Segurança cibernética: política brasileira e a experiência internacional

Alcyon Ferreira de Souza Junior
Universidade Católica de Brasília (UCB)

Rosalvo Ermes Streit
Universidade Católica de Brasília (UCB)

O ciberespaço comporta diferentes serviços baseados em infraestruturas críticas que necessitam de proteção contra os crimes cibernéticos, como as tentativas de acesso a ativos de informação das organizações públicas e privadas. Nesse contexto, as políticas de segurança cibernética são fundamentais, pois definem o marco regulamentar a partir do qual as ações de segurança cibernética são estabelecidas e monitoradas, e os papeis e as responsabilidades são designados. Este artigo aborda o tema da segurança cibernética e a sua importância em nível mundial. Para isso, realiza-se pesquisa documental com o uso da técnica de análise de conteúdo para comparar as diretrizes da Política Cibernética de Defesa do Brasil (PCD) com as diretrizes das políticas de outros países (EUA, Índia, África do Sul e Reino Unido). O objetivo é enriquecer a discussão de ações nessa área.

Palavras-chave: segurança da informação, internet, tecnologia da informação, administração federal

Ciberseguridad: la política brasileña y la experiencia internacional

El ciberespacio comprende diferentes servicios basados en infraestructuras críticas que necesitan protección contra los delitos cibernéticos, como los intentos de acceso a los activos de información de las organizaciones públicas y privadas. En este contexto, las políticas de seguridad cibernética son críticas porque definen el marco regulatorio desde el cual se establecen y supervisan las acciones de seguridad cibernética, bien como se designan funciones y responsabilidades. En este artículo se aborda el tema de seguridad cibernética y su importancia a nivel mundial. En este sentido, llevamos a cabo una investigación documental utilizando la técnica de análisis de contenido para comparar los lineamientos de la Política de Defensa Cibernética de Brasil (PCD) con las directrices de políticas de otros países (EE.UU., India, Sudáfrica y el Reino Unido). El objetivo es enriquecer la discusión de las acciones en este ámbito.

Palabras clave: seguridad de la información, internet, tecnología de la información, administración federal

[Artigo recebido em 23 de abril de 2015. Aprovado em 11 de julho de 2016.]

Cyber security: Brazilian politics and international experience

Cyberspace comprises different services based on critical infrastructure that needs protection against cyber crimes such as attempts to access information assets of public and private organizations. In this context, cyber security policies are critical because they define the regulatory framework from which cyber security actions are established and monitored, as well as roles and responsibilities are assigned. This article addresses the cyber security subject and its worldwide importance. In this regard, we carry out a documentary research using content analysis technique to compare the guidelines of the Brazilian Cyber Defense Policy (PCD) against policies of other countries (USA, India, South Africa and UK). The goal is to enrich the discussion of actions in this area.

Keywords: information security, internet, information technology, federal administration

Introdução

A rede mundial de computadores é utilizada por vários órgãos públicos nacionais, e esses dados necessitam de proteção para assegurar a sua confidencialidade. As estatísticas organizadas pelo Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), apresentam informações de ataques, invasões, relatos de incidentes e de roubo de informações na internet, reportados no período de 1999 a 2013 (Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil, 2015). Observa-se que a varredura de ativos de rede e seus serviços (*scan)*, que testa as portas lógicas de servidores remotos, invalidando os provedores de serviço por sobrecarga, totaliza aproximadamente 46% por cento dos ataques totais em 2013. Em 2013, o Cert.br registrou 352.925 notificações de incidentes de segurança ocorridos na internet brasileira. Apesar da queda de 24,3% em relação aos incidentes registrados em 2012, houve um aumento de 43% das notificações de computadores comprometidos (grande maioria referente a servidores Web que tiveram suas páginas desfiguradas) e um aumento de 23% das notificações de tentativas de fraude.

Os ativos de informação são essenciais para a administração pública federal (APF), porém, conforme os dados apresentados no parágrafo anterior, estão expostos a grandes riscos. Desse modo, os pilares da segurança da informação – que são a disponibilidade, a integridade, a confidencialidade e a autenticidade – estão sujeitos a vulnerabilidades (Mandarino Júnior; Canongia, 2010).

Esse ambiente, que comporta vulnerabilidades e está sujeito a ataques para o acesso indevido a informações importantes armazenadas em redes corporativas e governamentais, requer atenção cautelosa das autoridades responsáveis. Para se ter uma ideia dos tipos de risco, Pinheiro (2009) apresenta uma lista das maiores vulnerabilidades observadas em ambientes cibernéticos: (i) dependência de sistemas e tecnologias externas; (ii) baixo investimento em pesquisa e desenvolvimento, em centros de pesquisas e universidades, na área da segurança da informação; (iii) infraestrutura de telecomunicação e energia obsoleta ou estrangeira; (iv) baixo desenvolvimento e cultura nos temas de segurança da informação e de proteção do conhecimento nas instituições; (v) baixa capacitação do Poder Judiciário na matéria de delito cibernético e prova eletrônica; (vi) legislação que permita responder às solicitações internacionais de cooperação; (vii) permissão da rastreabilidade; (viii) falta de padronização de respostas a incidentes; e (ix) falta de um plano de segurança cibernética brasileira implementado.

Observa-se que os registros de ataques cibernéticos são crescentes em nível mundial e se caracterizam como um grande desafio para os governos. Por esse

motivo, segurança e a defesa cibernética assumem importância cada vez maior como funções estratégicas de governo.

Em 2008, foi publicado, pelo Presidente da República, o Decreto nº 6.703, de 18 de dezembro (Brasil, 2008), que aprovou a Estratégia Nacional de Defesa (END). Em 2012, essa estratégia foi revista, afirmando-se necessária a tomada de medidas para a segurança das áreas de infraestruturas críticas, inclusos os serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações. E o trabalho de coordenação, avaliação, monitoramento e redução de riscos foi designado ao Gabinete de Segurança Institucional da Presidência da República (GSI) (Brasil, 2012a). O Decreto, ainda, afirma que o Comandante do Exército é responsável pela aplicação da END, formulará a sua política e doutrina de defesa cibernética e preparará seus órgãos operativos e de apoio para o cumprimento da destinação constitucional.

Após o lançamento da END, foi criada a Política Cibernética de Defesa (PCD), em 2012, que contempla as diretrizes para a aplicação e o desenvolvimento de ações em todos os componentes da expressão militar do poder nacional, bem como nas entidades que venham a participar de atividades de defesa ou de guerra cibernética (Brasil, 2012b). A PCD estabeleceu a criação de uma equipe de respostas a incidentes, para a realização de exercícios de guerra e simulações de ataques. Além disso, a PCD criou o Sistema Militar de Defesa Cibernética (SMDC), nas Forças Armadas, com a competência de reprimir os crimes cibernéticos. O SMDC envolve a participação de militares, civis e acadêmicos, e deve assegurar de forma conjunta o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas, bem como impedir ou dificultar a sua utilização contra interesses da defesa nacional.

