PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Secretaria Executiva
Departamento de Segurança da Informação e Comunicações

LIVRO VERDE
SEGURANÇA CIBERNÉTICA NO BRASIL

Raphael Mandarino Junior e Claudia Canongia
(Organizadores)

Brasília - DF
2010

Presidente da República
Luis Inácio Lula da Silva

Vice-Presidente da República
José Alencar Gomes da Silva

Ministro Chefe do Gabinete de Segurança Institucional
Jorge Armando Felix

Secretário Executivo
Antônio Sérgio Geromel

Diretor do Departamento de Segurança da Informação e Comunicações
Raphael Mandarino Junior

Representantes do Grupo Técnico de Segurança Cibernética - GT SEG CIBER GSIPR-DSIC e ABIN
Raphael Mandarino Junior (Titular e Coordenador; DSIC/GSIPR)
Marlos Ribas Lima (Suplente; ABIN/GSIPR)
Drª Claudia Canongia (Convidada; DSIC/GSIPR)

Ministério das Relações Exteriores
Ministra Virgínia Toniatti (Titular)
Ricardo Poletto (Suplente)

Ministério da Justiça
Jorilson da Silva Rodrigues (Titular; Ministério da Justiça)
Carlos Eduardo Miguel Sobral (Suplente; Departamento da Polícia Federal)

Ministério da Defesa
Capitão de Fragata Alexandre Mariano Feitosa (Titular)
Capitão de Fragata Cássio Alexandre Ramos (Suplente)

Comando do Exército
Tenente Coronel José Ricardo Souza Camelo (Titular)
Coronel Said Brandão Sayd (Suplente)

Comando da Marinha
Capitão de Fragata Valter Monteiro Junior (Titular)
Capitão de Fragata Ricardo Brigatto Salvatore (Suplente)

Comando da Aeronáutica
Coronel Adrian Nicolaiev Pereira dos Santos (Titular)
Major Cláudio Ramos Cruz (Suplente)

Disponível em formato eletrônico: http://dsic.planalto.gov.br

Organizadores
Raphael Mandarino Junior
Claudia Canongia

Colaboradores
Grupo Técnico de Segurança Cibernética – GT SEG CIBER

Projeto gráfico, edição e impressão
Agência Brasileira de Inteligência/GSIPR

Apoio de revisão técnica
Marlene Isidro (DSIC/GSIPR)
Admilson Gonçalves Júnior (DSIC/GSIPR)

Ficha Catalográfica
Dados Internacionais de Catalogação na Publicação (CIP)

B823l

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações.
Livro verde : segurança cibernética no Brasil / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.
63 p.

1. Segurança Cibernética – Brasil. 2. Segurança da Informação e Comunicações. 3. Segurança das Infraestruturas Críticas da Informação. I. Título. II. Canongia, Claudia. III. Mandarino Junior, Raphael.

CDD 658.4038
CDU 004.056.57

Ficha Catalográfica produzida pela Biblioteca da Presidência da República.

Gabinete de Segurança Institucional (GSI/PR)
Secretaria Executiva (SE)
Departamento de Segurança da Informação e Comunicações (DSIC)
Praça dos Três Poderes
Anexo III do Palácio do Planalto. Térreo, Ala A – Sala 107
70150-900 - Brasília, DF
Fax: +55 (61) 3411-1217
Site: http://dsic.planalto.gov.br

APRESENTAÇÃO

É com grande satisfação que apresento este Livro Verde, o qual reúne propostas de diretrizes básicas, visando iniciar amplo debate social, econômico, político e técnico-científico sobre a Segurança Cibernética no Brasil, contemplando relevantes aspectos destacados, dada a complexidade do tema no cenário atual.

Dentre as motivações do Gabinete de Segurança Institucional, órgão essencial da Presidência da República, para esta obra, tem-se a própria prerrogativa do Gabinete de coordenar a atividade de Segurança da Informação, mantendo o compromisso com o Estado. Assim, motivado por esta missão e considerando a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação e comunicações como fundamentais para a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação; a possibilidade real e crescente de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído Grupo Técnico para estudo e análise de matérias relacionadas à Segurança Cibernética.

Este Livro Verde, além de assistir a missão do GSIPR, reúne visões técnico-estratégicas desenvolvidas por especialistas de diferentes órgãos da Administração Pública

Federal, direta e indireta. Tal diversidade enriqueceu e propiciou diversas e significativas opiniões, as quais, sem sombra de dúvida, fomentarão discussões e propostas de melhorias sobre o assunto.

Recomendo, portanto, a leitura desta obra, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Nacional, e convido-os a contribuir com propostas e sugestões para a evolução da mesma, visando formular, colaborativamente, a Política Nacional de Segurança Cibernética.

Boa leitura! Participe!

Jorge Armando Felix

Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República

LISTA DE SIGLAS E ABREVIATURAS

ABIN	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CAIS	Centro de Atendimento a Incidentes de Segurança
CDN	Conselho de Defesa Nacional
CERT	*Computer Emergency Response Teams*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIR Gov	Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal
CGI	Comitê Gestor da Internet
CGSI	Comitê Gestor de Segurança da Informação e Comunicações
CICTE	Comitê Interamericano contra o Terrorismo Cibernético
CITEL	Comissão Interamericana de Telecomunicações
COMAER	Comando da Aeronáutica
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
CSIRT	*Computer Security Incident Response Teams*
D.O.U.	Diário Oficial da União
DPF	Departamento da Polícia Federal
DSIC	Departamento de Segurança da Informação e Comunicações
EB	Exército Brasileiro
END	Estratégia Nacional de Defesa
e-PING	Padrões de Interoperabilidade de Governo Eletrônico
FCC	*Federal Communications Commission*
FNDCT	Fundo Nacional de Desenvolvimento Científico e Tecnológico
GGE	*Group of Governmental Experts*
GSIPR	Gabinete de Segurança Institucional da Presidência da República

GT	Grupo de Técnico
GT SEG CIBER	Grupo Técnico de Segurança Cibernética
IBGE	Instituto Brasileiro de Geografia Estatística
ICCP	*Comittee for Information, Computer and Communications*
IEC	*International Engineering Consortium*
ITU	*International Telecommunication Union*
LDO	Lei de Diretrizes Orçamentária
MB	Marinha do Brasil
MD	Ministério da Defesa
MJ	Ministério da Justiça
MRE	Ministério das Relações Exteriores
OCDE	Organização para Cooperação e Desenvolvimento Econômico
OEA	Organização dos Estados Americanos
ONG	Organizações Não Governamentais
ONU	Organização das Nações Unidas
PDE	Plano de Desenvolvimento de Educação
PNSIEC	Plano Nacional de Segurança das Infraestruturas Críticas
PPP	Parcerias Público-Privadas
REMJA	Reunião de Ministros da Justiça ou Procuradores Gerais das Américas
RNP	Rede Nacional de Ensino e Pesquisa
TIC	Tecnologia da Informação e Comunicações
WPISP	*Working Party on Information Security and Privacy*

LIVRO VERDE
SEGURANÇA CIBERNÉTICA NO BRASIL

SUMÁRIO

PREFÁCIO

O Grupo Técnico de Segurança Cibernética (GT SEG CIBER), instituído no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, tem como objetivo propor diretrizes e estratégias de Segurança Cibernética, e conta com 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).

Em nosso entendimento, a efetiva colaboração de todos do GT para a elaboração deste Livro Verde: Segurança Cibernética no Brasil, neste ano de 2010, caracteriza o desejo e preocupação de seus participantes, de que iniciativas que favoreçam maior engajamento e sincronicidade em torno da segurança cibernética sejam incrementadas e concretizadas brevemente no país, propiciando, assim, a construção da doutrina e da política nacional, e os subsídios iniciais para o planejamento estratégico e construção de visão de futuro.

Sabemos que ainda há muito a ser alcançado, pois estamos dando os primeiros passos, para criar as condições necessárias de segurança cibernética, principalmente, no que diz respeito ao entendimento das novas exigências para a proteção da sociedade e do Estado Brasileiro. Esta é uma realidade que deve estar presente nas agendas do governo, da academia, do setor privado, e do terceiro setor, não somente como um desafio do país, mas como um desafio de magnitude mundial. Salientamos que o país, apesar de estar construindo as bases de sua Política no tema, já vem sendo reconhecido internacionalmente como um dos protagonistas.

Ressaltamos que criar, cultivar e ampliar a cultura de segurança cibernética no Brasil, é um desafio de longo prazo e de grande alcance, que merece um olhar especial, priorização,

e principalmente o esforço de amplo trabalho participativo na construção de senso comum e das premissas e diretrizes para o Livro Branco: Política Nacional de Segurança Cibernética.

Estamos certos de continuar contando com o apoio e a contribuição dos especialistas no tema, tanto de órgãos governamentais federais, quanto das demais esferas de governo, do setor privado, da academia, e do terceiro setor, na consulta ora aberta[1], para análises e contribuições sobre os pontos apresentados, e as diretrizes apontadas neste Livro Verde: Segurança Cibernética no Brasil, o qual serve de base para a elaboração do almejado Livro Branco.

Registramos, por fim, os nossos profundos agradecimentos a todos do GT SEG CIBER, do DSIC, da ABIN, e do GSIPR, que apoiaram fortemente esta iniciativa, com especial ressalva ao apoio e confiança do Sr. Ministro Chefe do GSIPR, Jorge Armando Felix.

Raphael Mandarino Junior,
Diretor do DSIC/ GSIPR, e Coordenador do GT SEG CIBER, e

Claudia Canongia,
Assessora Técnica do DSIC/ GSIPR, e pesquisadora convidada do GSIPR no GT SEG CIBER.

[1] Portal DSIC – http://dsic.planalto.gov.br

LIVRO VERDE
SEGURANÇA CIBERNÉTICA NO BRASIL

INTRODUÇÃO

Todos os dias, milhões de brasileiros acessam a Internet, trocam informações e usam serviços tais como bancários, de comércio eletrônico, serviços públicos federais, estaduais e municipais, de ensino e pesquisa, das redes sociais, dentre outros, constituindo uma ampla rede de atividades digitais.

