Segurança Cibernética e Políticas Públicas no Brasil

Valéria Farias Alves
valeria.farias@gmail.com
CEFET RJ

Cristina Gomes de Souza
crisgsouza@gmail.com
CEFET RJ

Álvaro Chrispino
alvaro.chrispino@gmail.com
CEFET RJ

Eduardo Ogasawara
eduardo.ogasawara@gmail.com
CEFET RJ

Resumo:O uso cada vez mais amplo da internet fez propagar as chamadas ameaças cibernéticas, capazes de causar grandes danos às empresas, governos e sociedade em geral. O Brasil é um país vulnerável e pouco preparado para lidar com essas ameaças. A Seguranc?a Ciberne?tica no Brasil é um processo que ainda está em construção, sendo necessária uma maior disseminação da cultura da segurança e o envolvimento de todos os atores sociais. É através de políticas públicas que são estabelecidas regras e ações visando proteger e controlar o ambiente virtual no país. A partir desse contexto, esse artigo tem por objetivo apresentar o cenário da política pública de segurança da informação no Brasil, mais especificamente em relação à segurança cibernética, apontando conceitos básicos, estrutura organizacional, legislação e sistemas de controle existentes. O estudo foi desenvolvido a partir de pesquisa bibliográfica e documental, além do levantamento de informações nos sites de diversos órgãos da Administração Pública Federal. Espera-se que os resultados apresentados possam servir de fonte de consulta e fornecer subsídios para todos aqueles que lidam, direta ou indiretamente, com essa temática. Espera-se ainda que possa contribuir para uma maior conscientização e suscitar discussões sobre o assunto no âmbito da sociedade.

Palavras Chave: Segurança - Políticas Públicas - Informação - Ataques Ciberneticos -

1. INTRODUÇÃO

O Espaço Cibernético pode ser entendido como "o território não físico criado por meios computacionais, onde pessoas físicas e jurídicas, isoladamente ou em grupo, integrantes de empresas, órgãos públicos ou governos, podem se comunicar, realizar pesquisas e trafegar dados de maneira geral, valendo-se de Tecnologias da Informação e Comunicação (TIC) como suporte para seu funcionamento" (HOSANG, 2011).

Considerando-se o espaço cibernético, o uso cada vez mais amplo e disseminando da internet para a realização de atividades diversas, através da integração de vários sistemas e equipamentos, é um fenômeno que merecido atenção por parte dos governos, empresas, fornecedores de solução, instituições de pesquisa e universidades (ISONI e VIDOTTI, 2007), uma vez que, atrelado a este crescimento, sugiram as chamadas ameaças cibernéticas. Tais ameaças se caracterizam pelo roubo de informações confidenciais e invasões a sistemas através de acessos não autorizados, que são facilitados pelo anonimato que a internet propicia.

Para controlar este ambiente virtual foram sendo estabelecidas políticas de controle relacionadas à segurança da informação ou segurança cibernética. As políticas de segurança são adotadas por empresas públicas ou privadas com a finalidade de proteger seus ambientes tecnológicos e todas as informações neles contidas. Muita atenção também deve ser dada às políticas públicas relacionadas à segurança da informação, que são tratadas pelos órgãos governamentais, de forma a proteger os cidadãos e o Estado.

A importância dessa temática fica constatada diante de casos como a recente divulgação do roubo de informações realizado pela NSA – Agência Nacional de Segurança dos Estados Unidos (National Security Agency). Documentos revelados por Edward Snowden, ex-funcionário de uma consultoria que prestava serviço a NSA, mostraram a fragilidade do Brasil e de outros países quanto à guarda das informações e o poder político que tais informações podem ter.

Essa espionagem, que teve motivação econômica, política e diplomática, evidenciou o grande aparato técnico em poder dos Estados Unidos, em contraste com o despreparo de outras nações. Segundo o porta-voz substituto da ONU, Eduardo Del Buey, "todos os países-membros da ONU são obrigados por lei a respeitar a privacidade de comunicações diplomáticas e espera-se que o façam" (REVISTA ÉPOCA, 2013). No entanto, esse episódio mostra que movimentos relacionados à espionagem podem virar uma constante, passando por cima da ética e das leis, colocando em risco as nações.

Estudos realizados pelo centro de pesquisas Belga Security Defense Agenda (SDA) e pela McAfee revelam que o Brasil é um dos países menos preparados para ataques cibernéticos, em um ranking de 23 nações analisadas. Dos países estudados, nenhum obteve a nota máxima (5) de total prontidão contra ataques virtuais. O Brasil teve nota 2,5, ao lado de Índia e Romênia, ficando à frente apenas do México (GRAUMAN, 2012). Face aos acontecimentos, com prioridade alta, o Brasil deve planejar estrategicamente as políticas públicas relacionadas à defesa cibernética, de forma a promover a proteção da nação, guardando o bem maior, que são as informações.

