O GESTOR DA SEGURANÇA DA INFORMAÇÃO NO ESPAÇO CIBERNÉTICO GOVERNAMENTAL: GRANDES DESAFIOS, NOVOS PERFIS E PROCEDIMENTOS

Eduardo Wallier Vianna
Universidade de Brasília (UnB), eduardowallier@hotmail.com

Jorge Henrique Cabral Fernandes
Universidade de Brasília (UnB), jhcf@unb.br

RESUMO

Este artigo analisa os procedimentos realizados pelos agentes responsáveis quanto à gestão da segurança da Informação no espaço cibernético da Administração Pública Federal brasileira (APF) e busca estabelecer os perfis que caracterizam os diferentes profissionais no trato dessa sensível atividade organizacional, e em muitos casos ligada a questões de Estado. O espaço cibernético digital é constituído por sistemas de informação automatizados e redes de comunicação de dados, para provimento de informações a usuários e clientes em distintas organizações e para a sociedade. As instituições que formam a APF possuem como características a atuação distribuída em todo o território nacional, bem como presença internacional, e contingente de servidores públicos civis e militares, dentro de um universo de 1,6 milhão de pessoas. Nessas instituições, os gestores de segurança são responsáveis pela execução de ações gerenciais, administrativas (planejamento, direção e controle), além de ações técnicas, visando garantir, entre outros aspectos, a disponibilidade, integridade, confidencialidade e autenticidade das informações que são utilizadas para o cumprimento da missão do Executivo Federal. A segurança cibernética, ou do espaço cibernético, encontra-se inserida no contexto mais amplo e multifacetado da segurança da informação, envolvendo não somente o uso de computadores. O artigo fundamenta-se, entre outros, na análise dos Levantamentos de Governança de TI realizados pelo Tribunal de Contas da União e nas informações coletadas durante a segurança cibernética de grandes eventos internacionais ocorridos no Brasil entre 2012 e 2014. O artigo descreve as vulnerabilidades mais comuns e as ameaças de ocorrência mais factível, no atual cenário cibernético nacional. O estudo estratifica os procedimentos de gestão da segurança cibernética em três níveis de atuação: operacional (atuação direta em sistemas computacionais, de controle ou rede de computadores), estratégico (coordenação e planejamento de gestão de alto nível para alcançar resultados de longo prazo) e tático (ações de tratamento de incidentes de segurança em redes de computadores).

Palavras-chave: Segurança da informação; espaço cibernético; segurança cibernética; administração pública federal; organização pública.

1 INTRODUÇÃO

O governo do Brasil, à semelhança dos que existem nas demais grandes e modernas nações, utiliza, em larga escala, as mais diversas soluções computacionais para implantação de sistemas informatizados, e vem disponibilizando aos cidadãos um crescente acervo de páginas, documentos digitais, dados, aplicações e serviços, que podem ser acessados a qualquer tempo e lugar, por diversos dispositivos, desde computadores até aparelhos móveis, como telefones celulares, interligados por meio da rede mundial de computadores.

De acordo com o investigado no Senado Federal (2014), o Brasil é o terceiro país do mundo em números de usuários ativos de Internet. Além disso, verificou-se um crescimento significativo do número de organizações governamentais brasileiras que disponibilizam serviços na internet, passando o percentual de 49%, em 2012, para 88%, em 2014 (Brasil 2014).

A Administração Pública Federal (APF) brasileira, também conhecida como Poder Executivo ou Federal, possui grande número de entidades, uma complexa hierarquia, diferenças na qualificação de pessoal, nas práticas e políticas já estabelecidas, bem como nos níveis de segurança implementados. As instituições (órgãos e entidades) governamentais que formam a APF possuem como características a atuação distribuída em todo o território nacional, e contingente de servidores públicos civis e militares, dentro de um universo de 1,6 milhão de pessoas. A fim de apoiar as mais diversificadas ações governamentais, na abordagem de "governo eletrônico" (e-gov), a APF vem adotando soluções multifacetadas, fortemente suportadas nas infraestruturas de Tecnologias de Informação e Comunicação (TICs), inseridas no contexto do espaço cibernético[1]. Segundo a ISO/IEC 27032 (ISO/IEC 2012, tradução nossa), espaço cibernético é entendido como "um ambiente complexo resultante da interação de pessoas, *software* e serviços existentes na Internet, conectados entre si por meio de dispositivos de tecnologia e redes, o qual não existe como forma física" (*Cyberspace - the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form*). Os autores concordam com a complexidade e elementos constituintes do

[1] O termo cibernético deriva do grego *kybernetike* e significa aquele que conduz, possui o leme, timoneiro, governador ou piloto. No campo científico, Wiener (1965), partindo de análises comportamentais, apresenta cibernética como o estudo da comunicação e controle das máquinas, seres vivos e grupos sociais. Os autores consideram que, do ponto de vista da transmissão da informação, não há distinção entre máquinas e seres humanos.

ciberespaço, embora discordem de sua suposta inexistência na forma física, pois o mesmo existe enquanto infraestrutura, bem como tem muitos de seus efeitos concretamente sentidos no mundo real, e não apenas informacional e cognitivo.

A título de exemplo, pode-se citar a Lei 12.527/2011 de Acesso à Informação (LAI) que entrou em vigor em maio de 2012. A LAI estabeleceu que o Estado Brasileiro deve oferecer acesso rápido e fácil às informações que estão sob sua guarda; e que essas informações devem ser apresentadas de forma clara, objetiva e de fácil entendimento, empregando, sempre que possível, as TICs. A implantação da LAI e suas consequências de uma maior transparência nas informações são sentidas de forma concreta na necessidade de investimentos em infraestrutura, pessoas e procedimentos, bem como em ações de combate à corrupção e na busca por melhores serviços públicos.

Esse artigo avalia os perfis de atuação dos agentes públicos que planejam e executam a segurança do funcionamento dos espaços cibernéticos. Foi baseado na análise dos “Levantamentos de Governança de TI”, realizados pelo Tribunal de Contas da União - TCU (Brasil 2010, 2012, 2014), no Projeto Censo da Web.br (NIC.br 2010). Foram também utilizadas evidências coletadas por um dos autores, por meio de observação direta participativa quando das atividades desenvolvidas pelo Centro de Defesa Cibernética (CDCiber) do Exército Brasileiro/Ministério da Defesa, durante a realização de grandes eventos internacionais ocorridos entre 2012 e 2014 no Brasil. Também foram analisados trabalhos realizados pelos autores nas áreas de segurança e defesa cibernéticas.