A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras.

Diante de tais desafios, as Nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os 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 para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de idéias, de iniciativas, de dados e informações, de melhores práticas, para a cooperação no tema, no país e entre países.

Entender, portanto, tais movimentos e as respectivas oportunidades e desafios são questões estratégicas que o Estado Brasileiro vem se aprimorando e se organizando para melhorar seu posicionamento tanto no nível nacional quanto, consequentemente, no que se refere à sua inserção internacional, no tema.

Chama a atenção que o chamado espaço cibernético, não tem suas fronteiras ainda claramente definidas, impacta o dia a dia de todos os dirigentes governamentais, de empreendimentos privados e dos próprios cidadãos.

Na nova conformação da Sociedade da Informação, vale destacar os seguintes fenômenos:

a) Elevada convergência tecnológica;
b) Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;
c) Aumento crescente e bastante substantivo de acesso à Internet e das redes sociais;
d) Avanços das tecnologias de informação e comunicação (TICs);
e) Aumento das ameaças e das vulnerabilidades de segurança cibernética; e,
f) Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças.

Neste contexto, as estratégias internacionais no tema apontam para o estabelecimento de parcerias e ações colaborativas efetivas entre países, que propicie a análise, a coordenação, e a integração dos conhecimentos, permitindo, além da correlação entre tais conhecimentos, o entendimento dos impactos que a convergência e a interdependência existentes, e ainda por vir, têm e terão no futuro. Há uma tendência de que tais esforços devam ser suportados por macro-coordenação e governança bem estabelecidas, bem como baseados em modelos efetivos e eficazes de colaboração entre governo, setor privado e academia.

Ressalta-se a transversalidade[2] e particularidade da segurança cibernética, bem como a tendência mundial de destacar as diretrizes estratégicas, os planos e as ações neste tema, além do interesse do Brasil em protagonizar tal tema nos diferentes fóruns internacionais, sendo reconhecidamente um dos *players* na arena internacional.

Os desafios da segurança cibernética são muitos, e portanto, é fundamental desenvolver um conjunto de ações colaborativas entre governo, setor privado, academia, terceiro setor, e sociedade, para lidar com o mosaico de aspectos que perpassam a segurança cibernética.

[2] s. f.: 1. Qualidade do que é transversal; 2. Direção transversal. 3. Jur. Qualidade de ser colateral.

As ameaças naturais (por força da natureza) ou intencionais (sabotagens, crimes, terrorismo e guerra) ganham uma conotação e dimensão muito maior quando se trata do uso do espaço cibernético.

A construção de ambiente no País que permita sistematizar a identificação, a monitoração, a minimização e a mitigação de riscos cibernéticos, impulsionando o desenvolvimento de ações preventivas, pró-ativas, reativas, e de repressão, a todo o tipo de ameaças, prescinde de Política de Estado, visando assegurar e defender os interesses do país e da sociedade brasileira.

O desafio é, portanto, de todos, é premente, e requer agilidade na formação de senso comum a fim de que o país cresça, em segurança, se apropriando dos benefícios da Internet, rede global em mudança contínua, e minimizando impactos negativos decorrentes de desastres ou de uso malicioso da Rede.

Este Livro Verde: Segurança Cibernética no Brasil apresenta, assim, breve visão do país, sem qualquer pretensão de ser exaustivo, mas destacando alguns marcos recentes, oportunidades e desafios, nos vetores: Político-estratégico, Econômico, Social e Ambiental, CT&I[3], Educação, Legal, Cooperação internacional, e Segurança das Infraestruturas Críticas.

E, finalmente, sinaliza potenciais diretrizes estratégicas para cada vetor em análise, como subsídios ao amplo debate no âmbito do governo e da sociedade em geral, visando à construção da Política Nacional de Segurança Cibernética, a qual se constituirá no Livro Branco do País para enfrentamento de tal temática, reconhecidamente o grande desafio do século XXI.

[3] Ciência, Tecnologia e Inovação

LIVRO VERDE
SEGURANÇA CIBERNÉTICA NO BRASIL

I. OBJETIVO

O Livro Verde: Segurança Cibernética no Brasil visa expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, articulando visão de curto (2 - 3 anos), médio (5 – 7 anos), e longo (10 – 15 anos) prazo no tema, 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.

I.1. MOTIVAÇÃO E PERSPECTIVAS

Os avanços científicos e tecnológicos dos últimos 30 anos promoveram um aumento substantivo por produtos e serviços baseados em tecnologia, especialmente os relacionados com computação, telecomunicações, automação, robótica, bioinformática, mecatrônica, nanotecnologia, dentre outras.

Toda e qualquer reflexão sobre o porvir da Sociedade da Informação deve apoiar-se numa análise da mutação contemporânea da relação com o saber, em que a velocidade do surgimento e da renovação dos saberes e do *know-how* é avassaladora. Constata-se que a maioria das competências adquiridas no início do percurso profissional serão praticamente obsoletas ao final da carreira. Outro fenômeno refere-se à nova natureza do trabalho: trabalhar, atualmente, equivale cada vez mais a aprender, transmitir saberes e produzir conhecimentos. Soma-se, ainda, que o ciberespaço (ou espaço cibernético) suporta tecnologias que ampliam, exteriorizam e alteram muitas funções cognitivas humanas: a memória (bancos de dados, hipertextos, fichários digitais [numéricos] de todas as ordens), a imaginação (simulações), a percepção (sensores digitais,

telepresença, realidades virtuais), os raciocínios (inteligência artificial, modelização de fenômenos complexos).

Segundo Pierre Levy, o espaço cibernético é entendido numa visão de inteligência coletiva e mutante, totalmente baseado em redes e trocas de saber, conforme citação a seguir:

> *"Pierre Levy - A emergência do ciberespaço e as mutações culturais*
>
> *O que seria o espaço cibernético? O espaço cibernético é um terreno onde está funcionando a humanidade, hoje.(...) é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores. Atualmente, temos cada vez mais conservados, sob forma numérica e registrados na memória do computador, textos, imagens e músicas produzidos por computador. Então, a esfera da comunicação e da informação está se transformando numa esfera informatizada. (...) Com o espaço cibernético temos uma ferramenta de comunicação muito diferente da mídia clássica, porque é nesse espaço que todas as mensagens se tornam interativas, ganham uma plasticidade e têm uma possibilidade de metamorfose imediata. E aí, a partir do momento que se tem o acesso a isso, cada pessoa pode se tornar uma emissora, o que obviamente não é o caso de uma mídia como a imprensa ou a televisão. (...) Do interior do espaço cibernético encontramos uma variedade de ferramentas, de dispositivos, de tecnologias intelectuais. Por exemplo, um aspecto que se desenvolve cada vez mais, nesse momento, é a inteligência artificial. Há também os hipertextos, os multimídia interativos, simulações, mundos virtuais, dispositivos de tele-presença. (...) O importante é que a informação esteja sob a forma de rede e não tanto a mensagem, porque esta já existia numa enciclopédia ou dicionário".*
>
> *(http://www.sescsp.org.br/sesc/conferencias/subindex.cfm?Referencia=168&ID=35&ParamEnd=9)*

Em decorrência de tais avanços tecnológicos e da velocidade com que os mesmos vêm ocorrendo é possível verificar um movimento acentuado de re-arranjo das proposições das nações em termos de segurança e defesa. Tal está sendo propiciado quer seja por meio da revisão e/ou reforço de suas políticas, estratégias, e normas, quer seja pela atualização e/ou reformulação das competências essenciais de órgãos chave de governo, visando principalmente criar as condições necessárias de segurança e defesa do espaço cibernético, notadamente no que diz respeito ao entendimento das novas exigências para a proteção de uma nação.

A Segurança Cibernética, portanto, vem se caracterizando cada vez mais como uma função estratégica de Estado, e essencial à manutenção e preservação das infraestruturas críticas[4] de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, Informação, dentre outras.

Em relação aos conceitos tanto de Segurança Cibernética quanto de Defesa Cibernética, cabe colocar que estes vêm sendo construídos. Entende-se que o escopo de atuação da Segurança Cibernética compreende aspectos e atitudes tanto de prevenção quanto de repressão. E para a Defesa[5] Cibernética entende-se que a mesma compreende ações operacionais de combates ofensivos.

Para fins deste Livro tomou-se como base, então, a seguinte conceituação, como ponto de partida, sobre segurança cibernética, qual seja: *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 infra-estruturas críticas*[6]. É

[4] Por infraestruturas críticas (IEC) entendem-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade.

[5] De acordo com o Glossário das Forças Armadas (MD35-G-01;2007) o termo defesa é entendido como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança", ou ainda, como "reação contra qualquer ataque ou agressão real ou iminente".

[6] Conceito publicado na Portaria No. 45, Grupo Técnico de Segurança Cibernética, de 08 de setembro de 2009, publicada no D.O.U. No. 172 de 09

um conceito abrangente, portanto, e maior que segurança em TI, pois envolve pessoas e processos.

Fica em evidência que a proteção efetiva das infraestruturas críticas requer, comunicação em escala mundial, coordenação e cooperação entre todas as partes interessadas.

Soma-se o fato de que os países desenvolvidos vêm cada vez mais tratando do tema com bastante propriedade e seriedade, notadamente após o episódio de 11 de setembro de 2001, nos Estados Unidos. Cabe acrescentar que os resultados das ações já empreendidas fazem parte de ampla discussão em fóruns internacionais ocorridas sistematicamente, desde então.