Diante da premência e atualidade do tema, esse artigo aborda as políticas públicas como ações governamentais para controlar determinada ação que, neste caso, são desenvolvidas visando controlar os ataques cibernéticos ao Brasil. É através dessas políticas que são estabelecidas formas de controle e implementadas ações visando proteger e controlar o ambiente virtual no país. Dentro desse escopo, o estudo tem por objetivo apresentar o cenário da política pública de segurança da informação no Brasil, mais especificamente em

relação à segurança cibernética, apontando conceitos básicos, a estrutura organizacional, legislação voltada para a proteção da informação e sistemas de controle existentes.

Espera-se que esse estudo, desenvolvido a partir de uma revisão bibliográfica, pesquisa documental e do levantamento de informações junto a diversos órgãos, possa ser fonte de consulta e fornecer subsídios para todos aqueles que lidam, direta ou indiretamente, com essa temática. Espera-se ainda que possa contribuir para uma maior conscientização, bem como, suscitar discussões sobre o assunto no âmbito da sociedade. Afinal, conforme apontado por Alves Jr. (2011) "Como tema emergente, os conceitos e contornos da segurança cibernética estão ainda sendo delineados, e os registros na literatura acadêmica são vagos".

2. AS POLÍTICAS PÚBLICAS DE SEGURANÇA DA INFORMAÇÃO

De acordo com Chrispino (2002), as Políticas Públicas constituem o centro de equilíbrio de forças sociais diferentes. Para compreender o seu conceito, é preciso antes conhecer a definição do que é política e do que é pública. Política é a arte de governar ou de decidir os conflitos que caracterizam os agrupamentos sociais. Pública é aquilo que pertence a um povo, que é relativo às coletividades. Política Pública, portanto, é um meta-conceito que significa a ação do governo que visa atender a necessidade de uma coletividade, o que demanda agregar variáveis, instituir valores, perceber arranjos de forças, identificar processos e metas, e propor avaliações.

Souza (2006) diz que o interesse em estudar políticas públicas, que é um subcampo da ciência política, vem aumentando nos últimos anos. A autora explica que as políticas públicas, como campo do conhecimento, teve origem no ambiente acadêmico dos EUA, a partir do momento em que os estudos passaram a se concentrar na ação dos governos em detrimento das teorias sobre o papel do Estado na sociedade, que era o enfoque predominante das pesquisas realizadas na Europa.

Neste artigo, as políticas públicas são tratadas como ações governamentais para controlar determinada ação. As políticas públicas podem ser entendidas como resultantes de transações envolvendo os diversos atores políticos, tais como entidades governamentais, organizações públicas o privadas, cidadãos, entidades de classe e outros, sendo condicionadas por um jogo político e pelas ações das instituições, que variam de acordo com suas características de natureza constitucional e histórica (SPILLER e TOMMASI, 2003; MARCIANO, 2006).

Um dos grandes desafios do século XXI, alvo de políticas públicas dos mais diversos países, é a segurança da informação ou segurança cibernética, que busca garantir a integridade, disponibilidade, confidencialidade e autenticidade de sistemas de informação. A Segurança Cibernética é considerada como "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas" (GSI, 2009a). Essa definição abrange dois outros conceitos:

- Ativos de Informação: "os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso"; e
- Infraestruturas Críticas: "as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade".

Em se tratando de informações, tem-se a seguinte definição (GSI, 2009b):

- Infraestruturas Críticas da Informação: "o subconjunto de ativos da informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade".

Diante de tais desafios, as nações vêm se preparando para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação do governo e demais segmentos da sociedade. Dessa forma, o entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* de desenvolvimento requerendo, dentre outras ações, a promoção de diálogos e intercâmbio de ideias, iniciativas, dados, informações e melhores práticas visando à cooperação no tema no país e entre países (CANONGIA et al., 2010).

A defesa cibernética, por sua vez, pode ser entendida como o "conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente" (MINISTÉRIO DA DEFESA, 2010 citado por DE CARVALHO, 2011).

Conforme apontado por Da Cruz Jr. (2013), os conceitos de segurança e defesa são complementares, podendo-se entender o termo segurança como a função destinada a proteger as infraestruturas críticas e os sistemas de informação, ao passo que a defesa está relacionada a ações do Estado – normalmente atribuída a militares – com o objetivo de proteger o país de ameaças que possam por em risco a soberania nacional.