O artigo analisa uma minuta de procedimentos operacionalizados por agentes responsáveis pela gestão da segurança da Informação no espaço cibernético da APF. Esse espaço é constituído por sistemas de informação automatizados e redes de comunicação de dados, para provimento de informações a usuários e clientes de organizações da APF. Na APF, os gestores de segurança são responsáveis pela execução de ações gerenciais, administrativas (planejamento, direção e controle), além de ações técnicas, visando garantir, entre outros aspectos, a disponibilidade, integridade, confidencialidade e autenticidade das informações que são utilizadas para o cumprimento da missão do Executivo Federal.

Os procedimentos analisados foram estratificados em três níveis de atuação: 1) nível operacional, com atuação direta em sistemas computacionais, de controle ou rede de computadores; 2) nível estratégico, relativo à coordenação e planejamento de gestão de alto nível para alcançar resultados de longo prazo; e 3) nível tático, com ações de tratamento de incidentes de segurança em redes de computadores.

O restante do trabalho é composto por mais seis seções. A seção 2 faz uma breve análise das ameaças à segurança e defesa do espaço cibernético. A seção 3 descreve os principais procedimentos implementados na prática, para se contrapor às ameaças cibernéticas. A seção 4 analisa as vulnerabilidades gerenciais e técnicas presentes nas organizações do Brasil, especialmente em relação aos sítios *Web* governamentais e a situação de governança de Tecnologia da Informação na APF. A seção 5 caracteriza, na forma de um breve estudo de caso, como foram realizadas as ações de segurança e defesa, nos espaços cibernéticos afins aos quatro grandes eventos de significativa visibilidade internacional, realizados no Brasil entre 2012 e 2014, e nos quais um dos autores teve ativa participação. Ainda nessa seção, a título de comparação com a realidade brasileira, aborda-se como foi organizada a resposta à ameaça cibernética nos Jogos Olímpicos de 2012 em Londres, bem como, o Programa Nacional de Segurança Cibernética do Reino Unido, no que concerne à gestão e capacitação de recursos Humanos. A seção 6 apresenta a justificativa para o uso de três perfis profissionais ligados à segurança cibernética, bem como apresenta uma lista de procedimentos relevantes desempenhados pelos agentes públicos que nos atuam diferentes perfis. A seção 7 apresenta as conclusões do trabalho e sugere ações para aprimoramento da pesquisa.

2 AMEAÇAS[2] DO MUNDO DIGITAL (CIBERNÉTICO)

A APF coloca à disposição da sociedade brasileira um imenso acervo de conteúdos digitais públicos ou de utilização restrita, desde páginas de hipertextos, até arquivos no formato de imagens, textos, som, vídeos e códigos de programação. Esse acervo tem sido alvo de ações mal-intencionadas por diferentes grupos com os mais diversos e escusos objetivos.

A observação do cenário internacional revela que países como Brasil, EUA e Alemanha têm sido expostos a ações de vigilância e espionagem cibernética, comprometendo a soberania de Estados e nações, erodindo a privacidade de pessoas e de organizações. Tal situação foi amplamente evidenciada em 2013, com a revelação de que o governo dos Estados Unidos realiza espionagem de dados em escala global, bem como internamente ao país.

A situação mais conhecida é o "caso Snodew" (nome do delator do esquema de monitoramento - Edward Snowden), que revelou o *modus operandi* de um esquema de

[2] Considerando ameaça um conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para uma organização.

espionagem, onde, entre outros fatos, o governo americano obtém acesso aos correios eletrônicos (*emails*), fotos e ligações dos usuários de serviços de empresas como Google, Microsoft e Facebook. O caso também revela a existência de um programa de vigilância secreta que envolve setores de inteligência de “gigantes” da Internet. A mídia brasileira publicou diversas matérias sobre o monitoramento de chamadas telefônicas e *emails* brasileiros, inclusive levantando denúncias de espionagem sobre a Presidência da República e empresas brasileiras como a Petrobrás. Em âmbito nacional, as repercussões do “Caso Snowden” levaram o Senado Federal brasileiro a instaurar uma Comissão Parlamentar de Inquérito (CPI) da Espionagem (Senado Federal 2014).

No imaginário popular mais comum, o atacante de espaços cibernéticos é um jovem adolescente que pratica um ataque individual. Para o estudo de um ataque cibernético a um País ou nação, entretanto, tal conceito é insuficiente, e vem sendo ampliado, uma vez que Estados buscam impactos de longo prazo nos planos psicológico, econômico ou da segurança de sociedades ou nação com as quais competem. As ações de resposta a ataques, por sua vez, devido a implicações em nível de nação, devem ser coordenadas no âmbito do Estado, sob complexo gerenciamento e legislação específica.

Dessa forma, no contexto da gestão da segurança cibernética na APF brasileira, um atacante (oponente) cibernético deve ser entendido não como um indivíduo, mas sim como um grupo, suficientemente coordenado, especializado, inteligente e disciplinado, que dispõe de recursos financeiros e materiais expressivos, bem como tem disponibilidade de conhecimento e tempo. Naturalmente, a segurança contra a ação de *hackers* individuais deve ser sempre considerada, mas mantém-se importante analisar e prevenir a ameaça maior representada por adversários detentores de potencial ofensivo significativo e organizado (Revista Brasileira de Inteligência, 2007).

Cabe destacar que qualquer infraestrutura de TIC pode ser alvo de uma ação cibernética adversa. A Internet tornou-se importante veículo para atuação de grupos dos mais diversificados interesses, extremistas ou não, tendo em vista que as facilidades de ações à distância, com possibilidade de anonimato, propiciam um ambiente efetivo para alcance de objetivos. As ameaças mais factíveis de acontecer no atual cenário cibernético associado à Internet são:

a) uma ação cibernética hostil (também denominada de ataque cibernético) realizada por grupos antagônicos às infraestruturas críticas à sociedade em um

estado-nação[3], que pode ser empregada como multiplicador de efeitos, ao potencializar os danos causados por um ataque físico (causador de pânico imediato com imagens de fogo e destruição, por exemplo), mediante obstaculização ou desinformação;

b) divulgação de boatos, realização de sabotagem ou mesmo espionagem comercial e industrial cibernéticas, em relação às infraestruturas críticas da sociedade de um estado-nação ou mesmo em segmentos econômicos privados, por atos de grupos internacionais interessados em comprometer a imagem, o funcionamento ou o desenvolvimento de um estado-nação;

c) sabotagem ou protestos, durante a preparação e a realização de eventos de grande visibilidade internacional, promovidos por um país. As ações citadas seriam realizadas por grupos estrangeiros ou mesmo ativistas nacionais, com interesses em macular a imagem de um estado-nação no contexto internacional.