Contudo, o documento da política não trata de aspectos que são fundamentais para a constituição de cooperações internacionais, ou seja, alianças estratégicas para contribuições e crescimento das partes aliadas. Por exemplo, nas políticas de segurança dos Estados Unidos da América (2009), República da África do Sul (2011) e Índia (2011), constam diretrizes e ações relacionadas à cooperação internacional para promover a coordenação global de respostas a tratamentos e vulnerabilidades, participação em eventos para nivelamento de conhecimento e criação de parcerias bilaterais e/ou multilaterais para ações coordenadas.

Verifica-se, desse modo, que há diretrizes distintas entre as políticas de segurança cibernética de diferentes países, apesar dos problemas e vulnerabilidades nessa área serem de conhecimento comum. Essa constatação pode ser esperada para algumas diretrizes específicas, mas surge a dúvida sobre aspectos de mesma natureza e de grande relevância. Assim, em razão da importância do tema para a

segurança e a soberania nacional, o presente estudo tem como objetivo verificar a aderência das diretrizes da Política de Segurança Cibernética do Brasil (PCD) com as políticas de outros países nessa área, com vistas a enriquecer a discussão das ações futuras de defesa do espaço cibernético brasileiro.

Segurança cibernética

Moresi (2012) alerta que a segurança cibernética é um dos grandes desafios a ser enfrentado pelos governos de diversos países, particularmente no que se refere à garantia do funcionamento de infraestruturas críticas, tais como energia, defesa, transporte, telecomunicações, finanças, entre outras. Os termos defesa (do inglês, *cyberdefense*), segurança (do inglês, *cybersecurity*) e guerra cibernética (do inglês, *cyberwar*) são parecidos, mas, ao mesmo tempo, trazem diferentes conceitos e, por isso, é importante esclarecer as diferenças entre eles.

Podemos definir o termo guerra cibernética como uma ferramenta de ação política ou militar. Já o perito especialista em crimes digitais Milagre (2012) define guerra cibernética mediante três abordagens diferentes, segundo o desenvolvimento do conflito, segundo o tipo de arma e segundo as forças empregadas em confronto:

> Cyberwar segundo o desenvolvimento do conflito: guerra fria (conflitos indiretos, de espionagem, de subversão ou tecnológicos) ou guerra subversiva ou de guerrilha (guerra não convencional, cujo escopo é subverter a ordem estabelecida) – Também pode se enquadrar em guerra psicológica; [...]
>
> Cyberwar segundo o tipo de arma: Guerra tecnológica;
>
> Cyberwar segundo as forças em confronto: Guerra irregular, travada entre um exército e uma guerrilha, com campo de batalha indefinido. De difícil distinção entre civis e soldados. Mas também pode ser regular, entre exércitos virtuais (Milagre, 2012, p.10).

Para Mandarino Júnior e Canongia (2010), a segurança cibernética compreende aspectos e atitudes, tanto de prevenção quanto de repressão, enquanto a defesa cibernética abrange ações operacionais de combates ofensivos. De acordo com a Portaria n˚ 45 (Brasil, 2009), a esfera pública utiliza dois termos alinhados à noção da segurança cibernética: (i) infraestrutura crítica da informação; e (ii) ativos de informação. Nesse documento, considera-se infraestrutura crítica da informação o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. A noção de ativos de informação, por sua vez, refere-se aos meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

A revisão de literatura deste estudo permitiu identificar três níveis de segurança cibernética adotados pelos países, conforme mostra a Figura 1.

Figura 1 – Níveis de segurança cibernética

Fonte: Elaboração própria.

A seguir, são apresentados os níveis distintos de segurança em mais detalhes e a sua importância no cenário atual.

Estratégia Nacional de Defesa (END)

A END, aprovada no final de 2008 e revista em 2012, estabeleceu diretrizes relativas ao preparo e ao emprego das Forças Armadas para a defesa nacional, com destaque a três setores de importância estratégica: o espacial, o cibernético e o nuclear (Brasil, 2012a).

> A Estratégia Nacional de Defesa é o **vínculo entre o conceito e a política** de independência nacional, de um lado, e as Forças Armadas para resguardar essa independência, de outro. Trata de questões políticas e institucionais decisivas para a defesa do País, como os objetivos da sua "grande estratégia" e os meios para fazer com que a nação participe da defesa. Aborda, também, problemas propriamente militares, derivados da influência dessa 'grande

> estratégia' na orientação e nas **práticas operacionais** das três Forças. A Estratégia Nacional de Defesa será complementada por planos para a paz e para a guerra, concebidos para fazer frente a diferentes hipóteses de emprego (Brasil, 2012a, p. 5, grifo nosso).

A END abrange o conceito de segurança cibernética, setor cuja responsabilidade de proteção é do governo. Entretanto, conforme Acácio (2012, p. 7), no detalhamento da END, "o setor cibernético é aquele que possui mais incertezas e menos informações". Nesse aspecto, cabe destacar a dependência tecnológica do Brasil em relação a produtos importados e a operadoras não nacionais de telecomunicações. Essa dependência em relação a países com elevado grau de desenvolvimento na área da tecnologia da informação e comunicações dificilmente poderá ser superada em curto prazo e gera a necessidade de desenvolvimento de uma estratégia de grande alcance.

De acordo com Alves Júnior (2011), os Estados Unidos já possuem tradição em formular estratégias de segurança cibernética. Tanto a administração de Bill Clinton, em 2000, quanto a de George W. Bush, em 2002 e 2008, elaboraram programas com esse mote.

Poltica Cibernética de Defesa (PCD)

De acordo com Hunker (2010), uma política de segurança cibernética refere-se às medidas tomadas para garantir a segurança no ciberespaço. Não apenas as agências governamentais devem construir tais medidas, mas as empresas privadas, provedores de internet e ONGs devem adotar políticas de segurança cibernética. Segundo o autor, o primeiro pensamento evocado pela política de segurança cibernética é a proteção contra a cibercriminalidade. No entanto, as políticas também baseiam-se em infraestruturas ligadas ao ciberespaço e ao armazenamento de dados, entre outras, respeitando a cultura e peculiaridade de cada país.

Conforme Brasil (2012b, p. 11), a PCD "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". A PCD 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. Os seus objetivos são:

> 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;

> 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 (Brasil, 2012a, p. 2).

A estratégia tem uma forte relação com a política. Segundo Ribeiro (2011, p. 161), o escopo de um direcionamento estratégico contempla a criação de um centro especializado de referência, o desenvolvimento de metodologias e sistemas, a definição de métricas e indicadores e a cooperação entre os setores público e privado, além da comunidade internacional. Esses elementos devem ter como base um arcabouço legal e um marco regulatório consistentes com essas finalidades.

Nas políticas de segurança elencadas neste estudo, alguns elementos são recorrentes, sendo que os que mais se destacam são: (i) a criação de um centro de coordenação de segurança cibernética; (ii) a criação de equipes de respostas a incidentes; (iii) a preocupação com a capacitação, o desenvolvimento e a pesquisa; (iv) a promoção e fortalecimento de cooperação local; e (v) a aquisição de criptografia própria ou adquirida.

A partir da análise das políticas e das estratégias, infere-se que um modelo de segurança cibernética deve englobar a formulação, implantação, controle e revisão de políticas, diretrizes, regras, procedimentos, instrumentos e tecnologias que orientem a prática de gestão desse modelo. Ainda, entende-se que, para a solidez do modelo, é importante que a política de segurança cibernética considere todas as lacunas de segurança e, sobretudo, a participação dos atores indispensáveis ao seu planejamento, execução, verificação e ação.