I.1.1. Brasil – um dos protagonistas – iniciativas e fóruns internacionais

- ✓ Uma iniciativa que vale frisar é a adoção, pela OEA, desde 2004, de uma "Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética"[7], visando a criação de uma cultura de segurança cibernética para lutar contra as ameaças aos cidadãos, à economia e aos serviços essenciais, que não possam ser enfrentadas por um único governo ou combatidas por meio de uma disciplina ou prática solitária. No ano de 2009, o "Workshop Hemisférico Conjunto da OEA sobre o Desenvolvimento de uma Estrutura Nacional para Segurança Cibernética" foi realizado de 16 a

---

de setembro de 2009. Complementarmente acrescenta-se o conceito de ativos de informação que são os 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. (Portaria CDN/SE No. 34, Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, publicada no D.O.U No. 149 de 06/08/2009)

[7] CONSELHO PERMANENTE DA ORGANIZAÇÃO DOS ESTADOS AMERICANOS. COMISSÃO DE SEGURANÇA HEMISFÉRICA. Adoção de uma estratégia interamericana integral para combater as ameaças à segurança cibernética: uma abordagem multidimensional e multidisciplinar para a criação de uma cultura de segurança cibernética. (CP/CSH-635/04 rev. 2,13 de maio 2004)

20/Nov/2009, contando na organização, além do Governo brasileiro, anfitrião, por intermédio do GSIPR, da OEA representada pelos seguintes fóruns: Comitê Interamericano contra o Terrorismo Cibernético (CICTE), Comissão Interamericana de Telecomunicações (CITEL), e, Reunião de Ministros da Justiça ou Procuradores Gerais das Américas (REMJA), o que fortaleceu o papel do Brasil como um dos protagonistas no tema;

- ✓ A participação de representante do Brasil, do GSIPR, na categoria de observador *ad hoc* no "*Working Party on Information Security and Privacy - WPISP*", e do "*Comittee for Information, Computer and Communications - ICCP*", promovidos pela "Organização para Cooperação e Desenvolvimento Econômico - OCDE", realizados em Paris/França, em 2009 e 2010, também merece destaque. Por ocasião da reunião de 2010, o Brasil apresentou proposta de realização de "Estudo comparativo das estratégias nacionais de segurança cibernética"; a qual foi plenamente aceita e, para tanto, foi criado Grupo com presença de países voluntários para tal finalidade. O Grupo é presidido pelo representante de Portugal na OCDE, e conta com a participação dos seguintes países: Portugal, EUA, Coréia, Austrália, Japão, Espanha, e Brasil. O que realça a competência articuladora, de gestão, e técnica do país, no tema;
- ✓ Cabe citar, também, o evento "*Meridian Conference*", um encontro de alto nível, com a participação de especialistas e tomadores de decisão de governo, atuantes nas questões de segurança das infraestruturas críticas da informação e correlatas, que vem explorando os benefícios e oportunidades de cooperação entre

governos, e promovendo fórum de excelência para compartilhamento das melhores práticas mundiais, no tema. Neste contexto, vale citar que o Reino Unido introduziu o conceito de Meridiano e promoveu a 1ª Conferência em 2005, no ano seguinte ocorreu o Meridian 2006 em Budapeste, e posteriormente, o Meridian 2007 em Estocolmo, o Meridian 2008 em Singapura, e o Meridian 2009 nos EUA. Este último evento contou pela 1ª. vez com a participação de países latino-americanos, tendo sido convidados além do Brasil, a Argentina, Barbados, e Chile, sendo que o Brasil foi o único país latino americano com direito a voz, representado pelo GSIPR, nos debates e trocas de experiências;

- ✓ Acrescenta-se, ainda, que dentre as posições dos países que integram o "*Group of Governmental Experts*" (GGE) on "*Developments in the Field of Information and Telecommunications in the Context of International Security*" no âmbito da Organização das Nações Unidas (ONU), grupo em que o Ministério da Defesa (MD) representa o Brasil desde sua criação, e no qual nas reuniões ocorridas em 2010, contou com a participação do GSIPR, na qualidade de observador, foram debatidos, nos últimos anos, cerca de 35 itens, e chegou-se ao consenso de aproximadamente 18, sendo que dentre os itens considerados polêmicos e para futuras recomendações, tem-se o de não proliferação de armas de informação[8] e o de liberdade de expressão. O

[8] O Glossário das Forças Armadas (MD35-G-01; 2007) não define arma de informação, no entanto, define guerra de informação como "conjunto de ações destinadas a obter a superioridade das informações, afetando as

texto final do GGE, com recomendações de ações, especialmente no campo da cooperação internacional no tema segurança cibernética, será apresentado na próxima Assembléia Geral da ONU, em novembro de 2010. O país mais uma vez alcança reconhecimento e valorização no tema, em nível internacional;

- ✓ Finalmente, destaca-se a importância para o país de construir as bases para o entendimento internacional sobre a segurança cibernética, especialmente sobre crime cibernético, o quanto antes, e contando com a maior participação de órgãos possível. Já é entendido por vários países que, atualmente, a Convenção de Budapeste não atende as exigências atuais de crimes cibernéticos, dado os avanços tecnológicos ocorridos e tampouco é suficiente em termos da cooperação internacional. Assim, como resultado da Convenção do Crime Cibernético, ocorrida no ano de 2010, em Salvador/Brasil, foi emitida Declaração, consensada pelos 158 países sobre tal aspecto, o que abriu a oportunidade de criação de grupo para tratar globalmente a matéria - crime cibernético. Existe, portanto, proposta em andamento de uma nova Convenção, de caráter global, a qual teria como ponto de partida, a cooperação no âmbito dos BRICS (Brasil,

---

redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos". E guerra cibernética como "conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil".

Rússia, Índia, China e África do Sul). Destaques que o MRE, representante do Brasil neste fórum, aponta:

a) O Brasil terá um papel importante na negociação da nova Convenção;

b) Há que se desenvolver mecanismo pedagógico sobre o tema;

c) É essencial que o trabalho de negociação da nova Convenção e seus desdobramentos, bem como de apoio pedagógico, seja realizado rapidamente para dentro do país, e junto aos países vizinhos, bem como aos da África do Sul; e,

d) O grupo é presidido pelo Embaixador do Brasil que atua em Viena, e o ponto focal no país é o MRE, que mobilizará os debates no país, desenvolverá e levará o posicionamento do país ao citado grupo.

De acordo com o *ITU*[9], as áreas consideradas foco para promoção da segurança cibernética nos países membros da *OECD*[10], são:

- ✓ *Áreas de elevada atenção (prioritárias)*: Combate ao crime cibernético, criação em nível nacional de *CERTs/CSIRTs* (*Computer Emergency Response Teams/Computer Security Incident Response Teams*); aumento da cultura de segurança cibernética e suas atividades; e promoção da educação; e,

[9] *International Telecommunication Union.* Agência sediada em Genebra, Suiça, cuja missão é o crescimento e o desenvolvimento sustentado das telecomunicações e redes de informação, bem como facilitação de amplo acesso e fortalecimento da Sociedade da informação. A ITU conta com 192 Estados-membros, e mais de 700 setores membros e afiliados.

[10] *Organization for Economic Co-operation and Development*

- ✓ *Áreas que merecem maior reforço (relevantes)*: pesquisa e desenvolvimento; avaliação de risco e monitoramento; e atendimento às demandas de pequenas e médias empresas (PMEs).[11]

Urge formalizar, portanto, a estrutura da Segurança Cibernética no País, bem como apoiar e fortalecer suas atividades, de forma a viabilizar e agilizar tanto a formulação de políticas, normas e regulação, a pesquisa e o desenvolvimento de metodologias e tecnologias, quanto à cooperação internacional e a implantação e promoção de uma macro-coordenação que propicie a integração de processos, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de interesse do Estado brasileiro e da sociedade, bem como a resiliência de suas infraestruturas críticas.

Destaca-se que a iniciativa na direção efetiva da criação da "Política Nacional de Segurança Cibernética", cujo "Livro Verde de Segurança Cibernética do Brasil" serve de subsídio e deverá, na medida do possível, ser precedida de análises e consensos construídos com a participação de *stakeholders* para a viabilização e otimização do processo como um todo, criando uma Agenda de Estado político-estratégica e técnica.

Tal Agenda de Estado proporcionará conhecimentos sólidos e intercâmbio de experiências que poderão aprimorar o trabalho colaborativo para tal finalidade, cuja dificuldade reside na complexidade e dimensão do tema.

É neste contexto, que se faz mister construir visão de futuro e traçar metas e datas alvo, para o alcance do objetivo, qual seja, expressar potenciais diretrizes estratégicas, para o estabelecimento da Política Nacional de Segurança Cibernética.

[11] SUND, Christine. Promoting a Culture of Cybersecurity. In.: ITU Regional Cybersecurity Forum for Eastern and Southern Africa. Lusaka, Zambia. 25-28 August 2008.

I.2. COMPETÊNCIAS ESSENCIAIS

Inicialmente, vale acompanhar as recomendações da *OECD*[12] aos países membros, sobre segurança das infraestruturas críticas de informação, as quais são entendidas, em geral, como indicativos das competências essenciais de segurança cibernética, conforme apresentado a seguir:

- ✓ Definir a política e as normas específicas, com objetivos claros, no âmbito do mais alto nível de governo;
- ✓ Atuar como o órgão central de governo com competência (responsabilidade e autoridade) para prover as melhores condições de implantação da política de segurança cibernética e seus objetivos;
- ✓ Promover tanto a cultura de, quanto a educação em, segurança cibernética;
- ✓ Promover mútua cooperação entre os *stakeholders* – setor privado, agência(s), terceiro setor, governo – visando à efetiva implantação da política nacional de segurança cibernética;
- ✓ Atuar com transparência assegurando delegação de competência, ou seja, governança estabelecida, facilitando e fortalecendo a cooperação, em especial entre governo e setor privado;
- ✓ Rever sistematicamente a política, normas e respectivo(s) marco(s) legal(is), com especial atenção às ameaças e vulnerabilidades das infraestruturas críticas da informação de cada país, buscando minimizar riscos e desenvolver novos

[12]ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) - Guidelines for the Security of Information Systems and Networks: Towards a culture of security. (Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002). Paris: OECD. 2002. 28p. e, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATION POLICY (ICCP Committee) – OECD Recommendation of the Council on the Protection of Critical Information Infrastructure. (Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 April 2008). Seoul/Korea. June. 2008.