3 SEGURANÇA DA INFORMAÇÃO E A SEGURANÇA CIBERNÉTICA

3.1 Aspectos gerais

A princípio, poder-se-ia supor que segurança cibernética, também conhecida como segurança digital ou do espaço cibernético, seria uma evolução de segurança da informação. Para os autores deste trabalho, segurança cibernética encontra-se inserida no contexto mais amplo e multifacetado da segurança da informação, em consonância com o descrito pela Academia Latino-Americana da Segurança da Informação (2006)**:**

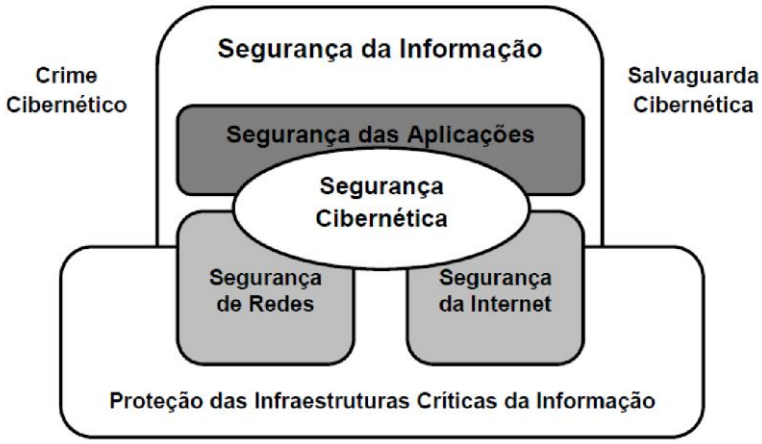
> a segurança da informação tem como propósito proteger as informações registradas, sem importar onde estejam situadas: impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem.

A norma ISO/IEC 27032- *Guidelines for cybersecurity (*Diretrizes para a segurança cibernética*)*, alinhada com o "espírito" de segurança da informação inerente à família das normas internacionais 27000, define segurança cibernética (*Cybersecutity* ou *Cyberspace secutity*) como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético**.** Adicionalmente, outras propriedades, tais como: autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas nesse contexto (ISO/IEC 27032 2012, tradução nossa).

[3] No Brasil, são consideradas Infraestruturas Críticas, “instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade” (Fernandes 2012).

A Figura 1, extraída da norma ISO/IEC 27032, exemplifica uma forma de inserção da segurança cibernética no campo da segurança da informação.

Figura 1: Relacionamento entre segurança cibernética e outras seguranças



Fonte: adaptado de ISO/IEC 27032 (2012, tradução nossa)

Interessante ressaltar que o chamado espaço cibernético (ou ciberespaço) não se encontra restrito ao uso da Internet ou dos computadores, como corrobora Klimburg (2012, tradução nossa): "o ciberespaço é mais do que a internet, incluindo não somente o *hardware*, *software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes" (*Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks*). De fato, o próprio conceito de cibernética está relacionado às ações de controle e comunicação da informação, não apenas feitas com o uso de computadores. Esse é um assunto abordado em Fernandes (2013), sobre o qual não entraremos em detalhes. Nesta discussão, o espaço cibernético está diretamente vinculado à dinâmica que ocorre dentro dos computadores.

Dessa forma, pode-se inferir que os ataques cibernéticos simples ou individuais, que causavam e ainda causam em geral males controláveis e prejuízos limitados, estão dando lugar a operações sofisticadas e bem financiadas, capazes de causar danos econômicos e de reputação significativos a vítimas dos setores público e privado, atingindo nações e grandes empresas mundiais. Nesse contexto, o cidadão, no seu cotidiano, toma consciência de parte dessas ações danosas em pelo menos três situações: (1) ao perceber o vazamento de seus dados privados que estavam sob custódia de um órgão público ou (2) ao descobrir que valores numéricos pessoais, armazenados em uma base de dados governamental, foram alterados sem a

aquiescência e conhecimento do responsável pela guarda das informações, ou, ainda, (3) quando não consegue acessar um serviço público porque o sítio (*site*) de governo eletrônico está fora do ar.

O exemplo anterior tipifica, respectivamente: (1) rupturas na confidencialidade, (2) comprometimento da integridade e (3) perda da disponibilidade da informação, sob a responsabilidade do e-gov. A despeito de algumas variações e discussões conceituais, essas são as três propriedades mais importantes relativas à segurança da informação, conhecidas pela sigla (tríade) CID ou CIA (*confidentiality, integrity and availability*). Ou seja, as atividades de segurança cibernética buscam a preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético considerado, bem como de outras propriedades como: autenticidade, responsabilidade, não repúdio e confiabilidade - *Cybersecurity: preservation of confidentiality, integrity and availability of information in the ciberspace. In addition, other properties. such as authenticity, accountability, non-repudiation, and reliability can also be involved* (ISO/IEC 27032, 2012, tradução nossa).

As propriedades da segurança da informação são, assim, definidas com base na ISO/IEC 27000 (2014):

a) confidencialidade (*confidentiality*) - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

b) integridade (*integrity*) - propriedade de exatidão e completeza;

c) disponibilidade (*availability*)- propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada;

d) autenticidade (*authenticity*) - propriedade de que uma entidade é o que ela diz ser;

e) responsabilidade (*accountability*) - propriedade na qual o responsável pela informação deve prestar contas da mesma;

f) não repúdio (*non-repudiation*) - capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias;

g) confiabilidade (*reliability*) - propriedade de que o comportamento e o resultado são consistentes com a intenção.

A gestão de segurança visa implementar ações que preservem essas propriedades por meio do controle e da comunicação da informação. Uma das atividades

mais relevantes nesse contexto é o tratamento de incidentes, aprofundado no próximo item.