O evento ocorrido em 11 de setembro de 2001 deu origem à reformulação de muitos procedimentos e normas relacionados à segurança de modo geral e, mais especificamente, à segurança da informação, não só nos Estados Unidos, onde ocorreu o fato, mas em vários locais do mundo, que puderam identificar pontos a serem melhorados. Poucos dias após o incidente, foi criado nos Estados Unidos o Office of Homeland Security (Secretaria de Segurança Interna), com status de ministério (RELYEA, 2002). A partir de então, os atores políticos – através da rede política – iniciaram ações de interesse comum com o objetivo de garantir a segurança, estabelecendo medidas de prevenção e controle após um fato altamente relevante.

No Brasil, o setor cibernético é considerado como um dos três setores estratégicos de defesa, juntamente com o nuclear e o espacial (MINISTÉRIO DA DEFESA, 2008). O espaço cibernético do país apresenta as seguintes características (HOSANG, 2011):

- a armazenagem e o processamento da informação estão hospedados, em grande parte, em outros países;
- a infraestrutura é dominada por empresas multinacionais estrangeiras;
- o quantitativo de pessoas qualificadas na área é insuficiente para atender às demandas do país; e
- os profissionais da área normalmente atuam na academia ou no mercado, não havendo muita interação entre esses dois ambientes.

A educação em segurança da informação (TAKEMURA et al., 2008), a formação de pessoal qualificado e a interação e cooperação entre todos os atores envolvidos – sociedade civil, governo, meio acadêmico e setor empresarial – é fundamental para se avançar na questão da segurança cibernética (DA CRUZ JR., 2013).

Diante da necessidade de se estabelecer diretrizes básicas e de se ampliar a cultura cibernética no país, o governo brasileiro, por meios de seus órgãos e secretarias responsáveis pela segurança da informação, também se mobilizou visando articular um debate social,

econômico, político e técnico-científico sobre a Segurança Cibernética. Dentro desse contexto foram criados os chamados Livro Verde e Livro Branco.

O **Livro Verde: Segurança Cibernética no Brasil** (MANDARINO JR. e CANONGIA, 2010), elaborado em 2010, aponta potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, articulando uma visão de curto (2 – 3 anos), médio (5 – 7 anos), e longo (10 – 15 anos) prazo, abrangendo, como ponto de partida, os seguintes vetores: Político-Estratégico; Econômico; Social e Ambiental; CT&I; Educação; Legal; Cooperação Internacional; e Segurança das Infraestruturas Críticas. O Grupo Técnico de Segurança Cibernética, responsável pelo desenvolvimento da obra, contou com a participação de vários representantes dos seguintes órgãos: Gabinete de Segurança Institucional da Presidência da República (GSIPR – DSIC e ABIN); Ministério da Justiça (MJ e DPF); Ministério das Relações Exteriores (MRE); Ministério da Defesa (MD); e Comandos da Marinha, do Exército e da Aeronáutica. A coordenação do grupo foi realizada pelo Gabinete de Segurança Institucional da Presidência da República.

O **Livro Branco de Defesa Nacional** (BRASIL, 2012), por sua vez, foi elaborado em 2012 e apresenta assuntos relacionados à defesa da nação destacando, como atribuição do Estado, prover a segurança e defesa necessária para a sociedade. Conforme mencionado pelo então Ministro da Defesa, "o Livro Branco de Defesa Nacional soma-se à **Estratégia Nacional de Defesa** (MINISTÉRIO DA DEFESA, 2008) e à **Política Nacional de Defesa** (BRASIL, 2005) como documento esclarecedor sobre as atividades de defesa do Brasil". Nesse livro são abordados pontos relacionados à defesa cibernética, sendo essa relacionada como um dos 3 setores estratégicos, cujas ações devem ser coordenadas pelo Exército. Foram definidas, como premissas do projeto, contemplar a multidisciplinaridade e dualidade das aplicações, fomentar a base industrial de defesa e induzir a indústria nacional a produzir sistemas inovadores e componentes críticos nacionais.

3. ESTRUTURA DA GESTÃO POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

De modo geral, todas as instâncias do Estado devem buscar garantir e melhorar o nível de segurança da informação a nível nacional (DE CARVALHO, 2011). No entanto, de forma mais específica, a segurança cibernética encontra-se sob responsabilidade de dois órgãos principais: o Gabinete de Segurança Institucional da Presidência da República (GSIPR) e o Centro de Defesa Cibernética do Exército Brasileiro vinculado ao Ministério da Defesa (CDCiber/EB/MD).

Conforme apontado por De Cruz Jr. (2013), a direção das ações de segurança da informação e defesa cibernética foram segregadas nesses dois órgãos distintos, o que tende a fragilizar a proteção cibernética nacional. A Figura 3 apresenta as competências do GSIPR e do Ministério da Defesa em relação à Defesa e a Segurança Cibernética.