Modelos de Segurança Cibernética

Conforme comentado, a END e a PCD estabelecem os níveis de operacionalização e as diretrizes relacionadas à segurança cibernética. Na PCD (Brasil, 2012b), as diretrizes explicitam as atividades a serem implementadas pelo Ministério da Defesa, contendo elementos doutrinários básicos e de alto nível. Cabe ressaltar as diretrizes que contemplam o alcance do objetivo de desenvolvimento do setor cibernético (St Ciber) da PCD:

> 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 S(MD)C; [...] f) designar o órgão central do SMDC como responsável por propor as inovações e atualizações de doutrina para o setor cibernético no âmbito da Defesa (Brasil, 2012a, p.3).

Com base nessas diretrizes, entende-se que um dos grande desafios será a elaboração de um documento que contemple os requisitos e os elementos de governança, com tópicos relacionados ao planejamento, estratégia e o processo decisório integrados. Neste trabalho, o documento é denominado Modelo de Segurança Cibernética.

Mandarino Júnior e Canongia (2010) alertam que ainda não existe um modelo formatado e testado para a formalização de ações estruturadas para a prevenção e combate a ataques e crimes cibernéticos. Contudo, cabe ressaltar que o Governo Federal criou o Grupo Técnico de Segurança Cibernética, mediante a Portaria n˚ 45 (Brasil, 2009), composto por representantes dos Ministérios da Justiça, da Defesa, das Relações Exteriores e Comandantes das Forças Armadas, com o objetivo de propor diretrizes e estratégias para a segurança no âmbito da administração pública federal. Desse modo, observa-se o empenho do governo para o desenvolvimento de um modelo de segurança cibernética.

Em termos internacionais, é possível verificar diversos esforços para a criação de modelos de segurança cibernética. Um bom exemplo é o do Departamento de Energia americano, que desenvolveu o Modelo Federal para a Segurança Cibernética. De acordo com *Network Security* (2009, p. 2), esse modelo "atua como um programa virtual. Se uma instituição sofre ataque em sua infraestrutura, a comunicação segura e pontual com os outros órgãos da Federação auxiliará a protegê-la do ataque e até mesmo através de resposta ativa". Em seu estado atual, o sistema transmite informações sobre endereços IP e nomes de domínio suspeitos, mas, em breve, será capaz de compartilhar endereços de e-mail suspeitos e URLs da web entre os sistemas da Federação. O desenvolvimento do sistema ganhou o Prêmio de Inovação em Segurança Cibernética de 2009 (do inglês, *DoE 2009 Cyber*

Security Innovation Achievement Award). Além de proteger ativos do governo, a equipe acredita que pode ser utilizado no setor privado.

O *National Institute of Standards and Technology* (Nist), órgão americano responsável por promover a inovação e a competitividade industrial mediante o desenvolvimento de padrões que garantem melhor segurança econômica e qualidade de vida, desenvolveu e mantém um modelo criado com a colaboração entre o governo e o setor privado. Esse modelo é um conjunto de padrões industriais e melhores práticas que ajudam as organizações a gerenciar os riscos de cibersegurança (National Institute of Standards and Technology, 2014). O modelo guia as atividades de cibersegurança, considerando os riscos relacionados a essa área como parte dos riscos de gestão dos processos de negócio (utiliza uma linguagem comum para a gestão desses riscos).

Os modelos são importantes para o desenvolvimento e a compreensão da teoria da segurança cibernética, pois ajudam a mitigar os riscos de cibersegurança. Entretanto, ainda estão em fase de organização pelos países. De acordo com Baker, Waterman e Ivanov (2010), que realizaram pesquisa em nível mundial com 600 executivos de segurança de TI, existe um modelo comum a todos os países pesquisados:

> Uma questão levantada reiteradas vezes em entrevistas com especialistas de diferentes setores e países foi a maneira como os governos estavam se organizando para enfrentar a nova ameaça. Existem modelos comuns — todos os países pesquisados, por exemplo, estabeleceram equipes de resposta a emergências em computadores (CERTs – *Computer Emergency Response Teams*) para tratar de resposta a incidentes, embora sua eficácia varie, de acordo com as entrevistas. No entanto, muitos governos continuam a lutar com a questão do "organograma" e, em alguns países, o resultado é, claramente, um trabalho em andamento (Baker; Waterman; Ivanov, 2010, p. 36).

Metodologia

Para a avaliação da aderência das diretrizes da Política de Defesa Cibernética do Brasil (PCD) com as políticas de outros países, realizou-se pesquisa documental, de natureza qualitativa. A pesquisa documental, conforme Godoy (1995), é constituída pelo exame de materiais que ainda não receberam um tratamento analítico ou que podem ser reexaminados buscando-se interpretação nova ou complementar.

Foram analisadas as políticas de segurança cibernética dos seguintes países: Estados Unidos da América (2009), Reino Unido (2011), África do Sul (2011), Índia (2011) e Brasil (2012a). A seleção dos países ocorreu devido à disponibilidade de acesso aos documentos para a pesquisa. E, para a compreensão dessas políticas,

utilizou-se a análise de conteúdo, que é uma técnica de análise de dados qualitativa. Cabe destacar que a análise de conteúdo tem sido uma das técnicas mais utilizadas para a pesquisa documental, ou seja, a codificação e análise dos dados (Godoy, 1995). Segundo Bardin (1977), a análise de conteúdo compreende:

> [...] um conjunto de técnicas de análise das comunicações, visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitem a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) dessas mensagens (Bardin, 1977, p. 42).

Neste trabalho, utilizou-se a frequência como medida de contagem de aparição da unidade de análise definida para o estudo: diretrizes das políticas. Os segmentos de texto foram selecionados em função da unidade de análise.

Após a categorização e a classificação dos segmentos de textos, foi realizada a avaliação desses resultados, mediante tratamento estatístico simples. Essa avaliação proporcionou a organização dos dados em tabelas e a comparação das políticas de segurança dos cinco países.

Análise e interpretação dos dados

Inicialmente, com a análise de conteúdo, foram identificadas as categorias e realizados os agrupamentos das diretrizes das políticas de segurança cibernética. As categorias e suas descrições encontram-se no Quadro1.

Quadro 1 – Categorias resultantes da análise de conteúdo

Categoria	Descrição
Segurança da informação	Adequação de estruturas e normas em segurança cibernética.
Interação com outros órgãos e atores	Interações com órgãos da APF, atores locais e internacionais (indivíduos e organizações).
Cultura de segurança cibernética	Desenvolvimento da cultura de segurança cibernética.
Cooperação técnica	Cooperação com outros atores para desenvolvimento da segurança cibernética.
Infraestrutura de segurança	Ações relacionadas à infraestrutura para o aprimoramento da segurança cibernética.
Normatização	Desenvolvimento e adequação das políticas e normas de segurança cibernética.
Capacitação em segurança cibernética	Capacitação e mobilização de pessoal especializado.

Fonte: Elaboração própria.