3.2 Incidentes de segurança

Manter a segurança das informações de uma organização no ambiente computacional interconectado, nos dias atuais, é um grande desafio, que se torna mais difícil, à medida que são lançados novos produtos e serviços acessíveis pela rede mundial de computadores e novas ferramentas de ataque são desenvolvidas e difundidas rapidamente. Na visão do TCU (2012, 16):

> uma gestão inadequada da segurança da informação pode causar prejuízos significativos à instituição, e ainda, no caso de entes públicos, afetar ou interromper serviços necessários à sociedade e aos cidadãos. A indisponibilidade de um sistema de uma operadora de energia elétrica, resultando na interrupção do fornecimento de energia, ou o acesso indevido à conta bancária de um cliente de uma instituição financeira são exemplos comuns dos prejuízos que uma falha de segurança da informação pode ocasionar.

A NBR ISO/IEC - 27002 (ABNT 2013) afirma que a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios ou cumprimento da missão de uma organização e consequentemente necessita ser adequadamente protegida; descreve que segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao mesmo, maximizar o retorno sobre investimentos e as oportunidades de negócio.

Dessa forma, um ataque cibernético pode ocorrer sob diversas formas, sendo as mais relevantes:

a) instalação de um programa ilícito[4] como vírus, cavalos de troia ou spywares;

b) negação de serviço disponibilizado (*Denial-of-Service* (DoS));

c) introdução de funcionalidades não autorizadas nos sistemas operacionais (de forma que estes passem a reconhecer o acesso do atacante, privilegiando-o com permissões especiais, ao garantir que seu trânsito no sistema seja absolutamente livre, inclusive não rastreável pelas rotinas de auditoria);

[4] Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos; cavalos de troia: programa normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário; *spywares:* programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros (CERT.br, 2012).

d) inserção de vulnerabilidades em sistemas estratégicos, como os referentes a comandos não documentados que tornariam possível a terceiros (mais exatamente, a seus próprios programadores) desabilitar ou alterar a operacionalidade desse sistema crítico;

e) *hacking*: exploração das vulnerabilidades que inevitavelmente se manifestam em qualquer arcabouço de controles e sistemas integrados numa rede;

f) infiltração de pessoas (*insiders*) com objetivos diversos como: disponibilização de senhas que permitam o acesso externo de terceiros não autorizados e instalação prévia de programas hostis que produzam ou facilitem o ataque e modificações de *hardware* (Wallier Vianna 2011).

Em relação aos eventos que possam comprometer a segurança das informações, a Norma Complementar n. 05/IN01/DSIC/GSIPR (Brasil 2009), promovida pelo órgão responsável por normatizar a segurança da informação no estado brasileiro, define que um incidente de segurança "é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores". No trato com incidentes de segurança, devem ser observados os seguintes aspectos:

a) tentativas (com ou sem sucesso) de ganhar acesso não autorizado a um sistema cibernético ou a seus dados;

b) interrupção indesejada ou negação de serviço prestados pelo sistema;

c) uso não autorizado de um sistema para processamento ou armazenamento de dados;

d) furto de informação sigilosa em formato eletrônico digital;

e) extorsão via o uso de computadores;

f) modificações nas características de *hardware, firmware* ou *software* de um sistema, sem o conhecimento, instruções ou consentimento prévio do responsável pelo sistema;

g) obtenção, guarda e preservação de evidências;

h) detecção (monitoração de redes e sistemas para detecção da intrusão, ou da tentativa);

i) violação ou quebra da Política de Segurança da Informação (PSI) de forma explícita ou implícita.

A Política de Segurança da Informação é comumente conhecida no âmbito da APF como Política de Segurança da Informação e Comunicações - POSIC (Brasil 2008). Trata-se de documento que declara o comprometimento da alta administração de instituição pública federal e o seu apoio aos princípios e metas da segurança da informação, além de estabelecer as diretrizes referentes à segurança da informação. Deve ser formalmente instituída, como norma de cumprimento obrigatório pelos integrantes da organização e do conhecimento das partes externas relevantes.

4 ANÁLISE DE VULNERABILIDADES NA GESTÃO DA SEGURANÇA CIBERNÉTICA

A fim de coletar os dados sobre as vulnerabilidades inerentes ao espaço cibernético da APF, foram utilizados, como fonte principal, os levantamentos de governança de TI do Tribunal de contas da União realizados entre 2007 e 2014, complementados pelo Censo da *Web* governamental promovido pelo Comitê Gestor de Internet do Brasil em 2009.

4.1 O Projeto Censo da Web.br

O Projeto Censo da Web.br foi uma iniciativa do Comitê Gestor de Internet do Brasil – CGI.br, operacionalizada pelo Núcleo de Informação e Coordenação do Ponto BR – NIC.br (NIC.br, 2010). A pesquisa realizada intitulou-se "Dimensões e características da *Web*[5] brasileira: um estudo do '.gov.br' " e buscou realizar um raio-x da *Web* governamental, revelando características dos domínios, páginas *Web* e servidores *Web* da APF.

No Projeto, os domínios, também chamados de *Website*, sítio, ou sítio *Web*, identificam os conteúdos (páginas, documentos etc.) disponibilizados na Internet. A coleta de dados sobre os domínios do governo foi realizada em outubro de 2009 e identificou um total de 18.796 sítios sob o '.gov.br', a partir de URLs[6] percorridas.

De maneira geral, a pesquisa revelou baixo grau de maturidade na gestão da *Web* do governo brasileiro. Pela expressiva quantidade de páginas (6.331.256), percebe-se que o e-gov tornou-se também, sinônimo de modelo de competência e de governança estatal. Tal fato, de certa forma, pressiona os administradores públicos a acelerarem demasiadamente a acessibilidade dos serviços à população, em detrimento da complexidade da máquina pública e de especificidades técnicas de segurança.

---

[5] *World Wide Web* (rede de alcance mundial), também conhecida WWW.

[6] URL: do inglês Universal Resource Locator. Sequência de caracteres que indica a localização de um recurso na Internet como por exemplo, http://cartilha.cert.br/ (CERT.br, 2012).