Nível de decisão	Designação	Estrutura
Político	Segurança Cibernética	Gabinete de Segurança Institucional (GSIPR)
Estratégico	Defesa Cibernética	Ministério da Defesa

Fonte: Adaptado de CDCiber/EB/MD (http://www.defesa.gov.br)

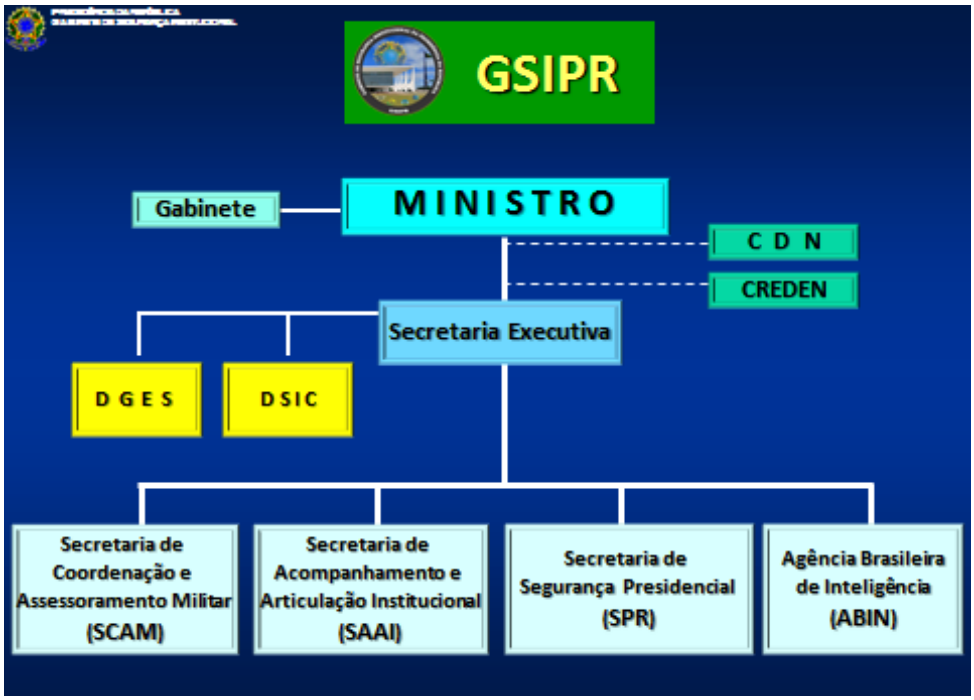
Figura 3: Níveis de decisão relacionados à Segurança e Defesa Cibernética

A seguir encontram-se relacionados diversos órgãos da administração federal que têm importante atuação nessa área.

3.1. GABINETE DE SEGURANÇA INSTITUCIONAL

O Gabinete de Segurança Institucional da Presidência da República (GSIPR), vinculado diretamente à Presidência da República, é um órgão considerado essencial na esfera do governo federal, possuindo status de Ministério. Dentre outras competências, cabe ao GSIPR a coordenação das atividades de inteligência federal e de segurança da informação.

Na estrutura do GSIPR, dois órgãos tratam de forma mais específica a segurança cibernética: o DSIC – Departamento de Segurança da Informação e Comunicação; e a ABIN – Agência Brasileira de Inteligência. O GSIPR ainda é responsável por exercer as atividades de Secretaria Executiva da Câmara de Relações Exteriores e Defesa Nacional – CREDEN, o qual também abrange questões relacionadas à segurança da informação e cibernética. A Figura 1 apresenta a estrutura organizacional do GSIPR.



Fonte: http://www.gsi.gov.br

Figura 1: Organograma do GSIPR

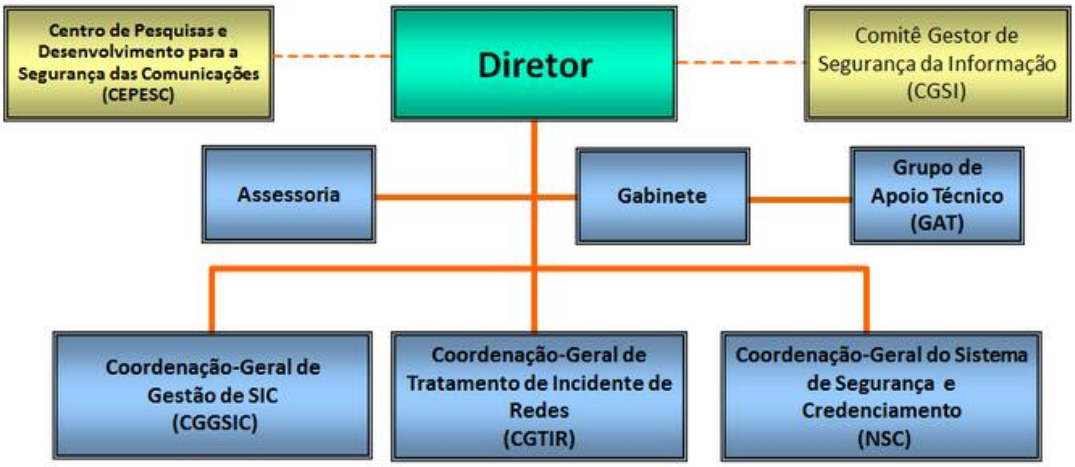
3.2. DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