Durante o processo de categorização, foi criado um código para identificar as diretrizes das políticas em estudo, composto por dois campos:

- primeiro campo: indica a sigla dos países, segundo a norma internacional ISO 3166 de siglas: (i) Brasil – BR; (ii) África do Sul – ZA; Estados Unidos da América – US; Índia – IN; e Reino Unido – GB;
- segundo campo: numeração sequencial, para a identificação de cada diretriz.

Devido à objetividade, à precisão e à clareza dos conteúdos dos documentos, não houve necessidade de mais de um ciclo de categorização, conforme orienta Bardin (1977). O Quadro 2 apresenta o número de diretrizes das políticas de segurança dos países identificadas para cada categoria.

Quadro 2 – Categorias da análise de conteúdo e quantidade de diretrizes

Categorias	Quantidade de diretrizes					Total por categoria
	Brasil	África do Sul	Estados Unidos	Índia	Reino Unido	
Segurança da informação	9	9	14	25	29	86
Normatização	14	9	9	4	12	48
Cultura de segurança cibernética	6	11	8	3	9	37
Interação com outros órgãos e atores	4	8	8	3	13	36
Cooperação técnica	9	4	5	0	5	23
Capacitação em segurança cibernética	7	0	2	2	6	17
Infraestrutura de segurança	1	5	0	0	5	11
Total	**50**	**46**	**46**	**37**	**79**	**258**

Fonte: Elaboração própria.

Verifica-se, no Quadro 2 que o Brasil privilegiou aspectos normativos nas diretrizes da PCD, enquanto que os Estados Unidos, Índia e Reino Unido abordaram com mais intensidade aspectos relacionados à segurança da informação. A África do Sul, por

sua vez, favoreceu diretrizes relacionadas à cultura na sua política de segurança cibernética. Além disso, com os resultados das categorizações, foi possível observar que as políticas dos Estados Unidos e da Índia não apresentam diretrizes sobre infraestrutura de segurança.

Finalizada a fase de categorização, iniciou-se a análise das políticas dos países, considerando as diretrizes que se encontram em uma mesma categoria, para avaliar a relação entre elas. Essa análise teve como referência as diretrizes da PCD do Brasil, que foram comparadas com as diretrizes das políticas dos demais países. Para tanto, foram definidos atributos que caracterizam a relação entre as políticas dos países, conforme mostra o Quadro 3.

Quadro 3 – Atributos para a comparação das políticas de segurança cibernética dos países sob análise

Atributo	Descrição
Aderência	Indica aderência entre as diretrizes, ou seja, ambas as diretrizes possuem as mesmas orientações.
Aderência parcial	Esse atributo assinala que a diretriz da política brasileira possui pelo menos uma característica coincidente com a política do país estrangeiro. Por exemplo, na categoria Interação com outros órgãos e atores, a diretriz BR-27 menciona: > 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 Ciência, Tecnologia e Inovação, nas áreas de interesse do setor cibernético. A diretriz norte-americana equivalente, por sua vez, relata: > O Presidente deve considerar a nomeação de um oficial de segurança cibernética na Casa Branca para gerar relatórios para o NSC e ainda acumulará funções para coordenar a segurança cibernética relacionada com as políticas e atividades da nação. Esse indivíduo será consultor para resolver prioridades concorrentes e coordenar interagências desenvolvimento das políticas e estratégias para cibersegurança. Nesse caso, a relação de aderência é parcial, pois a diretriz brasileira fomenta o envolvimento de outros atores, com a criação de um comitê, enquanto a diretriz americana propõe a designação de um responsável.
Não há aderência	As diretrizes da categoria não possuem aderência entre si.
Conflito entre as diretrizes	As diretrizes de uma mesma categoria são divergentes entre si. Cabe destacar que, no estudo, não foi identificada nenhuma diretriz brasileira conflitante com as diretrizes dos demais países.

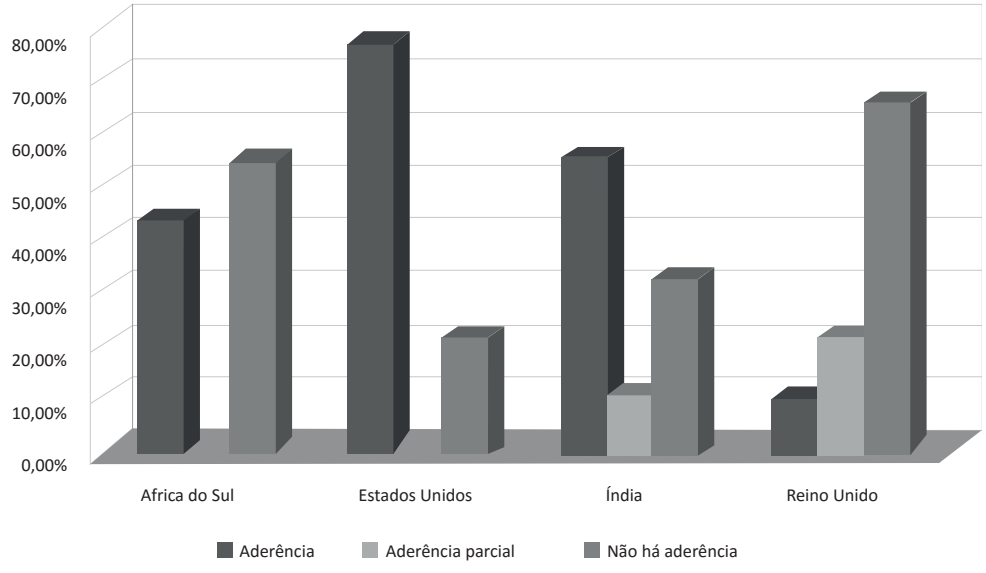
Fonte: Elaboração própria.

O processo de comparação da PCD do Brasil com as políticas da África do Sul, Estados Unidos, Índia e Reino Unido, utilizando-se os atributos especificados acima, foi realizado para todas as categorias. Cabe destacar que não foi identificado conflito entre as diretrizes do Brasil com as dos demais países. Os principais resultados são apresentados a seguir.

Categoria Segurança da informação

Nessa categoria, conforme se observa na Figura 2, evidenciou-se uma forte aderência entre as diretrizes do Brasil e as dos Estados Unidos, e uma maior divergência em relação às diretrizes do Reino Unido. O Reino Unido possui cinco diretrizes que dizem respeito a ações de combate direto ao ciberterrorismo e, principalmente, ao crime cibernético, visando garantir a segurança dos atores locais, como indústrias e áreas civis, para fomentar o desenvolvimento nacional, respeitando o direito individual de privacidade. Esses aspectos não são abordados na PCD do Brasil.

Figura 2 – Resultado da análise de aderência da categoria Segurança da informação



Fonte: Elaboração própria.