Neste contexto, a grande quantidade de administradores de sítios espalhados geograficamente leva ao questionamento de que, em prol da rapidez na prestação ou disponibilização de algum serviço ou informações, as soluções (desenvolvimento das aplicações e programas voltados para a Internet) não são exaustivamente testadas e validadas, apresentando vulnerabilidades no seu desenvolvimento, na sua implementação ou não recebendo a devida manutenção/atualização periódica de segurança. A falta de aderência ao padrão W3C[7] (apenas 5% estão completamente de acordo com o padrão) sustenta o questionamento supracitado, bem como a substancial diferença de sincronização de tempo dos servidores da *Web* brasileira (apenas 52% dos servidores estão corretamente sincronizados) em relação à hora certa mundial, conhecida como UTC (*Universal Time Coordinated*)[8].

Também é agravante o fato de que o total de vulnerabilidades descobertas em aplicações *Web* tem sido muito maior do que o número daquelas descobertas em sistemas operacionais nos últimos anos (NIC.br, 2010).

4.2 O levantamento de governança de TI do TCU

Para avaliar a situação de governança de Tecnologia da Informação na Administração Pública Federal, o Tribunal de Contas da União (TCU) tem realizado levantamentos baseados em questionários que abordam práticas de governança e de gestão de TI previstas em leis, regulamentos, normas técnicas e modelos internacionais de boas práticas (Brasil 2014).

Dessa forma, o TCU iniciou, em 2007, seu primeiro levantamento de governança de TI. Tal iniciativa buscou avaliar a situação da governança de TI, a partir da coleta de informações em questionário disponibilizado a instituições representativas de diversos segmentos da APF. Diante do cenário preocupante, identificado em 2007, que contou com a participação de 255 instituições da APF, o TCU prosseguiu na realização de novos levantamentos dessa natureza a cada dois anos, com a finalidade de acompanhar a situação da governança de TI e manter uma base de dados atualizada (Brasil 2010).

O levantamento de 2010, que, ao todo, avaliou 301 instituições da APF, revelou que a situação da governança de TI na APF era bastante heterogênea. Em relação à segurança da informação, de uma forma geral, verificou-se que seus processos de gestão

[7] W3C: o Consórcio World Wide Web (W3C) é uma comunidade internacional que desenvolve padrões com o objetivo de garantir o crescimento da *Web*. Disponível em: <http://www.w3c.br/Home/WebHome >. Acesso em: 29 nov. 2014.

[8] O horário preciso em que ocorreram as ações maliciosas ou dos registros (*Logs*) é relevante e necessário para solução do incidente de segurança.

ainda eram pouco implantados (Brasil 2010). Analisando os resultados do estudo e comparando-os com o levantamento de 2007, merecem destaque as seguintes vulnerabilidades:

a) baixa preocupação da alta administração com o uso e a gestão da TI institucional, o que pode induzir à ineficiência e à falta de efetividade da instituição como um todo;

b) a área de segurança da informação continuou a chamar a atenção pelos altos índices de não conformidade, sugerindo que, de forma geral, as organizações públicas, além de não tratarem os riscos aos quais estão expostas, desconhecem tais problemas;

c) nenhum dos indicadores relativos à segurança da informação, que envolveram confidencialidade, integridade e disponibilidade da informação, apresentou avanço substancial;

d) a despeito das recomendações emitidas pelo TCU e das publicações normativas do Gabinete de Segurança Institucional da Presidência da República (GSIPR) sobre segurança da informação, a Administração Pública, de forma geral, continuou a desconhecer e a não proteger suas informações críticas adequadamente;

e) quanto aos *softwares* utilizados, a não adoção, nem mesmo informalmente, de qualquer processo ou método para desenvolvimento, aliado à ampla terceirização dos serviços de desenvolvimento na maioria das organizações, amplia o risco de inserção de código malicioso ou falhas intencionais;

f) dependência de terceiros (pessoal de TI externo à instituição), gerando demora na avaliação [e correção] de eventos de segurança. Tal fato poderia acarretar uma reduzida capacidade de gerir incidentes de segurança de média e grande complexidade.

No prosseguimento, o levantamento de governança de TI 2012 (Brasil 2012) questionou ao todo 349 organizações da APF, selecionadas a partir de critérios como a representatividade no orçamento da União e a estrutura de governança e gestão de TI. Os dados coletados revelaram, em geral, um cenário de evolução na situação de 2010. Contudo, ainda havia muitas instituições na faixa inicial de governança de TI, o que estava distante do aceitável, tendo como referência os modelos de boas práticas de governança de TI, a legislação e a jurisprudência vigentes. Apesar da evolução, a alta administração das instituições públicas, em geral, continuou a não se preocupar com a

gestão e o uso de TI, situação que poderia comprometer o desempenho e, por consequência, o alcance dos objetivos institucionais. No que se refere à segurança da informação, percebe-se que houve melhoria percentual discreta em apenas metade dos critérios questionados em relação a 2010. A partir da análise do relatório (Brasil 2012), destacam-se as seguintes vulnerabilidades:

a) menos da metade das instituições questionadas implementaram uma Política de Segurança da Informação (PSI);

b) 90% das instituições públicas federais ainda não realizam Análise de Riscos (AR) aos quais a informação crítica para o negócio está submetida, considerando-se os objetivos de disponibilidade, integridade, confidencialidade e autenticidade;

c) apenas metade das instituições possuem equipe específica para gerenciar a segurança da informação;

d) somente 17% das instituições possuem processo de classificação das informações, apesar da Lei 12.527/2011- LAI, que regula o acesso a informações mantidas pelo Estado. A ausência de classificação pode implicar tratamento inadequado da informação, como a divulgação ostensiva de dados não públicos;

e) o percentual de instituições que implementaram (aprovaram e publicaram) os processos corporativos relativos à gestão dos incidentes de segurança da informação recuou em relação a 2010. Pode-se inferir que, apenas, 16% das instituições possuem uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) formalmente instituídas;

f) a proteção aos ativos de informação[9] permanece muito prejudicada, tendo em vista que 76% das instituições não implementaram os processos corporativos referentes ao Inventário dos ativos de informação (dados, *hardware, software* e instalações);

g) o índice de instituições que realizam auditorias internas[10] de segurança da informação diminuiu em relação a 2010. A ausência de pessoal com conhecimento especializado para realizar esse tipo de trabalho contribui para que 80% das instituições não realizem auditorias de segurança da informação;

h) também foi avaliado o controle sobre elementos críticos da gestão de segurança da informação, em linha com as normas da família ABNT NBR

[9] São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2009).