instrumentos e/ou mecanismos de segurança da informação e comunicações;

- ✓ Desenvolver e exercer macro-coordenação da política e estratégia nacional de segurança cibernética, envolvendo cúpula de governo e setor privado;
- ✓ Promover e exercer a macro-coordenação do monitoramento e da avaliação de risco, baseados na análise das vulnerabilidades e ameaças das infraestruturas críticas da informação, visando proteger a economia e a sociedade contra altos impactos;
- ✓ Promover e exercer a macro-coordenação do processo nacional de gestão de risco, orientando desde aspectos da organização, ferramenta(s), até mecanismos de monitoramento, para a implementação de uma estratégia nacional de gestão de risco que compreenda:
    a) Estrutura organizacional apropriada que promova melhores práticas de segurança, e que incluam prevenção, proteção, resposta e recuperação de ameaças naturais e maliciosas; e,
    b) Sistema de medidas que permita avaliar continuamente o processo, o que inclui itens de controle, níveis de maturidade, exercícios e testes apropriados;
- ✓ Promover e exercer a macro-coordenação da capacidade de resposta à incidentes em redes computacionais, como as das equipes que atuam em *CERTs/CSIRTs*, incluindo mecanismos de forte cooperação e comunicação entre tais equipes;
- ✓ Estreitar as relações com o setor privado:
    a) Estabelecendo parcerias público-privadas e acordos de cooperação, com foco na gestão de risco, tratamento de incidentes e recuperação de sistemas e redes de informação e comunicações, e na gestão da continuidade de negócios;

b) Estimulando o intercâmbio regular de informação, por meio do estabelecimento de acordos com cláusulas específicas para o caso de conhecimentos sensíveis ou informações classificadas;

- ✓ Estimular e apoiar a aceleração da inovação da segurança cibernética por meio da pesquisa e do desenvolvimento;
- ✓ Promover a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento das estratégias de segurança cibernética.

I.2.1. Comparação Internacional:

Economias desenvolvidas estão, exatamente neste momento, revisando ou lançando suas "Estratégias nacionais de segurança cibernética", como, por exemplo, EUA, Reino Unido, Japão, Espanha, Austrália, dentre outras, incluindo as questões de proteção das infraestruturas críticas da Nação, com uma sinalização forte do quanto há por fazer, principalmente em termos de cooperação internacional, legislação nacional e internacional, normalização, e capacitação de recursos humanos especializados. O que não quer dizer que o tema não faça parte das agendas anteriores de fóruns de governo, da iniciativa privada, das ONGs, nacionais e internacionais. As questões correlacionadas à segurança cibernética, em grande medida, tanto em termos de tecnologia quanto em termos de diretrizes, normalização, metodologias e capacitação, ao longo dos últimos anos, vinham sendo tratadas, mundialmente, no escopo da segurança da informação e comunicações, inclusive no Brasil.

I.2.2. Comparação Intertemporal:

O nível de preocupação da atualidade do que se refere ao espaço cibernético é marcante, em que pontos a serem

destacados sobre esta nova Sociedade da Informação, lá apresentados foram:

a) Convergência de tecnologias, aumento significativo de sistemas e redes de informação, aumento crescente de acesso à Internet, avanços das tecnologias de informação e comunicação;
b) Aumento das ameaças e das vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança;
c) Ambiente em constante, e rápidas mudanças; e,
d) Forças sócio-técnicas atuando em diferentes frentes - medidas de inclusão digital, acesso amplo e irrestrito à Rede, e, ambiente da Internet não regulado *vis a vis* medidas de proteção dos direitos de privacidade do cidadão, de proteção dos direitos de propriedade intelectual, de segurança das informações do Estado e da sociedade, de regulação e controle da Internet.

I.2.3. Tendências para 2020:

É importante apresentar o resultado divulgado do *Roadmap* que visualizou as forças motrizes que irão conformar o futuro da segurança da informação e segurança cibernética até 2020, estudo que foi encomendado pela Câmara de Estratégia de Tecnologia, e elaborado em conjunto com a *PricewaterhouseCoopers* LLP, do Reino Unido. As seguintes 7 (sete) tendências-chave foram levantadas:

1) Revolução da Infraestrutura: aumento na penetração da banda larga de alta velocidade e das redes sem fio; centralização de recursos de computação e ampla adoção da computação em nuvem; proliferação de IPs e de dispositivos conectados; crescimento de interfaces de usuário, com surgimento de novas tecnologias, potencialmente disruptivas;
2) Explosão de Dados: maior compartilhamento de dados confidenciais entre as organizações e

indivíduos; maior número de pessoas conectadas globalmente; multiplicação de dispositivos e aplicações geradoras de tráfego; maior necessidade de classificação da informação;

3) O mundo sempre conectado: maior conectividade entre as pessoas impulsionada por redes sociais e outras plataformas de conectividade de informação, e aumento de mineração de dados; aumento das infraestruturas críticas nacionais e da conectividade de serviços públicos;
4) Futuro das Finanças: aumento do uso do comércio eletrônico e de serviços bancários online; desenvolvimento de modelos novos de gestão, crescimento de novos modelos de pagamento;
5) Regulamentação e Normas mais severas: aumento da regulamentação relativa à privacidade; aumento das normas de Segurança da Informação e Segurança Cibernética; globalização e neutralidade das redes como forças contrárias à regulamentação e normalização;
6) Internets Múltiplas: censura; novas internets e mais seguras, redes sociais "fechadas"; e,
7) Nova identidade e modelo de confiança: identidade torna-se cada vez mais importante no movimento do perímetro de segurança da informação e segurança cibernética; novos modelos de confiança para desenvolver relações entre pessoas.

Assim, a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos e ao número de usuários, observados, especialmente, ao longo dos últimos anos.

Vale por fim acrescentar que dentre os diversos e crescentes movimentos e iniciativas mundiais em curso, no sentido de entender e construir visão sócio-técnica e de futuro sobre a segurança cibernética, encontra-se em fase final de consulta pública o documento intitulado "*The Cybersecurity*

Roadmap", estudo promovido pela Comissão Federal de Comunicações (FCC)[13], conforme reprodução a seguir da chamada localizada no sítio da mesma:

> *"The Cybersecurity Roadmap will establish a plan for the FCC to address vulnerabilities to core Internet protocols and technologies and threats to end-users, including consumers, business enterprises, including small businesses, public safety and all levels of government. Cybersecurity is a vital topic for the Commission because end-user lack of trust in online experiences will quell demand for broadband services, and unchecked vulnerabilities in the communications infrastructure could threaten life, safety and privacy . The NBP originally called for completion of the Cybersecurity Roadmap within 180 days (e.g., September 13, 2010). In order to ensure a complete and robust record in response to this Public Notice, we anticipate completion of the Cybersecurity Roadmap by November 2010."*
>
> *(http://www.cybertelecom.org/security/fcc.htm)*

[13] FCC é uma agência do governo americano, estabelecida pelo *Communications Act,* de 1934, sendo responsável pela regulação das comunicações via rádio, televisão, sem fio, satélite e cabo, interestadual e internacional.

II. VISÃO BRASIL: MARCOS RECENTES

Este Livro Verde: Segurança Cibernética no Brasil apresenta neste Capítulo, breve visão do país, sem qualquer pretensão de ser exaustivo, mas, apenas, colocando em destaque para reflexão, alguns marcos recentes no que se refere às oportunidades e aos desafios nos vetores: Político-estratégico, Econômico, Social e Ambiental, CT&I, Educação, Legal, Cooperação Internacional, e Segurança das Infraestruturas Críticas, tendo como foco central a segurança cibernética.

POLÍTICO-ESTRATÉGICO

OPORTUNIDADES

- ✓ Atores chave do governo federal com amplos conhecimentos no tema, bem como participantes de diversas redes de contatos e fóruns, no país e no exterior;
- ✓ Reconhecimento internacional do país como um dos protagonistas em vários temas globais, inclusive no tema segurança cibernética;
- ✓ Gabinete de Crise instituído desde 2003, acionado por demanda Presidencial, coordenado pelo GSIPR, e tendo atuado mais de 60 vezes até 2010, demonstrando capacidade de articulação entre as diversas esferas de poder, e pronta resposta em casos de extrema importância e defesa nacional;
- ✓ Criação da equipe de tratamento de incidentes em redes computacionais do governo, CTIR Gov em 2004, no GSIPR;
- ✓ Estratégia Nacional de Defesa - END (Decreto 6.703 publicado em 2008);
- ✓ Inclusão do tema segurança cibernética nos objetivos da Câmara de Relações Exteriores e Defesa Nacional – CREDEN, do Conselho de Governo (Decreto 7.009 publicado em 2009).

DESAFIOS

- ✓ Crescente complexidade nas relações e nos interesses dos Estados;
- ✓ Falta de clareza sobre a importância e real dimensão da problemática direta e indiretamente correlacionada à segurança cibernética, como tema de Estado, pela alta cúpula de governo, pensadores, e formadores de opinião;

- ✓ Múltiplos atores de governo envolvidos, por vezes com superposição de missões institucionais, e conseqüente deficiência no estabelecimento da governança;
- ✓ Carência de senso comum e de arcabouço conceitual da segurança cibernética, no país;
- ✓ Nível ainda baixo de fluxo e intercâmbio de informação entre as equipes de tratamento de incidentes em redes computacionais do governo e entre estas e as redes de inteligência de governo;
- ✓ Monitoramento do CTIR Gov aponta para cerca de 2 mil tentativas de invasão maliciosa, por hora, detectadas nas 320 grandes redes do governo;
- ✓ Extensão da capacidade da Defesa brasileira para abranger, além do espaço convencional, o espaço cibernético;
- ✓ Capacidades dissuasórias do país abrangendo o espaço cibernético.