Categoria Interação com outros órgãos e atores

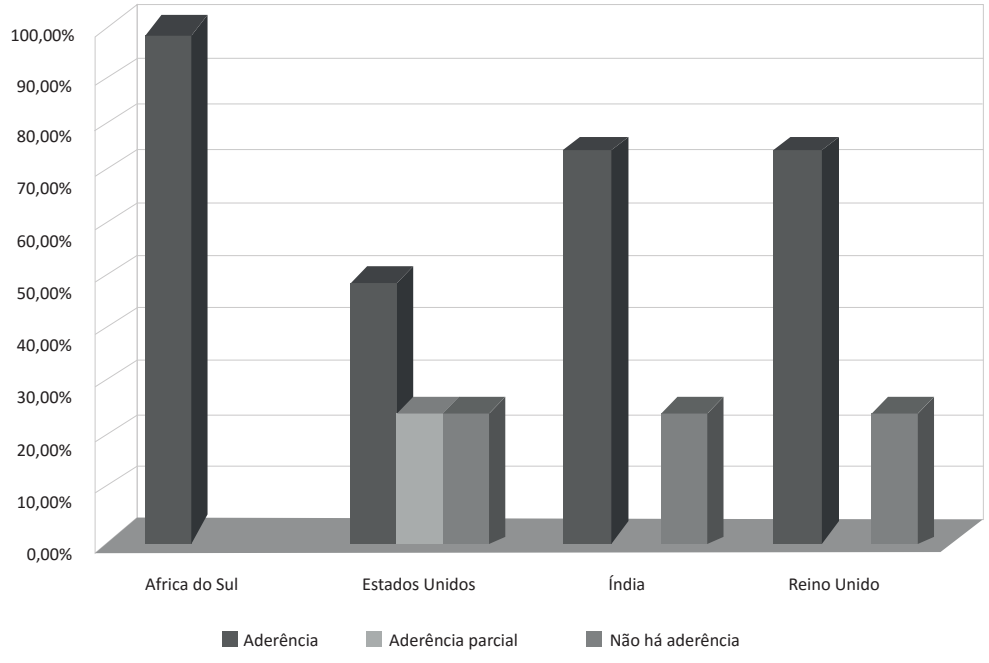
As diretrizes do Brasil, nessa categoria, estão totalmente aderentes com as diretrizes sul-africanas, conforme se verifica na Figura 3. Nesse tema, contudo, constata-se que

não há uma adesão maior que 50% com as diretrizes norte-americanas, pois essas não abordam aspectos relacionados à inserção da defesa cibernética nos exercícios de simulação de combate e nas operações conjuntas, que constam na PCD.

Em relação à Índia, cabe destacar a aderência das diretrizes que tratam do estabelecimento de critérios de risco, inerentes aos ativos de informação, e da realização do seu gerenciamento visando à redução dos riscos a níveis aceitáveis nas infraestruturas críticas de interesse da defesa nacional. Outra aderência com a Índia nessa categoria refere-se a uma coordenação central para identificar organizações de segurança nacional e organizar os assuntos relacionados à segurança da informação no país.

Nessa categoria, a PCD deixou a desejar em relação à política do Reino Unido, que orienta o estabelecimento de novas parcerias operacionais com setores privados, para a construção de pontos de informação importantes no ciberespaço. Essa diretriz evidencia a preocupação do Reino Unido no relacionamento com o setor privado na área da segurança e da defesa cibernética.

Figura 3 – Resultado da análise de aderência da categoria Interação com outros órgãos e atores

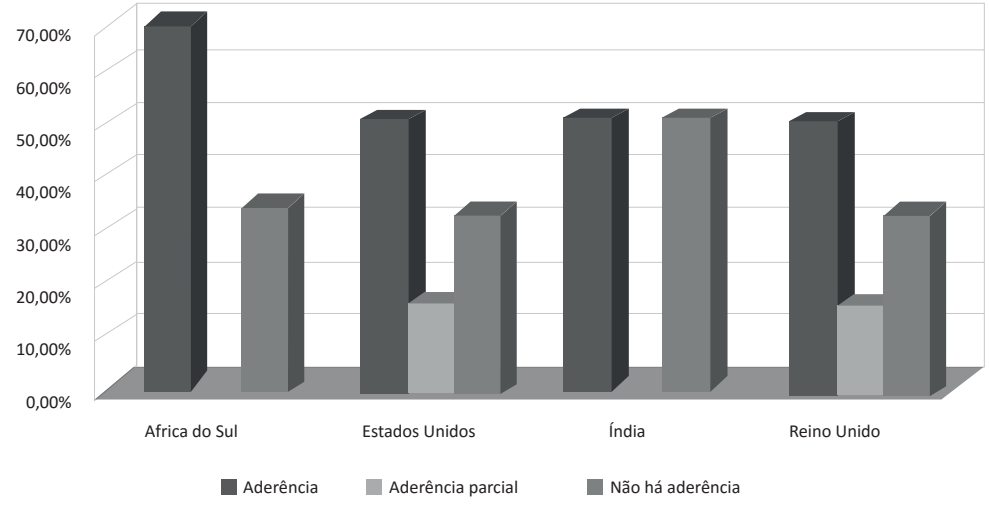


Fonte: Elaboração própria.

Categoria Cultura de segurança cibernética

A PCD possui maior aderência com as diretrizes das políticas dos países estrangeiros nessa categoria, conforme mostra a Figura 4. Entretanto, algumas diretrizes que não são abordadas na PCD possuem destaque nas políticas da África do Sul e dos Estados Unidos, como: (i) desenvolvimento da consciência sobre o risco no ciberespaço (diretriz da África do Sul); (ii) elaboração de campanhas nacionais de sensibilização sobre cibersegurança (diretriz da África do Sul); (iii) construção de uma visão de gerenciamento da identidade e da estratégia, que aborda desde a privacidade a interesses das liberdades civis (diretriz dos EUA); (iv) revisão e atualização do regime de privacidade existente (diretriz da África do Sul); (v) envolvimento da população na discussão de medidas de segurança para a solução de problemas (diretriz dos EUA).

Figura 4 – Resultado da análise de aderência da categoria Cultura de segurança cibernética



Fonte: Elaboração própria.

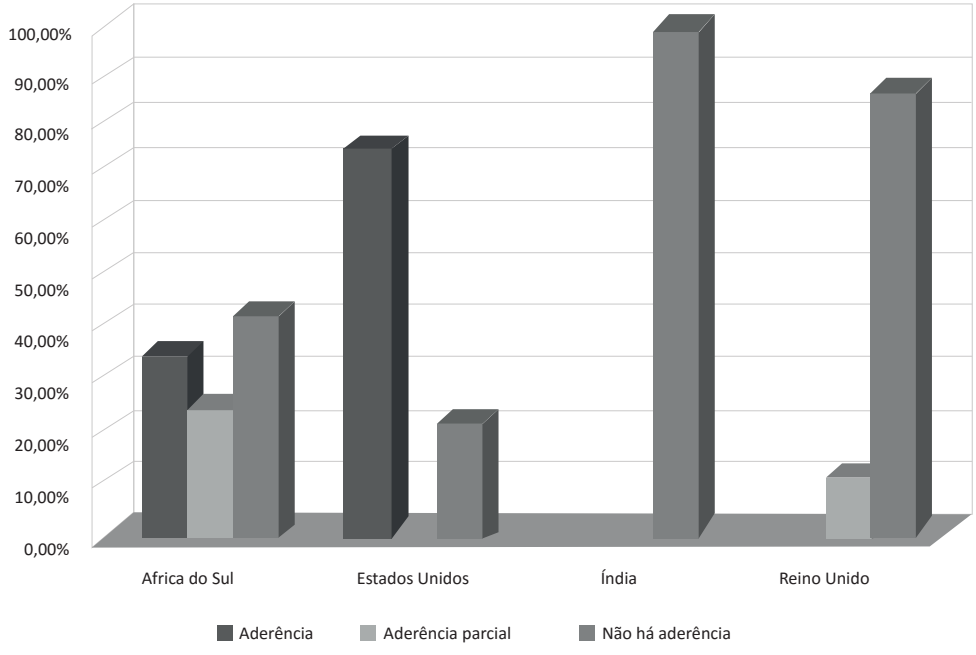
Categoria Cooperação técnica

A Figura 5 mostra que, nessa categoria, não foi classificada nenhuma das diretrizes da política de segurança cibernética da Índia. Cabe destacar duas diretrizes relativas à cooperação técnica dos países estrangeiros que não foram identificadas na PCD brasileira: (i) afiliar as organizações internacionais a fim de promover respostas coordenadas globais às ameaças e vulnerabilidades, manter