[10] É uma atividade, exercida de forma independente da gestão, que tem como um dos objetivos a avaliação dos controles internos, ou seja, mitigar os riscos de que a organização não alcance seus objetivos.

ISO/IEC 27000. A capacidade da alta administração da APF em controlar a gestão de processos e resultados de TI é baixa, tendo em vista que 72% das respostas concentraram-se na faixa inicial de capacidade;

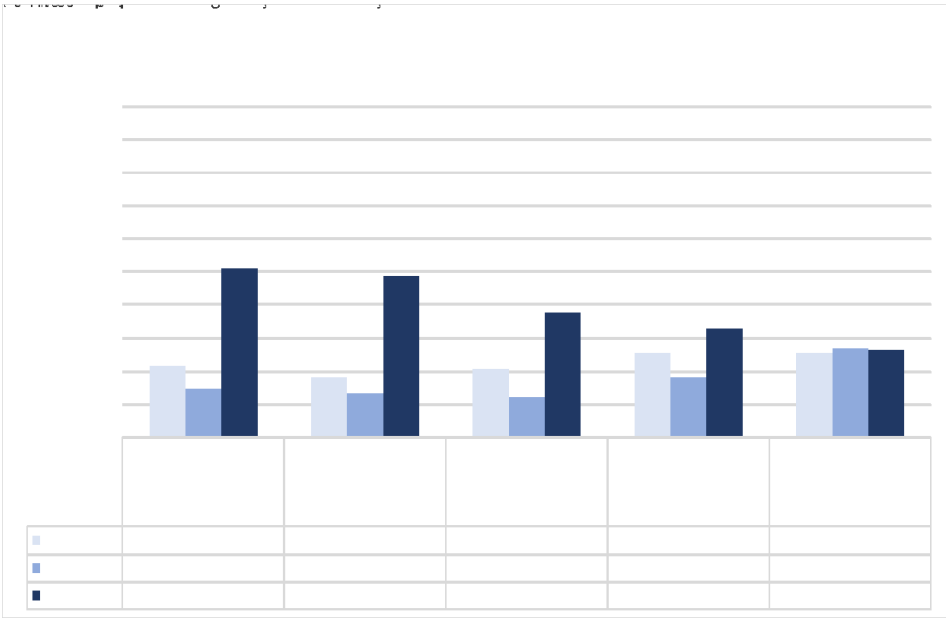
i) 40% de instituições são dependentes de pessoas externas aos seus quadros, o que gera dúvidas acerca da continuidade da gestão e dos projetos de TI, bem como impacta negativamente a capacidade de gerir incidentes de segurança.

Continuando o processo de avaliação do ciclo 2012, foram realizadas, em 2013, auditorias específicas em uma amostra de 20 organizações, com o objetivo de validar a situação apurada no levantamento anterior, bem como avaliar a gestão de risco e o alcance dos resultados de TI. As fiscalizações revelaram que, em geral, a situação real dos auditados era menos favorável do que a informada no questionário (Brasil 2014).

O ciclo de 2014, além de atualizar o panorama traçado em 2012, trouxe como aprimoramento a mudança da escala de resposta do questionário, que antes era binária (sim ou não), e passou a ter cinco categorias de resposta relativas ao nível de adoção da prática (não se aplica, não adota, iniciou plano para adotar, adota parcialmente, adota integralmente). A compilação dos dados coletados, por sua vez, demonstrou, em geral, uma tendência de evolução da situação. Todavia, ainda está distante do ideal, haja vista o nível de adoção insuficiente de muitas práticas fundamentais para que a TI agregue o valor devido aos resultados organizacionais.

No que tange à segurança da informação, como percebido em todos os levantamentos anteriores, o tema continua a ser de preocupação, por causa da baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis. A figura 2 apresenta os resultados obtidos em relação às políticas e responsabilidades para a gestão corporativa da segurança da informação questionados em 2014.

Figura 2: Gráfico de resultados de segurança da informação do TCU - 2014



Fonte: Relatório de Levantamento (Brasil 2014).

Analisando os dados levantados e em complemento aos já mapeados em anos anteriores, evidenciam-se as seguintes vulnerabilidades (Brasil 2014):

a) 34% das organizações não dispõem de Política de Segurança da Informação (PSI) formalmente instituída;

b) 38% das organizações não dispõem de comitê de segurança da informação formalmente instituído (responsável por formular e conduzir diretrizes para a segurança da informação corporativa), colocando em risco a efetividade de suas ações de proteção à informação;

c) metade das organizações não possuem gestor da segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação;

d) quase a metade (48%) dos órgãos não normatizam o controle de acesso às informações e aos recursos e serviços de TI;

e) apenas 54% possuem política de cópias de segurança (*backup*), que são necessárias para garantir a disponibilidade das informações em casos de falhas de sistemas ou pessoas;

f) somente 23% das organizações participantes dispõem de política corporativa de gestão de riscos;

g) é reduzido o número de organizações que monitoram a governança e o uso de TI. Apenas 37% das pesquisadas possuem estabelecida prática de avaliar

periodicamente seus sistemas de informação, enquanto 39% das organizações avaliam a gestão da segurança da informação.

A despeito da evolução identificada no período 2012 a 2014, o nível de adoção das práticas apresentadas está muito distante do esperado, situação que revela a existência de lacunas na coordenação e na normatização da gestão corporativa da segurança da informação e que expõe a APF a diversas situações desastrosas, como indisponibilidade de serviços e perda de integridade de informações. Dentre as vulnerabilidades levantadas, destacam-se, pela relevância e gravidade, as ausências das Políticas de Segurança da Informação (34%) e de Gestão de Riscos (77%) em parte significativa das instituições questionadas (TCU 2014).

Uma PSI corporativa é o principal instrumento direcionador da gestão da segurança da informação, sua não implantação pode implicar: procedimentos não padronizados relativos à segurança, deficiência nos controles de segurança, dificuldade de responsabilização em incidentes de segurança, risco de acessos não autorizados e de vazamento de dados e informações, entre outros. Não obstante, o nível baixo de maturidade do processo de gestão de riscos pode gerar potenciais efeitos negativos como: ineficiência na aplicação dos recursos, desconhecimento dos riscos aos quais os processos críticos da instituição estão expostos e ausência de critérios sólidos para planejamento e priorização das ações de segurança da informação. Além disso, as diretrizes da PSI e o resultado da análise de riscos são insumos fundamentais para outros processos essenciais, como a gestão de continuidade do negócio (TCU 2012, 2014).

