernética de Defesa - MD31-P-02 (1ª Edição/2012), anexa a esta Portaria Normativa.

Art. 2º Esta Portaria Normativa entra em vigor na data de sua publicação.

CELSO AMORIM

POLÍTICA CIBERNÉTICA DE DEFESA

CAPÍTULO I DA INTRODUÇÃO

1.1. Finalidade

A Política Cibernética de Defesa tem a finalidade de orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos.

1.2. Aplicação

A Política Cibernética de Defesa aplica-se a todos os componentes da expressão militar do Poder Nacional, bem como às entidades que venham a participar de atividades de Defesa ou de Guerra Cibernética.

1.3. Pressupostos Básicos

A definição dos objetivos e a determinação das diretrizes da Política Cibernética de Defesa obedecem aos seguintes pressupostos básicos:

- a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa;
- b) as atividades de Defesa Cibernética no MD são orientadas para atender às necessidades da Defesa Nacional;
- c) as ações cibernéticas de caráter ofensivo deverão estar em conformidade com o planejamento elaborado em atendimento às Hipóteses de Emprego (HE);
- d) a capacitação tecnológica do Setor Cibernético deve ser buscada de maneira harmônica com a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional (C,T&I);
- e) a eficácia das ações de Defesa Cibernética no MD depende diretamente do grau de conscientização alcançado junto às organizações e pessoas acerca do valor da informação que detêm ou processam;

f) a Segurança da Informação e Comunicações (SIC) é a base da Defesa Cibernética e depende diretamente das ações individuais; não há Defesa Cibernética sem ações de SIC; e

g) as ações cibernéticas no contexto do MD visam a assegurar o uso do espaço cibernético, impedindo ou dificultando seu uso contra os interesses do País e garantindo, dessa forma, a liberdade de ação.

CAPÍTULO II DOS OBJETIVOS

2.1. Objetivos

São objetivos da Política Cibernética de Defesa:

a) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional; ou dificultar sua utilização contra interesses da Defesa Nacional;

b) capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD;

c) 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, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);

d) desenvolver e manter atualizada a doutrina de emprego do St Ciber;

e) implementar medidas que contribuam para a Gestão da SIC no âmbito do MD;

f) adequar as estruturas de C, T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber;

g) definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber;

h) cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e

i) contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD.

CAPÍTULO III DAS DIRETRIZES

3.1. Definição

As diretrizes explicitam as atividades a serem implementadas pelo MD para alcançar os objetivos constantes da Política Cibernética de Defesa.

3.2. Diretrizes

3.2.1. Diretrizes atinentes ao Objetivo Nº I - assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional:

- a) conceber e implantar o Sistema Militar de Defesa Cibernética (SMDC), contando com a participação de militares das FA e civis;
- b) criar a estrutura para realizar a coordenação e a integração do St Ciber no âmbito do MD, como órgão central do SMDC, com a possibilidade de participação de militares das FA e civis;
- c) levantar as infraestruturas críticas de informação associadas ao St Ciber para contribuir com a formação da consciência situacional necessária às atividades de Defesa Cibernética;
- d) estabelecer critérios de risco, inerentes aos ativos de informação, e realizar o seu gerenciamento, reduzindo os riscos às infraestruturas críticas da informação de interesse da Defesa Nacional a níveis aceitáveis;
- e) criar e normatizar processos de Segurança Cibernética para padronizar procedimentos de acreditação no âmbito das infraestruturas críticas de informação de interesse da Defesa Nacional; e
- f) estabelecer programas/projetos a fim de assegurar a capacidade de atuar em rede com segurança, fortalecendo, dessa forma, a operacionalidade da atividade de Comando e Controle (C2) no MD.