O Departamento de Segurança da Informação e Comunicações (DSIC) possui como principais atividades:

- Planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal;
- Definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

- Estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança cibernética e à segurança da informação e comunicações;
- Avaliar tratados, acordos ou atos internacionais relacionados à segurança cibernética e à segurança da informação e comunicações;
- Coordenar a implementação de laboratório de pesquisa aplicada de desenvolvimento e de inovação metodológica, bem como de produtos, serviços e processos, no âmbito da segurança cibernética e da segurança da informação e comunicações.

A Figura 2 mostra o organograma do DSIC, que conta com o Comitê Gestor de Segurança da Informação, o Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações, o Grupo de Apoio Técnico, a Coordenação Geral de Gestão de Segurança da Informação e Comunicações, a Coordenação Geral de Tratamento de Incidentes de Rede e a Coordenação Geral do Sistema de Segurança e credenciamento.



Fonte: http://dsic.planalto.gov.br/organograma

Figura 2: Organograma do DSIC

Atendendo à sua missão e buscando assegurar ações voltadas para garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação na esfera da Administração Pública Federal, o DSIC coordenou a elaboração do **Guia de Referência para a Segurança das Infraestruturas Críticas da Informação**. Esse documento contempla (CANONGIA et al., 2010):

(1) Instrumentos para mapeamento e acompanhamento de ativos de informação;
(2) Requisitos mínimos necessários à segurança das infraestruturas críticas da informação, abordando segurança, resiliência e capacitação; e
(3) Método para identificação de ameaças e geração de alertas de segurança das infraestruturas críticas de informação.

3.3. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

A Agência Brasileira de Inteligência (ABIN) é o órgão central do Sistema Brasileiro de Inteligência, que tem como objetivo estratégico desenvolver atividades de inteligência voltadas para a defesa do estado democrático de direito, da sociedade, da eficácia do poder público e da soberania nacional. Dentre suas responsabiidades estão a execução da **Política**

Nacional de Inteligência (PNI) e a integração dos trabalhos dos órgãos setoriais de Inteligência, possuindo Superintendências Estaduais espalhadas pelo país. São competências da ABIN:

- executar a Política Nacional de Inteligência e as ações dela decorrentes, sob a supervisão da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo;
- planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;
- planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;
- avaliar as ameaças, internas e externas, à ordem constitucional;
- promover o desenvolvimento de recursos humanos e da doutrina de Inteligência; e
- realizar estudos e pesquisas para o exercício e o aprimoramento da atividade de Inteligência.

Apesar da criação da PNI ter sido definida na lei 9.883/99 – mesma lei que estabeleceu a ABIN, constando como uma das competências dessa Agência – até hoje não foi aprovada, aguardando a chancela da Presidência da República.

Dentre as atribuições da ABIN, no que interessa especificamente ao Setor Cibernético, destaca-se avaliar as ameaças internas e externas à ordem constitucional, entre elas, a cibernética. A ABIN atua em duas vertentes: Inteligência e Contra-Inteligência, de modo a produzir conhecimentos sobre fatos e situações que gerem ou possam vir a gerar ameaças, bem como, buscando antecipar e aproveitar oportunidades relacionadas à segurança do país.

3.4. CÂMARA DE RELAÇÕES EXTERIORES E DEFESA NACIONAL

A Câmara de Relações Exteriores e Defesa Nacional (CREDEN) é um órgão do governo para assessoramento do presidente da República nos assuntos pertinentes às relações e à defesa nacional. Sua presidência cabe ao ministro-chefe do GSIPR.

O CREDEN tem por objetivo: formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do governo federal; e aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, cujo escopo ultrapasse a competência de um único Ministério, abrangendo a segurança para as infraestruturas críticas, a segurança da informação e a segurança cibernética.