a par os envolvidos e desenvolver uma frente de cibersegurança (diretriz da África do Sul); e (ii) coordenar políticas e estratégias de inteligência e militar para o ciberespaço, inclusive para combater o terrorismo na internet (diretriz dos EUA). Com relação a esses itens, observa-se que a política brasileira tem o seu foco nas respostas a incidentes, com a criação de um banco de dados de ações e de incidentes ocorridos.

Cabe ressaltar a aderência das políticas brasileira e norte-americana nas diretrizes que destacam a necessidade de colaboração com o órgão coordenador de segurança cibernética dos países.

Figura 5 – Resultado da análise de aderência da categoria Cooperação técnica



Fonte: Elaboração própria.

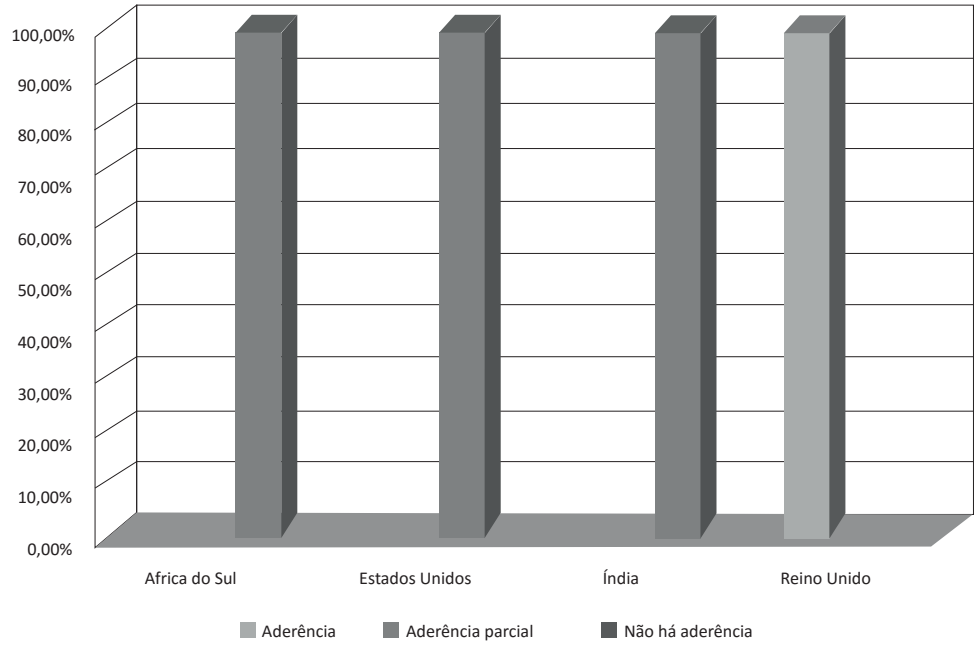
Categoria Infraestrutura de segurança

Nessa categoria, de acordo com a Figura 6, identificou-se total aderência da PCD com a política do Reino Unido. As políticas dos dois países norteiam a criação de estruturas de inteligência cibernética, visando à produção de conhecimento nesse setor. As demais políticas analisadas não explicitam aspectos relacionados à criação e ao desenvolvimento de infraestruturas de segurança.

Ainda, a política do Reino Unido também demonstra preocupação em construir e manter redes de tecnologia de informação e comunicação (TIC) do governo e

ajudar os consumidores a responder a ameaças cibernéticas mediante o uso de mídias sociais para o fornecimento de avisos sobre fraudes ou outras ameaças online. Essas preocupações não foram identificadas na PCD.

Figura 6 – Resultado da análise de aderência da categoria Infraestrutura de segurança



Fonte: Elaboração própria.

Categoria Normatização

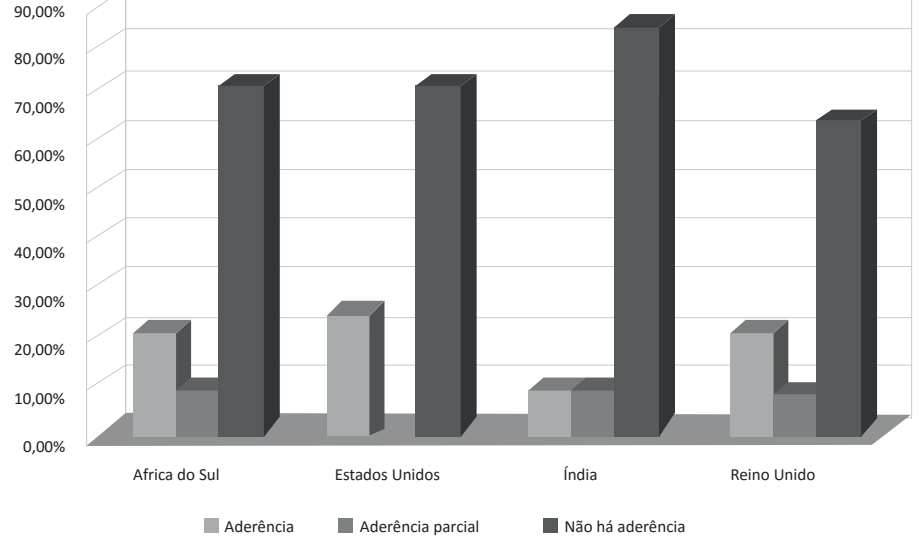
Nessa categoria, há uma particularidade relacionada à estrutura de coordenação de segurança cibernética. O Brasil separa a responsabilidade pelas ações de coordenação dos assuntos estratégicos. A segurança cibernética é de responsabilidade do GSI da Presidência da República, e a responsabilidade pela defesa cibernética é do Sistema Militar de Defesa Cibernética (SMDC) e do Centro de Defesa Cibernética (CDCiber), coordenado pelo Exército Brasileiro e Ministério da Defesa (diretriz BR-43). A estrutura dos Estados Unidos, por outro lado, define o Departamento de Defesa (DoD) como o órgão central responsável pela coordenação da segurança e da defesa cibernética.

A política do Reino Unido apresenta duas diretrizes com orientações normativas que não foram contempladas na PCD: (i) incentivo do governo ao uso de normas e orientações para ajudar as indústrias a elevar o padrão de

segurança; e (ii) a cooperação do Estado na execução da lei e negação de refúgio a cibercriminosos internacionais. A política indiana também indica uma diretriz de ações de incentivo e políticas para promover a aderência a melhores práticas internacionais de segurança.