A fim de constituir um panorama em dados e evidências para caracterização dos perfis, a última área analisada é relativa aos grandes eventos ocorridos no país e suas demandas por segurança cibernética, incluindo os Jogos Olímpicos de 2012 em Londres e o Programa Nacional de Segurança Cibernética do Reino Unido.

5 A SEGURANÇA CIBERNÉTICA E OS GRANDES EVENTOS

Os Grandes Eventos internacionais, particularmente os esportivos como os Jogos Olímpicos e a Copa do Mundo de Futebol, tem proporcionado ambiente propício para quebras de paradigmas e inovações no campo das TICs. Em consequência, processos, *modus operandi* e medidas de proteção e de segurança do espaço cibernético foram sendo ajustadas e otimizadas, bem como heterogêneas e assimétricas formas de ameaças foram mapeadas e mitigadas de acordo com as peculiaridades de cada evento e com as características ambientais e políticas de cada cidade sede.

5.1 Os grandes eventos no Brasil

A partir de 2012, um amplo e heterogêneo ciclo de eventos internacionais, sediados pelo Brasil, teve início com a Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio+20), seguida da Copa das Confederações (Copa Conf 2013), da Jornada Mundial da Juventude (JMJ 2013) e da Copa do Mundo de Futebol (FIFA 2014). Tal ciclo finaliza-se em 2016, com a realização dos Jogos Olímpicos e Paralímpicos.

A realização dos chamados "Grandes Eventos" trouxe aspectos diferenciados e inovadores no contexto da segurança do país. A participação do Centro de Defesa Cibernética (CDCiber)[11] na Rio+20 foi desafiadora pelo seu ineditismo e inovação para a Defesa Nacional. Pela primeira vez, um planejamento operacional militar levou em consideração as ameaças advindas do espaço cibernético, com potencial para comprometer o comando e o controle das operações de segurança e para afetar a imagem do Brasil como país capaz de organizar um grande evento internacional. Durante a realização da Rio+20, o CDCiber analisou e tratou diversos tipos de incidentes de segurança ocorridos em órgãos governamentais ou responsáveis pelas infraestruturas críticas nacionais, diretamente relacionadas ou não ao evento (Wallier Vianna 2013).

Segundo Camelo e Carneiro (2014), durante as realizações da Copa Conf e da JMJ, ambos em 2013, houve substancial incremento quanto ao nível de maturidade no modelo de ações de proteção baseado na metodologia de tratamento de incidentes de rede, em comparação àquele empregado na Rio+20. Segundo esses autores, tornou-se possível uma gestão mais ampla dos incidentes que estavam acontecendo, suportada em ferramentas de gerenciamento de risco, apoio à decisão e inteligência de negócio. Dentre os diversos tipos de incidentes de segurança passíveis de serem analisados e tratados, os autores destacam:

a) abuso de sítios (desfiguração, injeção de código etc.);
b) páginas falsas;
c) inclusão remota de arquivos (*remote file inclusion* - *RFI*) em servidores *Web*;
d) uso abusivo de servidores de correio eletrônico (*e-mail)*;
e) hospedagem ou redirecionamento de artefatos ou código malicioso;
f) ataques de negação de serviço ou indisponibilidade de domínio;
g) uso ou acesso não autorizado a sistemas ou dados;

[11] Organização Militar do Exército Brasileiro que nos Grandes Eventos internacionais coordenou e integrou as atividades de segurança e defesa cibernéticas em apoio a Segurança governamental do Evento.

h) varredura de portas;

i) comprometimento de computadores ou redes;

j) desrespeito à política de segurança ou uso inadequado dos recursos de TI;

k) ataques de engenharia social (*phishing)*;

l) cópia e distribuição não autorizada de material protegido por direitos autorais;

m) uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

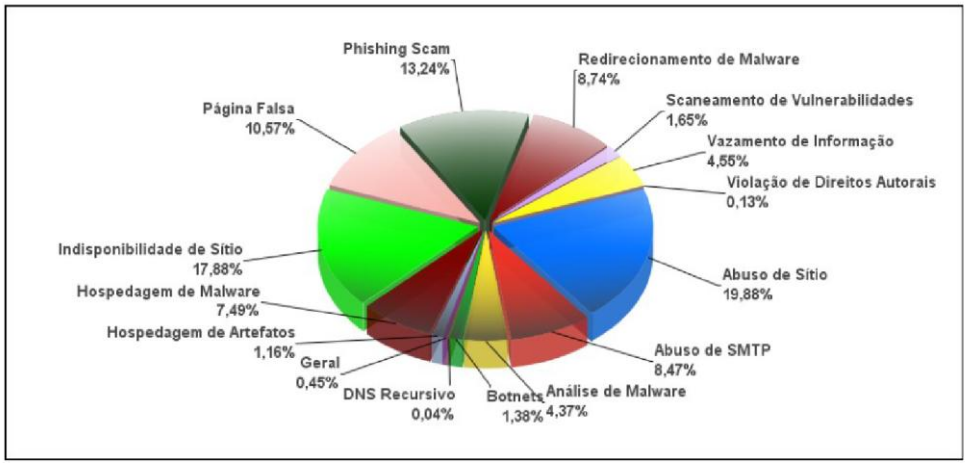
Dessa forma, durante as fases de planejamento, preparação e operação da Copa do Mundo 2014, diversas ações foram desenvolvidas e serviços disponibilizados, os quais podem ser concentrados nas seguintes atividades: identificação de ativos, análise de riscos, tratamento de eventos de segurança e notificação de incidentes[12].

Cabe destacar que a realização da segurança cibernética nos Grandes Eventos pode ser caracterizada como uma operação interagências (órgãos da APF, agências governamentais, órgãos estaduais e municipais, entre outros), inclusive na sua fase de planejamento. Tal fato consolidou a necessidade de estabelecimento de parcerias e do trabalho colaborativo nos diversos níveis organizacionais.