3.2.2. Diretrizes atinentes ao Objetivo Nº II - capacitar e gerir talentos humanos necessários à condução das atividades do St Ciber no âmbito do MD:

- a) definir os perfis do pessoal necessário para a condução das atividades do St Ciber;
- b) criar cargos e funções específicos e mobiliá-los com pessoal especializado para atender às necessidades do St Ciber;
- c) estabelecer critérios e controlar a mobilização e desmobilização de pessoal para a atividade de Defesa Cibernética;
- d) identificar, cadastrar e selecionar o pessoal com competências ou habilidades, existente nos ambientes interno e externo das FA, para integrar o SMDC;
- e) capacitar, de forma continuada, pessoal para atuar no St Ciber, sob a orientação do órgão central do SMDC, aproveitando estruturas existentes;
- f) viabilizar a participação de pessoal envolvido com o St Ciber em cursos, estágios, congressos, seminários, simpósios e outras atividades similares relacionadas no Brasil e no exterior;
- g) realizar, periodicamente, eventos que possibilitem a apresentação e discussão de temas relevantes em áreas de interesse do Setor Cibernético, a serem organizados e conduzidos pelo órgão central do SMDC, para nivelamento e atualização do conhecimento;
- h) criar instrumentos para viabilizar e motivar a permanência do pessoal especializado nas atividades do St Ciber, permitindo a continuidade da atividade;
- i) realizar parcerias estratégicas e intercâmbio entre as FA e instituições de interesse; e

j) incluir o conteúdo Defesa Cibernética nos currículos dos cursos, em todos os níveis, no que couber, dos estabelecimentos de ensino do MD.

3.2.3. Diretrizes atinentes ao Objetivo Nº III - colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o SINDE e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o GSI/PR:

a) adequar a doutrina de Inteligência de modo a inserir a fonte cibernética no contexto da integração de fontes de dados visando à produção de conhecimento;

b) criar estruturas de Inteligência Cibernética, conforme a

necessidade dos órgãos centrais de Inteligência das FA e do SMDC, para aplicar métodos científicos e sistemáticos, buscando extrair e analisar dados oriundos da fonte cibernética, produzindo conhecimento de interesse;

c) estabelecer um canal sistêmico/técnico entre o órgão central do SMDC e os órgãos centrais de Inteligência das FA, no âmbito do SINDE, no tocante ao St Ciber; e

d) levantar as infraestruturas críticas de informação associadas às ameaças internas e externas, reais ou potenciais, para contribuir com a formação da consciência situacional necessária às atividades de inteligência.

3.2.4. Diretrizes atinentes ao Objetivo Nº IV - desenvolver e manter atualizada a doutrina de emprego do St Ciber:

a) criar a doutrina de Defesa Cibernética mediante proposta do órgão central do SMDC;

b) fomentar o desenvolvimento e o intercâmbio de teses,

dissertações e outros trabalhos similares, com enfoque doutrinário, em instituições de ensino superior civis e militares de interesse para as atividades do St Ciber;

c) promover intercâmbio doutrinário, normativo e técnico, com instituições civis e militares, nacionais e de nações amigas;

d) inserir a Defesa Cibernética nos exercícios de simulação de combate e nas operações conjuntas;

e) criar um sistema de gestão de conhecimento de lições aprendidas para composição e atualização da doutrina; e

f) designar o órgão central do SMDC como responsável por propor as inovações e atualizações de doutrina para o St Ciber no âmbito da Defesa.

3.2.5. Diretrizes atinentes ao Objetivo Nº V – implementar medidas que contribuam para a Gestão da SIC no âmbito do MD:

a) implementar metodologia de Gestão de SIC na Defesa, levando em conta a legislação e normas vigentes, as melhores práticas,

a Doutrina de Inteligência de Defesa e padrões internacionais de interesse;

b) implementar uma infraestrutura de chaves públicas da Defesa (ICP Defesa);

- c) determinar padrões interoperáveis de criptografia de Defesa em complemento aos das FA; e
- d) implementar a sistemática de auditoria de SIC na Defesa.