Cabe destacar a diretriz norte-americana que indica o estabelecimento de métricas de desempenho na área da segurança cibernética, identificada somente na política dos Estados Unidos.

Figura 7 – Resultado da análise de aderência da categoria Normatização

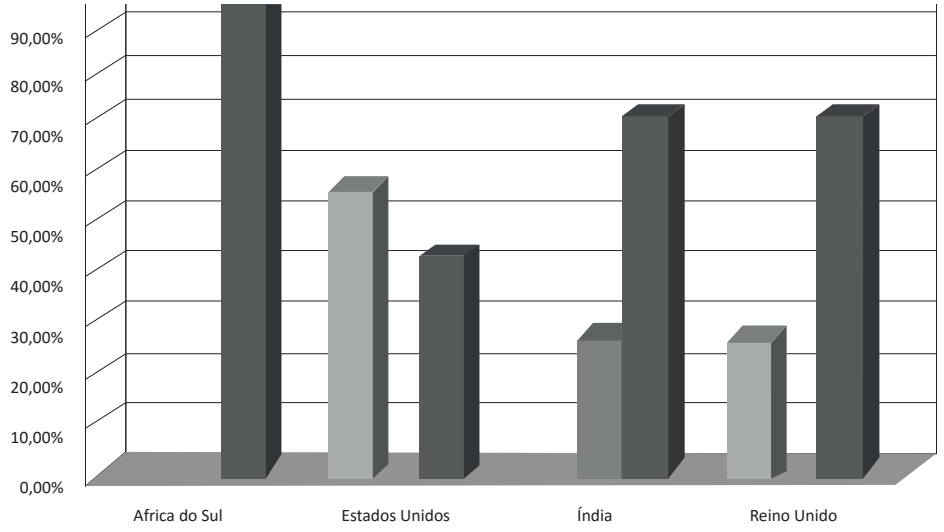


Fonte: Elaboração própria.

Categoria Capacitação em segurança cibernética

Nessa categoria, verificou-se que a PCD não tem aderência com as políticas da África do Sul e da Índia, de acordo com a Figura 8, e há algumas diretrizes comuns com as políticas dos Estados Unidos e do Reino Unido. Vale destacar a diretriz da PCD que enfoca a capacitação de pessoal, e, para fomentar a pesquisa no setor cibernético, a diretriz que orienta a criação de disciplinas em estabelecimentos de ensino. A preocupação com a sustentabilidade do setor também pode ser observada em uma diretriz específica da PCD.

Figura 8 – Resultado da análise de aderência da categoria Capacitação em segurança cibernética



Fonte: Elaboração própria.

Considerações finais

O estudo verificou a aderência da Política Cibernética de Defesa do Brasil (PCD) com as políticas de outros países, com o objetivo de enriquecer a discussão sobre o tema. Foi possível confirmar o destaque do assunto no cenário mundial pela revisão de literatura. Os resultados da pesquisa, por sua vez, permitiram compreender as diretrizes e, sobretudo, as principais diferenças e similaridades das políticas de segurança cibernética analisadas.

A principal limitação para o desenvolvimento do trabalho foi a dificuldade no acesso a documentos das políticas dos países estrangeiros, pois, em alguns casos, são tratados como assunto de segurança nacional. Desse modo, os documentos analisados são os que estavam disponíveis quando da realização do trabalho.

Durante o estudo, observou-se que alguns termos e definições nessa área se confundem, não somente entre os países, mas, também, nas publicações e trabalhos acadêmicos. Essas diferenças de entendimento dificultam a formação de conceitos e a compreensão do assunto pela população. Assim, considera-se de fundamental relevância a construção e a adoção de uma taxonomia de segurança cibernética em nível internacional.

Apesar de algumas dificuldades com a taxonomia, as diretrizes relativas à proteção dos ativos informacionais são abordadas de maneira geral com o mesmo

direcionamento pelos países. Constatou-se que todas as políticas analisadas priorizaram a proteção das informações.

Na comparação com os outros países, percebe-se que a política de segurança cibernética brasileira está bem estruturada. Um aspecto que merece atenção em termos de clareza diz respeito à estrutura de organização, para facilitar o entendimento do funcionamento das hierarquias de responsabilidade. Nesse aspecto, entende-se que a criação de um órgão central para a coordenação da defesa cibernética e da segurança cibernética pode ajudar a direcionar as ações e a normatização do setor, e facilitar a integração das Forças Armadas com os órgãos da administração pública federal nas ações de segurança cibernética. Atualmente, é possível notar que os órgãos e entidades responsáveis atuam de forma desarticulada.

O Brasil é um ator global que hoje tem destaque internacional, em função do desenvolvimento tecnológico tanto na área agrícola quanto no setor de exploração de petróleo e seus derivados. Nesse sentido, a PCD é um marco decisivo e de grande avanço no painel da segurança cibernética nacional e em nível internacional. Assim, entende-se necessária a construção de uma agenda nacional de ações para a adoção das diretrizes que constam na PCD.

Nesse contexto, algumas diretrizes merecem atenção e prioridade devido à sua importância para o desenvolvimento da doutrina que irá nortear as ações no setor cibernético. O desenvolvimento de tecnologias nacionais para o processamento de sistemas sensíveis, comunicação de dados e informações, por exemplo, tanto em nível de algoritmos e sistemas (s*oftwares*), como de equipamentos (*hardwares*), é fundamental para resguardar o Brasil contra ações de espionagem. Cabe destacar a iniciativa brasileira para a implantação da infraestrutura de chaves públicas (ICP Defesa), de crucial importância para garantir a segurança, a confidencialidade e a integridade dos dados e informações.

A interação e o envolvimento de parceiros civis, públicos e privados, auxilia no crescimento da consciência pública sobre a segurança cibernética, promove a educação e treinamento. Esse tipo de diretriz promove a cultura da segurança cibernética. As ações de aculturamento podem se iniciar, inclusive, na educação básica escolar, de maneira que as crianças, em sua formação, já podem ter conhecimento da importância de proteger suas informações. Também acordos de cooperação técnica com universidades e empresas privadas podem ser realizados para o desenvolvimento de metodologias, equipamentos e tecnologias de suporte ao setor cibernético.

A cooperação internacional é outro fator importante para o desenvolvimento da segurança cibernética. Assim como toda aliança, a cooperação deve ser baseada em uma relação de confiança. Diversos países estrangeiros criam esses acordos

de cooperação e explicitam a importância dessas ações em suas diretrizes que compõem as políticas de segurança cibernética. A PCD do Brasil tem essa diretriz no seu escopo e o Brasil já possui acordos bilaterais com países estrangeiros, principalmente com países situados na América do Sul.

Contudo, não há diretrizes específicas relacionadas à prevenção e resposta a desastres para a proteção dos ativos das informações e infraestruturas críticas, principalmente no campo das comunicações. A falta de acesso a canais de comunicação é crítica para a defesa cibernética.