ECONÔMICO

OPORTUNIDADES

- ✓ Expectativa da taxa anual de crescimento em 2010 da ordem de 7,2%;
- ✓ Brasil, Chile, Peru e Argentina vêm liderando o crescimento na utilização de recursos da tecnologia da informação na América Latina em 2010;
- ✓ Política nacional de Parcerias Público-Privadas (PPP) que favorecem projetos de infraestruturas;
- ✓ Potencial criação de emprego formal e renda no setor cibernético;
- ✓ Criação do Comitê Gestor da Internet (CGI) em 1995;
- ✓ Criação de equipes de tratamento de incidentes em redes computacionais no país em 1997, como o CERT.br no CGI para atender ao setor privado, e o CAIS na RNP para atender a área de pesquisa;
- ✓ De acordo com o Instituto Brasileiro de Geografia Estatística (IBGE), o Brasil possuía 67,9 milhões de usuários de Internet em 2009; e em 2008, 55,9 milhões. Assim, em 2009, os internautas representavam 41,7% da população e, no ano anterior, representavam 34,8%, o que demonstra curva significantemente crescente de acesso à Rede, no país;
- ✓ O Brasil transacionou US$ 8,7 milhões em vendas online em 2009, um aumento de 10,3% em relação a 2008. O Brasil ocupava o 1º lugar no ranking latino-americano em volume de

vendas eletrônicas. Em termos globais, o mercado é liderado pelos EUA, com movimento anual de US$ 134,9 milhões; seguido por Japão (US$ 51,2 milhões) e China (US$ 36,9 milhões), segundo dados da Convergência Digital, de junho de 2010;

- ✓ Sebrae patrocina circuito nacional de palestras, denominado MPE Net, com o objetivo de levar informações e conhecimentos sobre ferramentas tecnológicas e de comércio eletrônico para micro e pequenos empresários de diversas regiões do país.

DESAFIOS

- ✓ Cerca de 80% dos serviços de rede são de propriedade e operados pelo setor privado e por empresas internacionais;
- ✓ Ausência de orçamento específico para o desenvolvimento de ações e atividades de segurança cibernética em todas as esferas de governo;
- ✓ Ausência de carreira específica, de Estado, para atuação em segurança cibernética;
- ✓ Necessidade de atualização e ajustes da Política de Desenvolvimento Produtivo (PDP), com vistas e inserir o setor cibernético dentre suas prioridades;
- ✓ Indicadores do CERT.br destacam que, em 2009, os ataques cibernéticos mais freqüentes foram: a) contra o usuário final: fraudes, *phishing*, *bots*, *spyware*; b) do tipo força bruta contra serviços de rede: SSH, FTP; c) contra infraestrutura crítica da Internet: ataques DNS, d) contra protocolos de roteamento BGP; e, e) ataques a aplicações *Web* vulneráveis;
- ✓ Crescimento da nova classe média brasileira, segundo Censo 2010 do IBGE, alcançando cerca de 53% da população brasileira, apresentando novas demandas de consumo e de acesso.

SOCIAL e AMBIENTAL

OPORTUNIDADES

- ✓ Potencial e maior uso das tecnologias de informação e comunicações na redução de custos e melhorias de serviços públicos e privados à sociedade;
- ✓ Matriz energética limpa, caracterizada pela seguinte geração de energia elétrica, cujos dados de janeiro a setembro de 2010, são: hidroelétrica (79.789 MW); termoelétrica (29.735 KW); eólica (794 KW); e, importada (5.850 MW); sendo que para

tanto, conta com infraestrutura do sistema nacional, interligado 98 mil Km;

- ✓ Cidades digitais com projetos de ampliação da inclusão digital, por meio de telecentros e outras iniciativas;
- ✓ A audiência das redes sociais no Brasil cresceu 51% no último ano. Em agosto de 2010, mais de 36 milhões de usuários de Internet, com mais de 15 anos, visitaram uma rede social de casa ou do trabalho, segundo pesquisa divulgada pela empresa comScore.

DESAFIOS

- ✓ Ausência de conhecimento sobre as implicações sociais decorrentes do uso e aplicação de técnicas biométricas em controle de acesso, tais como digitais, íris, DNA;
- ✓ Projeção da evolução da matriz energética para 2020 aponta para um crescimento de cerca de 45,8% do uso de fontes renováveis, e 54,2% de uso de fonte não-renovável em relação aos dados do ano de 2007;
- ✓ Elevada complexidade para a segurança cibernética das infraestruturas críticas do país;
- ✓ Insuficiente monitoramento e proteção dos recursos naturais do país, uma vez que tendência mundial alerta tanto para a chamada "guerra pela água" quanto para a carência de alimentos, nos próximos anos;
- ✓ Uso crescente da Internet por organizações criminosas e pelo narcotráfico;
- ✓ É crescente a incidência de falhas e brechas de segurança nos portais das redes sociais mais usadas no país, *Orkut*, *Facebook*, *Twiter*, *YouTube*. A falha mais comum é a chamada de *Cross-site* Scripting (XSS), um tipo de brecha que permite ao atacante incluir um código no site.
- ✓ O IBGE prevê um crescimento populacional ao redor de 1,3% ao ano no final desta década, o que levará o país a registrar, em 2050, uma pirâmide etária com base estreita e topo mais alto, o que significa baixa taxa de fecundidade e elevada expectativa de vida;
- ✓ Integração do setor privado à segurança cibernética do país.

OPORTUNIDADES

- ✓ 336 instituições de C&T no país com 85 mil doutores em seus quadros, o caracteriza elevada capacidade de agregação de valor a produtos, processos e serviços;
- ✓ Fundo Nacional de Desenvolvimento Científico e Tecnológico (FNDCT) é atualmente 10 vezes superior ao que era em 2002, com cerca de R$ 3 bilhões de reais de orçamento em 2010, e sem contingenciamento ;
- ✓ Os investimentos em pesquisa e desenvolvimento, ao final de 2010, alcançarão 1,3% do PIB, o que é um avanço considerando anos anteriores;
- ✓ Universidades e Institutos de Pesquisa, ainda em número modesto, porém, com excelência acadêmica, desenvolvem atividades de monitoração de atividades maliciosas na Internet brasileira, dentre as quais: análise de riscos e testes de penetração; desenvolvimento seguro e análises de vulnerabilidades em aplicações críticas; e, aplicações *honeypots*;
- ✓ Universidades e Institutos de Pesquisa, ainda em número modesto, porém de excelência acadêmica, têm P&D em segurança da informação, em subáreas tais como computação forense, criptografia, biometria, dentre outras.

DESAFIOS

- ✓ Número, ainda, insuficiente de grupos de pesquisa e desenvolvimento de excelência acadêmica, com foco em ferramentas e soluções de segurança cibernética, bem como, de laboratórios de análises de artefatos maliciosos;
- ✓ Carência de programa, em nível nacional, que promova sistematicamente o desenvolvimento tecnológico e prospecção em temas como inteligência de sinais e de imagens, recursos criptográficos, segurança na computação em nuvem, desenvolvimento seguro de software, segurança cibernética, e segurança das infraestruturas críticas;
- ✓ Carência de conhecimento, mapeamento, e prospecção de tecnologias que apóiem a segurança cibernética do país, minimizando tanto suas vulnerabilidades quanto suas dependências tecnológicas externas e hiatos tecnológicos;
- ✓ Carência de linhas de fomento específicas ao desenvolvimento de tecnologias críticas essenciais, de rotas e soluções tecnológicas inovadoras, de desafios e/ou rupturas tecnológicas para a segurança cibernética do país, que contemplem uso dual;

- ✓ Inexistência de satélite geoestacionário nacional;
- ✓ Ações governamentais incipientes para estímulo ao setor privado demandar e financiar pesquisa, desenvolvimento e produção de soluções de segurança cibernética nas universidades ou outros centros de excelência;
- ✓ Inexistência de programa específico que contemplo ações, projetos e financiamentos governamentais que demandem diretamente soluções de segurança cibernética nas universidades ou outros centros de excelência, por meio de pesquisa, desenvolvimento e produção dessas soluções.

EDUCAÇÃO

OPORTUNIDADES

- ✓ Mudanças recentes na Constituição foram realizadas para dar sustentação ao Plano de Desenvolvimento de Educação (PDE) e reforça ações do Ministério da Educação e Cultura;
- ✓ Formação e atualização de professores para a educação básica tem sido foco da esfera federal, por exemplo, cita-se a criação da Universidade Aberta do Brasil, com mais de 500 pólos em atividade;
- ✓ Foram formados 10 mil e 12 mil doutores, respectivamente, em 2008 e 2009, e 37 mil e 40 mil mestres, respectivamente em 2008 e 2009, apontando para um crescimento na formação da pós-graduação do país;
- ✓ Recursos humanos de alto nível vêm sendo formados para atuação no tema ataque e defesa cibernética, em órgãos do governo;
- ✓ Há competências de recursos humanos formados no país em certificação digital, tratamento de incidentes em redes computacionais, criptografia, segurança de rede corporativa, dentre outras.

DESAFIOS

- ✓ Nível do ensino fundamental e médio do país, em escolas públicas e privadas, ainda é fraco. Por exemplo, resultado recente demonstra que permanência na escola, equidade, investimentos, desempenho, padrões educacionais, e carreira dos docentes, receberam notas entre regular e insatisfatório no 1º. Boletim da Educação no Brasil, organizado pela Fundação Lemann e pelo Programa de Promoção da Reforma Educativa na América Latina e no Caribe (Preal);

- ✓ Cerca de 80% dos mestres e doutores atuam na esfera pública e nas universidades, e apenas 20% encontram-se em atividades no setor privado;
- ✓ Carência de educação e formação de cultura de segurança cibernética em todos níveis, básico, fundamental, técnico, especialização, mestrado e doutorado;
- ✓ Incipiente formação de técnicos, especialistas, mestres e doutores, para a pesquisa básica e aplicada, bem como para a produção de protótipos de segurança cibernética;
- ✓ Os currículos de ensino de nível fundamental e médio do país não abordam, obrigatoriamente, temas como segurança da informação e correlatos, ainda que crianças e jovem façam uso intenso da Internet, em particular das redes sociais.