O CREDEN conta com um Grupo Técnico de Segurança Cibernética (GT SEG CIBER), instituído pela Portaria No. 45, de 8 de setembro de 2009, formado por representantes dos seguintes órgãos: Gabinete de Segurança Institucional da Presidência da República (GSIPR – DSIC e ABIN), Ministério da Justiça (MJ e DPF), Ministério das Relações Exteriores (MRE), Ministério da Defesa (MD), e Comandos da Marinha, do Exército e da Aeronáutica. A Coordenação do GT é exercida pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR), por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC).

Esse GT SEG CIBER, por sua vez, tem o objetivo de propor diretrizes e estratégias para a segurança cibernética, no âmbito da Administração Pública Federal. Conforme observação feita por Alves Jr. (2011), “percebe-se que o País reserva à segurança cibernética o viés da segurança e defesa nacional”.

3.5. CONSELHO DE DEFESA NACIONAL

O Conselho de Defesa Nacional (CDN) é um órgão de consulta do presidente da República para assuntos relacionados à soberania nacional e à defesa do Estado democrático de direito. Constitui um órgão de Estado e não de governo, que tem sua secretaria-executiva exercida pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSIPR).

A Secretaria Executica do CDN é assessorada por um Comitê Gestor da Segurança da Informação (CGSI), instituído pelo Decreto Nº 3505 de 13 de junho de 2000, nas questões relativas à na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de outros assuntos relativos aos objetivos estabelecidos no referido Decreto.

3.6. CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

Entre as atribuições da Casa Civil da Presidência da República está o Setor Cibernético, que trata de assuntos relacionados à execução de políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor de Infraestruturas de Chaves Públicas Brasileira (ICP-Brasil).

Vinculado à Casa Civil da Presidência da República está o Instituto Nacional de Tecnologia da Informação (ITI), que consiste em uma autarquia federal que tem por objetivo a manutenção da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, sendo a primeira autoridade da cadeia de certificação – AC Raiz. Cabe ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital.

3.7. CENTRO DE PESQUISAS E DESENVOLVIMENTO PARA SEGURANÇA DAS COMUNICAÇÕES

O Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC) foi criado em 1982 com o objetivo de sanar a deficiência do Brasil relacionada ao sigilo quanto à transmissão de informações oficiais, pois os órgãos governamentais não possuíam capacitação para realizar a criptografia dos dados nas comunicações relacionadas aos campos diplomático, comercial e militar.

O CEPESC é constituído por pesquisadores, tecnólogos e técnicos qualificados, recrutados em universidades e no mercado de trabalho. Tem como objetivo o desenvolvimento de tecnologias de criptografias relacionadas à transmissão de dados, além da promoção de pesquisa científica e tecnológica aplicada a projetos relacionados à segurança das comunicações. Fornece equipamentos e sistemas de segurança criptográfica a diversos órgãos governamentais e possui participação técnica no Programa Nacional de Proteção ao Conhecimento (PNPC) da ABIN, no Comitê Gestor de Segurança da Informação (CGSI), nos projetos Sistema de Proteção da Amazônia (SIPAM) e Sistema de Vigilância da Amazônia (SIVAM), em grupos de trabalho de sensoriamento remoto e na elaboração das especificações do sistema de infra-estrutura de chave púbica para o país.

3.8. CENTRO DE DEFESA CIBERNÉTICA DO EXÉRCITO BRASILEIRO

O Centro de Defesa Cibernética do Exército Brasileiro (CDCiber/EB/MD) foi criado em 02 de agosto de 2010, com a missão de coordenar as atividades do Setor Cibernético no Exército e promover ações alinhadas à Estratégia Nacional de Defesa, com ênfase na atuação em rede e redução das vulnerabilidades contra ataques cibernéticos.

4. LEGISLAÇÃO RELACIONADA À SEGURANÇA DA INFORMAÇÃO

Diante do novo cenário tecnológico e das novas demandas relacionadas à segurança da informação, a necessidade de marcos legais que disciplinem o uso do espaço cibernético se faz necessário, de forma a evitar potenciais conflitos e consequências danosas. O Brasil, buscando a evolução da sociedade, vem buscando formas de combater e restringir os ataques cibernéticos, por meios de políticas públicas de controle.

Hoje já existem normas federais que disciplinam o desenvolvimento de políticas de segurança da informação e comunicações em órgãos da Administração Pública Federal, como a que confere direitos e deveres ao gestor público, no que concerne à proteção dos sistemas e da informação públicos (FERNANDES, 2010).

A própria **Constituição Federal** de 1988, através dos artigos 5º, 23º, 37º e 216, aborda pontos relacionados à segurança da informação, onde são tratados temas voltados para a privacidade, contemplando o sigilo de informações relacionados à vida privada do indivíduo, disponibilidade de informações dos órgãos públicos e gestão das informações, de forma garantir a integridade, autenticidade, disponibilidade e sigilo. Também é abordado, através da **Consolidação das Leis Trabalhistas**, a proteção de informações sigilosas no exercício de emprego público (empresas públicas e sociedades de economia mista).