Como oportunidade de evolução do estudo, sugere-se a análise da aderência das diretrizes das políticas dos países estrangeiros às diretrizes existentes na política do Brasil, explorando aspectos que não fazem parte do escopo da PCD e que não fizeram parte do escopo deste trabalho. Também propõe-se que os resultados sejam verificados por especialistas de segurança cibernética, para avaliar se as diretrizes das políticas dos outros países podem indicar lacunas a serem exploradas pelas autoridades brasileiras. Ainda, ficou clara a necessidade de uma taxonomia na área da segurança cibernética, não apenas relacionada a riscos, como se observa em algumas publicações.

Para finalizar, entende-se que as diretrizes adotadas na Política Cibernética de Defesa brasileira são pertinentes e estão muito bem norteadas, apesar de alguns aspectos discutidos neste trabalho, que fazem parte das políticas dos outros países, não serem contemplados. Assim, sugere-se que se aprofunde na discussão sobre a PCD para o aprimoramento da política brasileira nessa área.

Referências bibliográficas

Acácio, Igor D. P. Segurança cibernética na política de defesa brasileira: um caso de securitização? In: Encontro Sul-americano de Defesa e Encontro da Associação Brasileira de Estudos da Defesa, 1./4., 2012, São Paulo. *Anais* … São Paulo: 2012. p. 1-17.

Alves Júnior, Sérgio A. G. *Políticas nacionais de segurança cibernética*: o regulador das telecomunicações – Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT). Brasília: UnB, 2011. Dissertação (Mestrado) – Programa de Pós-Graduação em Regulação e Gestão de Negócios (Regen) da Faculdade de Economia, Administração e Contabilidade (Face) da Universidade de Brasília (UnB), Brasília.

Baker, Stewart; Waterman, Shaun; Ivanov, George. *Sob fogo cruzado*: infraestrutura crítica na era da guerra cibernética. Center for Strategic and International Studies (CSIS). Relatório encomendado pela McAfee, 2010. Disponível em: <http://img.en25.com/Web/McAfee/CIP_report_final_pt-br_fnl_lores.pdf>. Acesso em: 10 mar. 2015.

Bardin, Laurence. Análise de conteúdo. Lisboa: Edições 70, 1977.

Brasil. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial da União (DOU)*, n. 247, Brasília, 19 dez. 2008. Seção 1, p. 4-14. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=19/12/2008&jornal=1&pagina=4&totalArquivos=160>. Acesso em: 09 fev. 2013.

_____. Gabinete de Segurança Institucional. Portaria n˚ 45, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (Creden), o Grupo Técnico de Segurança Cibernética e dá outras providências. *Diário Oficial da União (DOU)*, Brasília, n. 172, 9 set. 2009. Seção 1, p. 2-3. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009>. Acesso em: 09 fev. 2013.

_____. Decreto nº 576, de 17 de julho de 2012. Aprova a revisão da Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial da União (DOU)*, Brasília, n. 247, 17 jul. 2012a. Seção 1, p. 1-3. Disponível em: < http://www2.camara.leg.br/legin/fed/decleg/2013/decretolegislativo-373-25-setembro-2013-777085-publicacaooriginal-141221-pl.html>. Acesso em: 09 jun. 2016.

_____. Portaria n˚ 3.389/MD, de 21 de dezembro de 2012. Dispõe sobre a Política Cibernética de Defesa. *Diário Oficial da União (DOU)*, Brasília, n. 249, 27 dez. 2012b. Seção 1, p. 11-12.

Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert). *Incidentes reportados ao CERT.br – janeiro a dezembro de 2013*. Disponível em: <http://www.cert.br/stats/incidentes/2013-jan-dec/analise.html>. Acesso em: 14 mar. 2015.

Estados Unidos da América (EUA). *Cyberspace policy review*: assuring a trusted and resilient information and communications infrastructure. Washington, DC: The White House, 2009. Disponível em: <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em: 15 mai. 2012.

Godoy, A. S. Pesquisa qualitativa: tipos fundamentais. *Revista de Administração de Empresas*, v. 35, n. 3, p. 20-29, 1995.

Hunker, Jeffrey. US international policy for cybersecurity: five issues that won't go away. *Journal of National Security Law & Policy*, v. 4, n. 1, p. 197-216, 2010.

Índia. *National cyber security policy*: for secure computing environment and adequate trust & confidence in electronic transactions. Government of India, Department of Information Technology. Discussion Draft, 2011.

Mandarino Júnior, Raphael; Canongia, Claudia (Orgs.). *Livro verde*: segurança cibernética no Brasil. Brasília: Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações (GSIPR/SE/DSIC), 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 10 de novembro de 2013.

_____. Segurança cibernética: o desafio da nova Sociedade da Informação. *Revista Parcerias Estratégicas*, v. 14, n. 29, p. 21-46, 2009.

Milagre, José A. *Guerra e defesa cibernética*. Blog online. Disponível em: <http://josemilagre.com.br/blog/sala-de-estudos/cyberwar/pesquisas-2/guerra-e-defesa-cibernetica>. Acesso em: 23 fev. 2012.

Moresi, Eduardo A. D. *et al*. Defesa cibernética: um estudo sobre a proteção da infraestrutura e o software seguro. In: Conferencia Iberoamericana de Complejidad, Informática y Cibernética, 2., 2012, Orlando-FL. *Anais...* Orlando: 2012.

National Institute of Standards and Technology (Nist). *Framework for improving critical infrastructure cybersecurity*. Versão 1.0. 2014. Disponível em: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>. Acesso em: 10 mar. 2015.

Network Security. US lab develops federated model for defence against cyber attack. *Network Security – News*, v. 2009, n. 9, p. 2, 2009.

Pinheiro, Patrícia P. Leis digitais e suas vulnerabilidades. In: Seminário de Segurança Cibernética, 1., 2009, Brasília. *Anais...* Brasília: Estado-Maior do Exército, 2009.

Reino Unido. *The UK cyber security strategy*: protecting and promoting the UK in a digital world. 2011. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>. Acesso em: 15 mai. 2012.

República da África do Sul (RAS). *National cybersecurity policy framework for South Africa*. Department of Communications –Draft. 2011. Trabalho não publicado.

Ribeiro, Sérgio L. Estratégia de proteção da infraestrutura crítica de informação e defesa cibernética nacional. In: Barros, Otávio S. R.; Gomes, Ulisses M.; Freitas, Whitney L. (Orgs.). *Desafios estratégicos para a segurança e defesa cibernética*. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 145-163.

Alcyon Ferreira de Souza Junior

Mestre em Gestão do Conhecimento e da Tecnologia da Informação com ênfase em Segurança Cibernética pela Universidade Católica de Brasília (UCB). Doutorando em Engenharia Elétrica com ênfase em Segurança da Informação e Comunicações na Universidade de Brasília (UnB). Atualmente é Chief Information Security Officer no SEBRAE Nacional e professor na Universidade de Brasília (UnB) e IESB. Contato: alcyon@portaltic.com

Rosalvo Ermes Streit

Doutor em Administração pela UFRGS, na área de Sistemas de Informação e de Apoio à Decisão. Atualmente é docente-pesquisador do Mestrado em Gestão do Conhecimento e Tecnologia da Informação da Universidade Católica de Brasília (UCB), e analista do Banco Central do Brasil. Contato: rosalvo.streit@gmail.com