LEGAL

OPORTUNIDADES

- ✓ Competência federal de segurança da informação no Gabinete de Segurança Institucional da Presidência da República – GSIPR, desde 2003, Lei 10.683;
- ✓ O Código Penal do Brasil tem Artigos que atendem a determinados crimes com uso de computador;
- ✓ O Departamento de Polícia Federal tem cooperação policial internacional com INTERPOL, EUROPOL, AMERIPOL, dentre outras polícias, e atuam nos casos de crimes cibernéticos baseados no princípio da reciprocidade.

DESAFIOS

- ✓ Ausência de legislação nacional e internacional específica de segurança cibernética, em especial contra crimes cibernéticos;
- ✓ Ausência de regulação e mecanismos de certificação de segurança cibernética;
- ✓ Diversidade de termos e respectivas definições, a serem harmonizados, em nível nacional e internacional.

COOPERAÇÃO INTERNACIONAL

OPORTUNIDADES

- ✓ Tendência crescente, apesar de ainda incipiente, de multipolaridades, tendo a Rússia e o Brasil como exemplos de tais movimentos;

- ✓ Acordos bilaterais de cooperação em segurança da informação e comunicação, formalizados, por exemplo, com a Espanha, Rússia, França, e em negociação, por exemplo, com Itália, Israel, Luxemburgo, entre outros;
- ✓ Reconhecimento internacional do Brasil, como um dos protagonistas no tema segurança cibernética;
- ✓ Grupo de trabalho instituído em 2010, no âmbito da ONU, para elaborar proposta de uma nova Convenção, de caráter global, contra o crime cibernético, sob a coordenação do Embaixador do Brasil em Viena.

DESAFIOS

- ✓ Alta complexidade dado a extensão Continental do país;
- ✓ Tendência crescente nas relações interncaionais de bipolaridade entre EUA e China, inclusive na questão de "fronteira" no ciberespaço;
- ✓ Ausência de instrumentos internacionais específicos contra crimes cibernéticos para ação policial transfronteiras;
- ✓ Articulação, ainda incipiente, em termos de definição de ações transnacionais de segurança cibernética, com foco em crimes cibernéticos;
- ✓ A segurança cibernética de uma nação se estende além das suas fronteiras físicas, demandando ações conjuntas com outros Estados.

SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

OPORTUNIDADES

- ✓ No Brasil, a criação do Plano Nacional de Segurança das Infraestruturas Críticas (PNSIEC) prevê o estabelecimento de um processo integrado, por meio da criação de cultura de segurança e proteção, em todas as esferas de poder, de recursos humanos qualificados, equipamentos, instalações, conhecimentos, serviços, rotinas, dados, informações e processos estratégicos, e busca estender o esforço das iniciativas ao setor privado;
- ✓ Os Grupos Técnicos de Segurança das Infraestruturas Críticas de Energia, Transportes, Comunicações, Água, e Finanças, criados no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), bem como seus respectivos 11 subgrupos técnicos, envolvendo cerca de 100 especialistas, vêm se reunindo desde 2009, no sentido de apoiar o PNSIEC, e

consequentemente mitigar riscos e aumentar a resiliência das mesmas;

- ✓ O Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, criado no âmbito do Comitê Gestor de Segurança da Informação e Comunicações (CGSI), do Conselho de Defesa Nacional (CDN), vem desenvolvendo metodologias e instrumentos de apoio para, sistematicamente, assegurar, acompanhar, avaliar e melhorar a segurança das infraestruturas críticas da informação;
- ✓ Existência de equipes de resposta e tratamento de incidentes em rede computacionais, com capacitação de excelência e reconhecimento no país e no exterior, em que para atendimento as redes da Administração Pública Federal tem-se o CTIR Gov, para as redes privadas o CERT.br, e para as redes de pesquisa o CAIS da RNP.

DESAFIOS

- ✓ Falta de clareza e de identificação das interdependências nas infraestruturas críticas e entre infraestruturas críticas, e seus respectivos graus de criticidade e impactos;
- ✓ Ausência de integração das várias políticas setoriais, iniciativas e investimentos de segurança das infraestruturas críticas;
- ✓ Movimentos tardios de definição de prioridades estratégicas da Nação e harmonização das estratégias, com foco na prevenção;
- ✓ Limitado leque das infraestruturas críticas nacionais já priorizadas;
- ✓ Crescentes riscos de ataques cibernéticos a Sistemas SCADA[14];
- ✓ Insuficiente número de equipes de resposta e tratamento de incidentes em rede computacionais nos vários segmentos da sociedade, bem como insuficiente número de especialistas com competência para desempenhar tais atividades.

---

[14] É o conjunto de software e hardware que permitem o controle de sistemas industriais, como linhas de produção e processos de uma usina, e de infraestruturas, como energia, gás, água, tratamento de esgoto, entre outras.

III. DIRETRIZES A SEREM CONTEMPLADAS NA POLÍTICA NACIONAL DE SEGURANÇA CIBERNÉTICA

A Política Nacional de Segurança Cibernética deverá ter como uma de suas premissas, a sua construção a partir de visão multidisciplinar, interinstitucional, em que múltiplas competências se complementam na solução de problemas e na identificação de oportunidades.

Nesta direção, para que a "arte de assegurar a existência e a continuidade da Sociedade da Informação da nação brasileira, garantindo e protegendo, no Espaço Cibernético, os ativos de informação e as infraestruturas crítica do país", notadamente a de informação, seja eficaz e efetiva, e sem a pretensão de esgotar o assunto, indicam-se as seguintes diretrizes consideradas essenciais a serem desenvolvidas em prol da Política, para alcance da visão de futuro almejada, nos vetores destacados neste Livro:

POLÍTICO-ESTRATÉGICO

CARACTERIZAR a segurança cibernética como alta prioridade e de extrema urgência para o país, no curto prazo, implementando uma robusta estratégia nacional de segurança cibernética;

VALORIZAR E AMPLIAR as competências nos diversos temas que perpassam a temática da segurança cibernética, e temas correlatos, como o de segurança das infraestruturas críticas da informação, no curto e médio prazo;

LANÇAR, no curto prazo, a Política Nacional de Segurança Cibernética;

CRIAR órgão central para macro-coordenação da Política Nacional de Segurança Cibernética, no curto prazo;

ESTABELECER programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, no curto, médio e longo prazo;

DESENVOLVER arcabouço conceitual da segurança cibernética para o Estado brasileiro, no curto prazo;

ESTENDER a capacidade da Defesa do País para proteção da nação no espaço cibernético;

INCREMENTAR a capacidade dissuasória da Defesa do País para fazer frente a ameaça cibernética.

ECONÔMICO

DUPLICAR, a partir de 2011 e sistematicamente a cada 2 (dois) anos, portanto no curto, médio e longo prazo, os recursos financeiros alocados para a Segurança Cibernética, em Subfunção específica a ser criada para tal finalidade, na Lei de Diretrizes Orçamentária (LDO), desde 2011, com vistas a criar robusta capacidade de posicionamento e de resposta da Nação frente às potenciais ameaças cibernéticas;

ELABORAR E PROMOVER a devida regulação do mercado, no médio e longo prazo, por meio da adoção de padrões e especificações técnicas, bem como de modelos de gestão, de acompanhamento, e de auditoria da segurança cibernética;

ESTREITAR parcerias e ações colaborativas com o setor privado, estimulando as parcerias públicas privadas e as empresas estratégicas, promovendo o setor cibernético no país, no curto, médio e longo prazo;

APOIAR o segmento das micro, pequenas e médias empresas do país, em especial aquelas atuantes no comércio eletrônico, de forma a promover a cultura da segurança cibernética.

SOCIAL E AMBIENTAL

PROMOVER E UTILIZAR as redes sociais da Internet em prol da criação e fortalecimento da consciência nacional sobre segurança cibernética, no curto, médio e longo prazo;

DESENVOLVER programa de inclusão digital que incorpore consciência situacional sobre ameaças cibernéticas e segurança cibernética, no curto e médio prazo;

DEFENDER os direitos de privacidade do cidadão brasileiro, no curto, médio e longo prazo;

APOIAR o desenvolvimento da Internet no Brasil, promovendo política de acessibilidade com segurança do cidadão;

APLICAR políticas de incentivo para a integração do setor privado à segurança cibernética do país.

EDUCAÇÃO

DESENVOLVER programa nacional de capacitação em segurança cibernética e de recrutamento, que seja construído a partir da visão interdisciplinar que o tema requer, no curto, médio e longo prazo, nos níveis: básico, técnico, graduação, especialização, mestrado e doutorado;

DESENVOLVER programa de conscientização nacional no tema de forma a atingir, especialmente, no curto e médio prazo, diferentes comunidades do país, desenvolvendo material apropriado para os públicos: infantil; de adolescentes e jovens; de baixa renda; da terceira idade; de educadores em todos os níveis de formação educacional; e, de gestores e legisladores públicos, dentre outros segmentos a serem atendidos, no médio e longo prazo;

INCLUIR nos currículos de ensino de nível fundamental e médio do País a obrigatoriedade de temas como segurança da informação e correlatos.

MARCO LEGAL

COLABORAR estritamente para a atualização e por vezes para a construção do marco legal, nacional e internacional, contra ataques e crimes cibernéticos, no curto e médio prazo;

PROTAGONIZAR a articulação e a elaboração de Convenção global, sobre crime cibernético, no âmbito da ONU, no curto e médio prazo.

CT&I

ARTICULAR E PROMOVER o fortalecimento da ciência e pesquisa básica e aplicada, do desenvolvimento de tecnologias e metodologias, e da inovação em segurança cibernética, e em temas correlatos.