O **Código Civil**, nos artigos 927 e 932, destaca os pontos relacionados à responsabilidade do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.

O **Código Penal** trata a autenticidade e a privacidade das informações, com punições definidas para a violação de correspondência e crime de desvio, sonegação, subtração, supressão ou revelação de conteúdo de correspondência comercial.

O **Código de Defesa do Consumidor**, nos artigos 43 e 44, garante a integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

Em relação a proteção nas comunicações, o Ministério das Telecomunicações, como órgão responsável pela elaboração e cumprimento de políticas públicas no setor, com o apoio do órgão regulador, Agência Nacional de Telecomunicações (Anatel), estabeleceu políticas relacionadas a defesa cibernética de forma a elaborar estudos e adotar medidas de proteção da infraestrutura nacional de telecomunicações, contra falhas e ataques de guerra cibernética, com base em modelos da União Internacional de Telecomunicações e Federal Communications Commission. Nesse sentido, várias medidas de proteção estão sendo estudadas, implementadas e melhoradas gradativamente, a fim de manter a interconexão, interdependência e sustentabilidade das conexões, garantindo o lema "Tudo. Todos. Mesmo tempo. Todos os lugares" conectados de forma segura e confiável.

O Ministério de Defesa, por sua vez, lançou em 21 de dezembro de 2012 a Portaria Normativa 3.389/MD, que define a **Política Cibernética de Defesa**, visando orientar, no âmbito do Ministério da Defesa, as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos.

Apesar dessa regulamentação existente, o Brasil carece de uma **Política Nacional de Inteligência** que, conforme mencionado anteriormente, ainda encontra-se aguardando a aprovação da Presidência da República.

5. ÓRGÃO DE CONTROLE E INDICADORES

Com o objetivo de controlar e monitorar os indicadores relacionados a incidentes de segurança, órgãos específicos foram criados e são responsáveis por catalogar incidentes relacionados a segurança da informação, analisá-los e dar a tratativa necessária. Nesse contexto podem ser citados: o CTIR.gov e o CERT.br.

5.1. CTIR.gov

Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal ou CTIR.gov é o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal e está subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, tendo com função o atendimento aos incidentes em redes de computadores da Administração Pública Federal.

Entre os serviços prestados pelo CTIR.GOV está a notificação de incidentes, análise, suporte e coordenação à resposta a incidentes, a distribuição de alertas, recomendações e estatísticas, assim como a cooperação com outras equipes de tratamento de incidentes.

Da Cruz Jr. (2013), citando relatórios de avaliação de TI do Tribunal de Contas da União, diz que as redes da Administração Pública Federal (APF) apresenta níveis inaceitáveis de segurança. O autor menciona ainda dados do GSIPR que mostram que a APF registra cerca de 3 mil incidentes virtuais de segurança por mês.

5.2. CERT.br

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet. Desenvolve projetos de análise de tendências de ataques, com o objetivo de melhor entender suas características no espaço Internet Brasileiro, possibilitando assim melhores forma de combate e proteção, tendo como principal função a unificação das informações de incidentes de segurança com a colaboração de diversas entidades para a informação.

Os incidentes são registrados e catalogados, bem como, são gerados dados estatísticos de forma a facilitar a análise e fornecer subsídios para estudos que promovam melhorias contínuas nas mais diversas empresas.

6. CONCLUSÃO

Os ataques cibernéticos no cenário atual podem ser considerados o desafio do século, apresentando escala mundial crescente. Assim sendo, a Segurança Cibernética vem se tornando, cada vez mais, uma função estratégica de Estado, sendo essencial para manutenção e preservação das infraestruturas críticas de um país, tais como saúde, energia, defesa, transporte, telecomunicações e informação.

Para garantir essa proteção, se faz necessária a definição de estratégias, o estabelecimento de políticas e a criação de uma estrutura organizacional e regulatória voltadas para a segurança e defesa do espaço cibernético. Lidar com o mosaico de aspectos que perpassam a segurança cibernética demanda um conjunto de ações colaborativas envolvendo governo, setor privado, academia, terceiro setor e sociedade. Assim sendo, é preciso conscientizar e disseminar a cultura da segurança entre todos os atores que, direta ou indiretamente, são vulneráveis e podem ser afetados por ataques cibernéticos.