3.2.6. Diretrizes atinentes ao Objetivo Nº VI - adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber:

- a) planejar e executar a adequação das estruturas de Ciência, Tecnologia e Inovação (C,T&I), integrando esforços entre as FA para atender às necessidades do St Ciber;
- b) criar comitê permanente, no âmbito da Defesa, constituído por representantes do MD e convidados, de outros ministérios e de agências de fomento, para intensificar e explorar novas oportunidades de cooperação em C,T&I, nas áreas de interesse do St Ciber;
- c) prospectar as necessidades do St Ciber, na área de C,T&I, no âmbito da Defesa, para identificar as capacidades científico-tecnológicas necessárias ao desenvolvimento do Setor;
- d) identificar competências (individuais e organizacionais) específicas em C,T&I, de interesse do St Ciber, no âmbito do MD e dos centros de pesquisa e desenvolvimento civis (públicos e privados), estabelecendo parcerias entre centros de excelência, em nível nacional, para agregar as instituições e evitar a dispersão de recursos;
- e) criar parcerias e cooperação entre os centros militares de pesquisa e desenvolvimento e os centros de pesquisa e desenvolvimento civis (públicos e privados), para estimular a integração das iniciativas de interesse do St Ciber; e
- f) criar programas, no âmbito do MD, em parceria com o MCTI, que contemplem a característica dual (emprego civil e militar) das tecnologias de informação e comunicações (TIC) empregadas na área cibernética, para fortalecer o envolvimento do setor industrial nas fases de desenvolvimento dos projetos de interesse do St Ciber.

3.2.7. Diretrizes atinentes ao Objetivo Nº VII - definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber:

- a) colaborar com o órgão da Presidência da República (PR) encarregado da elaboração da Política Nacional de Segurança Cibernética;
- b) manter atualizada a Política Cibernética de Defesa em consonância com a Política Nacional de Segurança Cibernética, quando da sua existência;
- c) definir atribuições e responsabilidades para o exercício das atividades relacionadas à Defesa Cibernética;
- d) elaborar propostas de criação e adequação de legislação federal, a fim de amparar as atividades de Defesa Cibernética;
- e) propor criação de programa orçamentário para viabilizar as ações e atividades do St Ciber;
- f) revisar os planejamentos das Hipóteses de Emprego (HE) para considerar as ações no espaço cibernético; e

g) 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.

3.2.8. Diretrizes atinentes ao Objetivo N° VIII – cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber:

a) realizar levantamento sistemático de ativos de informação passíveis de serem mobilizados em prol do St Ciber;

b) elaborar e manter atualizado um banco de ativos de informação, de interesse para a mobilização, em prol do SMDC;

c) elaborar Planos de Mobilização de Ativos de Informação, com respectivos custos, em consonância com a Lei de Mobilização Nacional;

d) adequar as necessidades de mobilização do SMDC ao SINAMOB; e

e) propor, ao governo federal, a realização de campanha nacional de educação sobre Defesa Cibernética, visando à Mobilização Nacional, para elevar o nível de conscientização da sociedade brasileira.

3.2.9. Diretrizes atinentes ao Objetivo N° IX - contribuir para a segurança dos ativos de informação da APF, no que se refere à Segurança Cibernética, situados fora do âmbito do MD:

a) conhecer, por intermédio da PR, as infraestruturas críticas da informação dos órgãos da APF situados fora do MD;

b) colaborar, dentro dos limites da legislação em vigor, com os demais órgãos da APF, mediante solicitação e por intermédio da PR, para o restabelecimento da Segurança Cibernética;

c) manter um banco de dados e estabelecer um canal sistêmico/ técnico entre o órgão central do SMDC e os órgãos da APF, para compartilhamento de informações de incidentes de rede; e

d) atuar no reconhecimento de artefatos e desenvolvimento de ferramentas cibernéticas, em conjunto com a PR, contribuindo para a proteção dos ativos de informação da APF.

CAPÍTULO IV DAS RESPONSABILIDADES E DA ATUALIZAÇÃO

4.1. Responsabilidades

O Estado-Maior Conjunto das Forças Armadas (EMCFA) é o órgão responsável por assessorar o Ministro de Estado da Defesa na implementação e gestão do SMDC, visando a garantir, no âmbito da Defesa, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança desejados.

4.2. Atualização

Esta Política deve ser revisada e atualizada periodicamente pelo MD, por intermédio do EMCFA, por iniciativa própria ou por proposta de uma das Forças Armadas.