DESTACAR, dentre as prioridades de curto e médio prazo, as atividades de pesquisa aplicada, testes e ensaios em laboratório com tal finalidade, bem como a pesquisa, o desenvolvimento e a inovação (PD&I) no âmbito do setor cibernético (gestão de risco e de continuidade de negócio, recursos criptográficos, biometria, informação e análise de sinais e imagens, tratamento e resposta de incidentes em redes e sistemas computacionais, análises e monitoramento de tendências de *malware*, desenvolvimento de tecnologias cibernéticas, dentre outras);

AMPLIAR O ESFORÇO de padronização/harmonização do ambiente de segurança cibernética por meio de programa específico que: a) estenda a padronização/harmonização de especificações de bens e serviços, para o reforço de seu uso nas compras governamentais; b) crie modelos de

referência para apoio às atividades estratégicas de segurança cibernética; c) priorize o desenvolvimento e a compilação de padrões, de metodologias, de tecnologias de ponta; e, d) fomente/ estimule a utilização da arquitetura de interoperabilidade e do e-PING na integração de sistemas de informação do governo, bem como o maior intercâmbio de informações de incidentes computacionais entre as equipes especializadas de governo, setor privado e academia, para as devidas ações de prevenção e repressão contra ataques cibernéticos;

ESTIMULAR E ARTICULAR o aporte de recursos financeiros específicos, em programa a ser desenvolvido pelas Agências federais e estaduais de fomento em apoio à CT&I, para o setor cibernético;

ARTICULAR a aplicação de recursos do FUNTEL para o desenvolvimento continuado de CT&I do setor cibernético, especialmente no que tange à vertente da segurança;

FOMENTAR a demanda e financiamento, pelo setor privado, de pesquisa, desenvolvimento e produção de soluções de segurança cibernética nas universidades ou em outros centros de excelência;

FINANCIAR E ADQUIRIR, das universidades ou de outros centros de excelência, soluções de segurança cibernética por meio de pesquisa, desenvolvimento e produção dessas soluções para atender demandas do Estado.

COOPERAÇÃO INTERNACIONAL

PROMOVER a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento da estratégia nacional de segurança cibernética;

INSTITUCIONALIZAR no país a autoridade nacional de segurança, no curto prazo, com vistas a oficializar e sistematizar o processo de credenciamento de órgãos, entidades, empresas, e pessoas para intercâmbio de informações classificadas, entre governos;

PROMOVER E ARTICULAR acordos de cooperação técnica de segurança cibernética, no curto, médio e longo prazo;

PROMOVER visão alinhada e consensada entre os atores-chave atuantes na segurança cibernética, no curto, médio e longo prazo, visando a definição de posicionamento estratégico do país, no tema, em fóruns, comitês e colegiados internacionais;

ESTABELECER programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, no curto, médio e longo prazo;

ARTICULAR acordos internacionais de modo a potencializar a segurança cibernética do País, sua capacidade de defesa e dissuasão, além do aumento e atualização das suas competências essenciais.

SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

LANÇAR a Política Nacional de Segurança das Infraestruturas Críticas no curto prazo;

CONHECER E MAPEAR o grau de vulnerabilidade do país em relação aos seus sistemas de informação e as suas infraestruturas críticas de informação por meio de programa específico, no médio e longo prazo, que compreenda: a) a macro-coordenação do mapeamento dos ativos de informação das infraestruturas críticas; b) o apoio ao processo de auditoria de segurança das infraestruturas críticas da informação, definindo requisitos mínimos de segurança; e, c) a macro-coordenação e o desenvolvimento de sistema de monitoramento de ameaças cibernéticas e divulgação de alertas de suporte às infraestruturas críticas;

ELABORAR E/OU ADAPTAR metodologia, no médio e longo prazo, para avaliações de risco e de continuidade de negócio em segurança cibernética, o que inclui dentre outras ações: a) identificar o grau de interdependência dos serviços das infraestruturas críticas do país; b) desenvolver e/ou adaptar metodologia comum para avaliar as vulnerabilidades das infraestruturas críticas de informação, dos seus sistemas e de seus serviços; e, c) conceber um sistema dinâmico de medidas preventivas, próativas, e reativas contra ameaças e ataques cibernéticos;

DESENVOLVER PROGRAMA de capacitação de gestores atuantes nas infraestruturas críticas que contemple dentre outras competências: análise e gestão de riscos, segurança das infraestruturas críticas da informação, resiliência operacional e organizacional, monitoramento e resposta a ataques cibernéticos.

IV. CONSIDERAÇÕES FINAIS

A presente proposição do **Livro Verde Segurança Cibernética no Brasil** tem como principal objetivo, como se pode depreender tanto da argumentação quanto da lógica construtiva apresentada ao longo deste documento, a premente necessidade de construção de ambiente que propicie maior e melhor proteção do espaço cibernético do Estado brasileiro, e portanto, a formulação e lançamento da **Política Nacional de Segurança Cibernética**, o que, no país e no exterior, se traduz no lançamento do Livro Branco.

A tendência mundial caminha para a priorização da Segurança Cibernética e para o estabelecimento formal de órgão que centralize as competências básicas relacionadas ao tema, visando integrar esforços isolados e propiciar macro-coordenação no nível da Nação, a exemplo das experiências americana, inglesa, australiana, coreana, dentre outras.

A possibilidade de elaboração e lançamento da Política Nacional de Segurança Cibernética conformar-se-ia como a situação ideal, considerando o cenário atual vivido em termos das ameaças presentes e futuras no espaço cibernético, e as vulnerabilidades, seja no nível organizacional seja no doméstico.

Outrossim, há uma diversidade de atores que já vêm atuando no governo federal em prol da segurança cibernética, em que a título de exemplo cita-se o GSIPR (DSIC e ABIN), o MRE, o MJ (e o DPF), o MD, a MB, o EB, o COMAER, o que faz com que a proposição da Política fique ainda mais reforçada, uma vez que a mesma, viabilizará o exercício da macro-coordenação do tema, e propiciará a congruência dos esforços e iniciativas entre os diferentes atores da citada rede, apoiada no senso comum e suas derivações.

Soma-se o fato de que a Portaria No. 45, publicada no D.O.U. No. 172 de 09 de setembro de 2009, institui Grupo Técnico de Segurança Cibernética (GT SEG CIBER), no âmbito da Câmara de Relações Exteriores e Defesa (CREDEN), sob a Coordenação do Gabinete de Segurança Institucional da Presidência da República (GSIPR), e estabelece que tal Coordenação será exercida pelo Departamento de Segurança

da Informação e Comunicações (DSIC), que conta com a *expertise* necessária bem como rede de contatos no país e no exterior, no tema. Este GT SEG CIBER, composto por representantes, além do GSIPR, dos Ministérios da Justiça, da Defesa, das Relações Exteriores, e dos Comandos da Marinha; do Exército e da Aeronáutica; tem como objetivo propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal, uma missão considerada de relevante interesse público e do Estado. Há, também, a oportunidade de que sejam convidados especialistas, da academia e do setor privado, visando uma construção participativa no âmbito do citado GT. Este GT expressa o núcleo central de atores chave que vêm atuando no tema, e por ser um GT no âmbito da CREDEN, visa subsidiar esta Câmara em seu processo decisório, apontando diretrizes, ora elencadas neste Livro Verde.

Vale destacar também, dentre a sustentação legal necessária, que foi aprovado pelo Ministério de Orçamento, Planejamento e Gestão, no âmbito da Lei de Diretrizes Orçamentárias para o ano de 2010, a ampliação e o fortalecimento da finalidade e da descrição da "Ação 6232 – Capacitação de Recursos Humanos em Segurança da Informação e Comunicações", no âmbito do "Programa de Inteligência (0641)", a qual o GSIPR é a unidade administrativa responsável, conforme a seguir:

- ✓ FINALIDADE: Desenvolver ações de Segurança da Informação e Comunicações com vistas a fortalecer e implementar mecanismos capazes de prover a segurança do espaço cibernético brasileiro, em prol do bem estar da sociedade e da soberania do Estado.
- ✓ DESCRIÇÃO: Desenvolvimento de estratégias, normas e procedimentos; fortalecimento da proteção da infraestrutura crítica da informação; implementação e sistematização da gestão e da capacitação de recursos humanos; estímulo e fortalecimento da pesquisa, desenvolvimento e inovação; promoção e formalização de cooperação nacional e internacional; manutenção e reposição dos equipamentos, mobiliários e *softwares*, no âmbito

da Segurança da Informação e Comunicações e da Segurança Cibernética.

Não se pode deixar de registrar e colocar em evidência, como mais um importante e crucial passo na trilha da segurança e da defesa cibernética do país, o Decreto Nº 6.703/2008 que aprova a Estratégia Nacional de Defesa (END), a qual tem em sua dimensão o setor cibernético tratado no que se refere às tecnologias, capacitações, parcerias estratégicas e intercâmbios com nações amigas, neste último caso particularmente com as nações do entorno estratégico brasileiro e as da Comunidade de Países de Língua Portuguesa; bem como realça tal setor cibernético dentre os 3 (três) setores estratégicos a serem tratados no âmbito da citada Estratégia pelo Ministério da Defesa (MD) e Forças Armadas.

Finalmente, a segurança cibernética vem sendo tratada em nível estratégico pelas Nações e vários aspectos críticos correlatos ao tema, como "ciberguerra", ainda encontram-se em fase de discussão e longe de consenso.

Neste sentido, vale reproduzir a seguir o comentário final que consta do relatório FOI-R-2970-SE, de março de 2010, "*Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*", de Roland Heickero:

> *"As emergentes ameaças cibernéticas mostram o quanto é preciso incrementar tanto a segurança da informação quanto a cooperação internacional no sentido de evitar ou reduzir efeitos negativos de operações cibernéticas antagônicas. O tema ameaça cibernética deve ser resolvido em escala mundial, envolvendo o maior número de partes, de leis, e de agências de todas as Nações. Convenções têm de ser reescritas uma vez que a guerra cibernética confunde princípios como os da proporcionalidade, neutralidade e distinção. As regras cibernéticas necessitam ser melhor discutidas." (Heickero, R; 2010:55) - tradução do autor.*

GLOSSÁRIO

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2005).

Artefato malicioso: Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores (NC 05 DSIC/GSIPR, 2009).

Ativo de Informação: 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 (Portaria 45 SE-CDN, 2009).

Autenticidade: Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade (IN 01 GSIPR, 2008).