Comparando o Brasil a outros países desenvolvidos, podemos perceber que muito há de ser feito para que possamos garantir a proteção do ambiente cibernético. Nos Estados Unidos, segurança e defesa cibernética possuem uma estrutura de governança bastante centralizada, possuem leis que regulamentam a segurança cibernética, além de possuírem alta tecnologia e investimento, enquanto no Brasil, várias instituições respondem pelo assunto, o que tende a dificultar ações coordenadas de longo prazo.

Outro aspecto é a falta de um plano ou política estruturante de investimento e melhoria em segurança cibernética, apesar da Estratégia Nacional de Defesa, Livro Verde de Defesa e do Livro Branco terem reconhecido a importância do tema. A deficiência de governança das tecnologias da informação dentro dos próprios órgãos da administração federal e a falta de programas de cooperação, investimento e capacitação de longo prazo contribuem para o aumento da vulnerabilidade. Desta forma, se conclui que mesmo com as melhoras implementadas até o momento, o Brasil ainda precisa avançar muito para enfrentar os desafios inerentes ao ambiente virtual.

7. REFERÊNCIAS

ALVES JR., S.A.G. Políticas Nacionais de Segurança Cibernética: O regulador das telecomunicações – Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT). 2011. Dissertação (Programa de Pós-Graduação em Regulação e Gestão de Negócios) – Faculdade de Economia, Administração e Contabilidade, Universidade de Brasília (UnB), Brasília, 2011.

BRASIL. Livro Branco de Defesa Nacional. Brasília: Presidiência da República, 2012.

CANONGIA, C.; GONÇALVES, JR., A.; MANDARINO JR., R. (Orgs). Guia de Referencia para a Segurança das Infraestruturas Críticas da Informação. Versão 01. 2010. Brasília: GSI – Gabinete de Segurança Institucional, 2010.

CHRISPINO, A. Binóculo ou Luneta: os conceitos de política pública e ideologia e seus impactos na Educação. Revista Brasileira de Política e Administração da Educação, v. 21, 2005, pp. 61-90.

DA CRUZ JR., S.C. A segurança e defesa cibernética no brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual. Texto para Discussão 1850. Brasília: IPEA, 2013.

DE CARVALHO, P.S.M. O Setor Cibernético nas Forças Armadas Brasileiras. In: Desafios Estratégicos para a Segurança e Defesa Cibernética. 1ª. Ed. Brasília: Presiência da República, 2011, pp. 13-34.

FERNANDES, J.H.C. Gestão da Segurança e Comunicações. Série Segurança da Informação. 2010

GRAUMAN, B. Cyber-security: The vexed question of global rules. Bruxelas,: SDA – Security & Defense Agenda, 2013.

GSI – GABINETE DE SEGURANÇA INSTITUCIONAL. Portaria 34, de 5 de agosto de 2009. Publicada no DOU em 06/08/2009. Brasília: DOU, 2009b.

GSI – GABINETE DE SEGURANÇA INSTITUCIONAL. Portaria 45, de 8 de setembro de 2009. Publicada no DOU em 09/09/2009. Brasília: DOU, 2009a.

HOSANG, A. Política nacional de segurança cibernética: uma necessidade para o Brasil. Monografia do Curso de Altos Estudos de Política e Estratégia. Departamento de Estudos da Escola Superior de Guerra. ESG, Rio de Janeiro, 2011.

ISONI, M.M.; VIDOTTI, S.A.B.G. E-crime em ambientes digitais informacionais da Internet. DataGramaZero – Revista de Ciência da Informação, v.8, n.2, 2007.

MANDARINO JR., R.; CANONGIA, C. (Orgs.). Livro Verde: Segurança Cibernética no Brasil. Brasília: GSI – Gabinete de Segurança Institucional, 2010.

MARSIANO, J.L.P. Bases teóricas para a formulação de políticas de informação. Informação & Sociedade: Estudos, v.16, n.2, 2006, pp. 37-50.

MINISTÉRIO DA DEFESA. Estratégia Nacional de Defesa. 2ª. Ed. Brasília: Ministério da defesa, 2008.

MINISTÉRIO DA DEFESA. Minuta de nota de coordenação doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Exército Brasileiro – Estado-Maior do Exército, Brasília, 2010.

RELYEA, H.C. Homeland secutiry and information. Government Information Quarterly, v.19, n. 3, 2002, pp. 213-233.

REVISTA ÉPOCA. Julho de 2013. Numero: 792 - Rio de Janeiro

SOUZA, C. Políticas Públicas: uma revisão da literatura. Sociologias, v.8, n.16, 2006, pp. 20-45.

TAKEMURA, T.; OSAJIMA, M.; KAWANO, M. Positive analysis on vulnerability, information security incidents, and the countermeasures of Japanese internet service providers. World Academy of Science, Engineering and Technology, v.2, 2008, pp. 10-26.