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado (IN 01 GSIPR, 2008).

Continuidade de Negócios: Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido (NC 06 DSIC/GSIPR, 2009).

Defesa: O ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança, ou ainda, reação contra qualquer ataque ou agressão real ou iminente. (Glossário MD35-G-01;2007).

Disponibilidade: Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade (IN 01 GSIPR, 2008).

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores (NC 05 DSIC/GSIPR, 2009).

Fonte de Risco: Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco (ISO 31000, 2009).

Gestão de riscos de segurança da informação e comunicações: Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (NC 04 DSIC/GSIPR, 2009).

Guerra de informação: Conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos. (Glossário MD35-G-01, 2007).

Guerra cibernética: Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil. (Glossário MD35-G-01, 2007).

Impacto: Mudança adversa no nível obtido dos objetivos do negócio (ABNT, 2008).

Infraestruturas Críticas: 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 (Portaria 45 GSI, 2009).

Infraestruturas Críticas da Informação: Subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (Portaria 34 SE-CDN, 2009).

Interdependência: Relação de dependência ou interferência de uma infraestrutura crítica em outra, ou de uma área prioritária de infraestruturas críticas em outra (Política Nacional de Segurança de Infraestruturas Críticas, 2010 – aprovada na CREDEN, e ainda não sancionada pelo Presidente da República).

Resiliência: Poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre. (NC 06 DSIC/GSIPR, 2009) Capacidade de resistir a fatores adversos e de recuperar-se rapidamente. (Política Nacional de Segurança de Infraestruturas Críticas, 2010 – aprovada na CREDEN, e ainda não sancionada pelo Presidente da República).

Risco: Efeito da incerteza nos objetivos (ABNT ISO GUIA 73, 2009).

Riscos de segurança da informação: Possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira, prejudicando a organização (ABNT, 2008).

Riscos de segurança da informação e comunicações: Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização. (NC 04 DSIC/GSIPR, 2009).

Segurança Cibernética: 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 infra-estruturas críticas (Portaria 45 SE-CDN, 2009).

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

Segurança da Informação e Comunicações: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (IN 01 GSIPR, 2008).

Vulnerabilidade: Propriedade intrínseca de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma conseqüência (ISO 31000, 2009). Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação (NC 04 DSIC/GSIPR, 2009).

BIBLIOGRAFIA CONSULTADA

ABNT. ABNT NBR ISO/IEC 27001:2006: Tecnologia da Informação : Técnicas de Segurança da Informação: Sistemas de Gestão de Segurança da Informação : Requisitos. Rio de Janeiro, 2006.

ABNT. ABNT NBR ISO/IEC 27002:2005: Tecnologia da Informação : Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ABNT. ABNT NBR ISO/EIC 27005:2008: Tecnologia da Informação : Técnicas de Segurança : Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008. BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instituiu Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC). Portaria nº 2, de 8 de fevereiro de 2008. Diário Oficial da União, nº 27, Pag. 1, 2008.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Portaria nº 34, de 5 de agosto de 2009. Diário Oficial da União, nº 149, Pag. 4, 2009.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Institui Grupo Técnico de Segurança Cibernética, no âmbito da Câmara de Relações Exteriores e Defesa Nacional. Portaria nº 45, de 8 de setembro de 2009. Diário Oficial da União, nº 172, Pag. 2, 2009.

BRASIL. Lei Nº 10.683, de 28 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Disponível em: www.planalto.gov.br. Acesso em out. 2010.

BRASIL. Ministério das Minas e Energia - MME. Secretaria de Planejamento e Desenvolvimento Energético. Matriz Energética

Nacional 2030. (colaboração da Empresa de Pesquisa Energética - EPE). Brasília: MME:EPE. Novembro, 2007. 254 p.

CABINET OFFICE. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. (UK Office of Cyber Security (OCS) and UK Cyber Security Operations Centre (CSOC)). UK: TSO – The Parliament Bookshop. June. 2009. 25p.

CANONGIA, C. Anotações técnicas da autora durante o evento X Encontro Nacional de Estudos estratégicos: Rumo a 2022 – Estratégias para a Segurança e o Desenvolvimento do Brasil. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República. Setembro, 2010.

CANONGIA, C. Relatório Técnico de participação no evento Workshop Hemisférico Conjunto da OEA sobre o Desenvolvimento de uma Estrutura Nacional para Segurança Cibernética. Rio de Janeiro: OEA: Comitê Interamericano contra o Terrorismo Cibernético (CICTE), Comissão Interamericana de telecomunicações (CITEL), Reunião de Ministros da Justiça ou Procuradores Gerais das Américas (REMJA); e DSIC/GSIPR. Novembro. 2009. 11p.

CANONGIA, C. Relatório Técnico de participação no evento I Seminário de Defesa Cibernética. Brasília: Ministério da Defesa e Exército Brasileiro. Junho. 2010. 8p.

CANONGIA, C. Relatório Técnico de participação no evento I Seminário de Infraestruturas Críticas (IEC). Brasília: Núcleo de IEC/Sec. Exec./GSIPR. Agosto. 2010. 8p.

CANONGIA, C e MANDARINO JUNIOR, R. Segurança Cibernética: o desafio da nova Sociedade da Informação. Revista Parcerias Estratégicas. Brasília:Centro de Gestão e Estudos Estratégicos (CGEE); v.14; n.29; dezembro/2009; pág 21 - 46.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Securing Cyberspace for the 44th. Presidency: a report of the

CSIS Commission on Cybersecurity for the 44th. Presidency. CSIS_Washington. December. 2008. 88p.

CREDEN. Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo: Resolução nº 2, de 24 de outubro de 2007. Brasília, 2007.

CREDEN. Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), Agosto. 2010. (ainda não sancionada pelo Presidente da República)

GLOSSÁRIO das Forças Armadas - MD35-G-01;2007.

INSTRUÇÃO NORMATIVA IN 01 GSIPR. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Gabinete de Segurança Institucional – Presidência da República, 2008. 5p. Brasília. 2008.

MANDARINO JUNIOR, R. Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro. (monografia aprovada no Curso de Especialização em Gestão da Segurança da Informação e Comunicações; orientador: Prof. Dr. Jorge Henrique Cabral Fernandes). Universidade de Brasília - UnB/ Departamento de Ciência da Computação - DCE:Brasília. Junho de 2009. pág. 29.

NORMA COMPLEMENTAR NC 04 DSIC/ GSIPR. Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Departamento de Segurança da Informação e Comunicações - Gabinete de Segurança Institucional – Presidência da República. 6 p. Brasília, 2009.

NORMA COMPLEMENTAR NC 05 DSIC/ GSIPR. Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Departamento de Segurança da Informação e Comunicações - Gabinete de Segurança Institucional – Presidência da República. 7 p. Brasília, 2009.

NORMA COMPLEMENTAR NC 06 DSIC/ GSIPR. Estabelece as Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Departamento de Segurança da Informação e Comunicações - Gabinete de Segurança Institucional - Presidência da República. 7p. Brasília, 2009

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) - Guidelines for the Security of Information Systems and Networks: Towards a culture of security. (Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002). Paris: OECD. 2002. 28p.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATION POLICY (ICCP Committee) – OECD Recommendation of the Council on the Protection of Critical Information Infrastructure. (Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 April 2008). Seoul/Korea. June. 2008.

PRESIDÊNCIA. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos: Decreto nº 3.505, de 13 de junho de 2000. Brasília, 2000.

PRESIDÊNCIA. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos: Decreto nº 4.553, de 27 de dezembro de 2002. Brasília, 2002.

PRESIDÊNCIA. Presidente da República: Decreto nº 6.371, de 12 de fevereiro de 2008. Brasília, 2008.

PRESIDÊNCIA. Presidência da República. Secretaria de Assuntos Estratégicos (SAE). Ciclo de Palestras: Educação (Ministro Fernando Haddad em 20/05/2010). Brasília: SAE/PR. 2010. 52 p.

PRESIDÊNCIA. Presidência da República. Secretaria de Assuntos Estratégicos (SAE). Ciclo de Palestras: Ciência e Tecnologia (Ministro Sergio Rezende em 15/04/2010). Brasília: SAE/PR. 2010. 36 p.

PRESIDÊNCIA. Presidência da República. Secretaria de Assuntos Estratégicos (SAE). Ciclo de Palestras: Planejamento (Ministro Paulo Bernardo em 27/05/2010). Brasília: SAE/PR. 2010. 36 p.

SUND, Christine. Promoting a Culture of Cybersecurity. In.: ITU Regional Cybersecurity Forum for Eastern and Southern Africa. Lusaka, Zambia. 25-28 August 2008.

STEVENS, J. F. Information Asset Profiling: CMU – Carnegie Mellon University, June 2005. 61 p. (CMU/SEI-2005-TN-021). Disponível em: <www.cert.org/archive/pdf/05tn021.pdf>. Acesso em: julho, 2010.

TECHNOLOGY STRATEGY BOARD - TSB, PRICEWATERHOUSECOOPERS LLP. Revolution or evolution? Information Security 2020. UK: TSB: Pricewathercoopers. 2010. 44p.

SÍTIOS CONSULTADOS NA INTERNET

Departamento de Segurança da Informação e Comunicações – dsic.planalto.gov.br

Estratégia Nacional de Defesa - END – https://www1.defesa.gov.br/eventos_temporarios/2009/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf

Federal Communications Commission - FCC: *Cybersecurity* - http://www.cybertelecom.org/security/fcc.htm

Government Information Security Articles - GovInfoSecurity.com E-news – www.govinfosecurity.com

Governo Eletrônico - http://www.governoeletronico.gov.br

Instituto Brasileiro de Geografia e Estatística – www.ibge.gov.br

International Telecommunications Union – ITU - www.itu.int

Ministério da Educação – www.mec.gov.br

Portal Convergência Digital – convergenciadigital.uol.com.br

Secretaria de Assuntos Estratégicos – Presidência da República: www.sae.gov.br

The White House Blog - www.whitehouse.gov/blog/2010/

Valor online – www.valoronline.com.br