Não obstante, apesar das operações realizadas nos grandes eventos serem definidas em tempo, espaço e motivação peculiares; as ameaças, vulnerabilidades e os incidentes de segurança, ocorridos ou mapeados, são semelhantes àqueles enfrentados, diariamente, pelos agentes responsáveis pela gestão da segurança nos órgãos e instituições da Administração Pública Federal. Neste contexto, a Figura 3 apresenta as estatísticas de distribuição de incidentes por categoria na APF, compiladas pelo Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal – CTIR Gov, referentes ao 3° trimestre de 2014.

[12] Palestra realizada no 3º Fórum Brasileiro de CSIRTS. Disponível em: <http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf>. Acesso em: 01 dez. 2014.

Figura 3: Distribuição de incidentes por categoria



Fonte: CTIR Gov.

http://www.ctir.gov.br/arquivos/estatisticas/2014/Estatisticas_CTIR_Gov_3o_Trimestre_2014.pdf.

Soma-se ao rol de vulnerabilidades anteriormente citadas, oriundas do NIC.br, do TCU e dos Grandes Eventos, a carência de um arcabouço jurídico específico, com penas severas, bem como a necessidade de implementação de ritos processuais mais céleres e adequados aos "crimes cibernéticos". Essas fragilidades legais ampliam a sensação de impunidade e podem constituir fator indutor de instalação de bases cibernéticas para terroristas, fraudadores bancários, narcotraficantes e criminosos em geral.

5.2 A experiência do Reino Unido

A fim de proporcionar um quadro claro e compreensível dos riscos e responder aos incidentes de segurança cibernética relativos aos Jogos Olímpicos e Paralímpicos de 2012, foi constituído um Centro de Operações de Segurança Cibernética do Reino Unido (*UK Ciber Security Operations Centre* - CSOC). O CSOC foi composto por profissionais oriundos de vários departamentos governamentais e dentre as atividades realizadas pode-se destacar:

a) avaliação da ameaça cibernética antes e durante os Jogos;

b) criação de um programa de exercícios cibernéticos relacionados às Olimpíadas;

c) planejamento, implementação e liderança da Equipe de Coordenação Cibernética para as Olimpíadas;

d) resolução de incidentes de segurança cibernética durante os Jogos;

e) apoio ao Centro de Coordenação Olímpica Nacional e ao Centro de Inteligência Olímpica;

f) manutenção do quadro de consciência situacional cibernética da comunidade.

Cabe destacar que duas ações específicas da Olimpíada de Londres, relacionadas à cooperação entre departamentos governamentais e ao estabelecimento de um programa de exercícios cibernéticos, estavam inseridas no Programa Nacional de Segurança Cibernética (*National Cyber Security Programme* - NCSP)[13]. O NCSP, lançado pelo governo do Reino Unido em novembro de 2011, buscou, na essência, incrementar o nível de proteção às atividades públicas ou privadas (sociedade em geral e comerciais) realizadas no espaço cibernético britânico, tratando-se de um esforço nacional para capacitar e promover a segurança cibernética em todos os setores da sociedade.

No que tange à área de recursos humanos, o NCSP, na sua versão de dezembro de 2014[14], apresenta o objetivo n. 4: *"Building Cross Cutting Knowledge, Skills and Capability"*, centrado em cinco ações:

a) desenvolver, por meio do uso massivo de cursos abertos à distância, a força de trabalho de hoje e do futuro, incluindo desde o ensino de programação para os estudantes do ensino fundamental até a educação superior;

b) aumentar a pesquisa em segurança cibernética *(Cybersecurity)*;

c) desenvolver uma profissão de segurança cibernética;

d) influenciar profissões associadas;

e) entender, gerenciar, promover e sustentar (como ações gerenciais) a segurança cibernética.

Destaca-se que a Universidade de Cranfield, um dos 13 Centros Acadêmicos de Excelência do Reino Unido acreditados para o ensino e a pesquisa em segurança do espaço cibernético, além de cursos centrados nas TICs, oferece, também, cursos de pós-graduação que abordam temas relacionados às tecnologias sociais e ao comportamento humano.

No ambiente comportamental diretamente relacionado ao espaço cibernético da Administração Pública Federal brasileira, o capítulo a seguir estratifica os procedimentos

---

[13] Maiores informações estão disponíveis em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf >.

[14] Maiores informações estão disponíveis em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386094/Infographic_The_UK_Cyber_Security_Strategy_December_2014.pdf>.

dos agentes que atuam na gestão da segurança cibernética em três níveis de atuação (perfis profissionais): operacional, estratégico e tático.

6 SUGESTÕES DE PERFIS E DE MINUTAS DE PROCEDIMENTOS PROFISSIONAIS

Como já foi anteriormente comentado, para fins deste estudo, considera-se que as atividades inerentes à segurança cibernética estão inseridas no contexto mais abrangente da segurança da informação. Ou seja, o profissional que atua na segurança cibernética, também "realiza" segurança da informação. A segurança cibernética, além de herdar diversas características da segurança da informação, carrega, no seu bojo, a necessidade de resposta rápida, particularmente em face dos eventos de segurança[15] que venham a ocorrer.

As atividades de segurança cibernética extrapolam a simples utilização das denominadas soluções de segurança para as TIC como antivírus, *Firewall* ou sistemas detectores de intrusão (*Intrusion Detection System* - IDS). Devem, as mesmas, ser tratadas com maior abrangência, envolvendo o comportamento das pessoas inseridas nos mais diversos níveis da organização e nos processos que elas executam. Dessa forma, a cultura de segurança informacional, particularmente as diretamente ligadas ao uso de TI e da Internet, deve permear todo o contexto organizacional. Não obstante, considera-se a necessidade de uma equipe especializada e responsável pelo tratamento e resposta dos incidentes de segurança nas redes de computadores da instituição.

No contexto governamental, a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, disciplinou a Gestão de Segurança da Informação e Comunicações (considerada aqui como sinônimo de segurança da informação) na Administração Pública Federal, direta e indireta, determinando, entre outros assuntos, no seu Art. 5º, que aos órgãos e entidades da APF compete: coordenar as ações de segurança da informação e comunicações, aprovar Política de Segurança da Informação e Comunicações e implementar equipe de tratamento e resposta a incidentes em redes computacionais (Brasil 2008).

Assim sendo, apresentam-se diversos procedimentos que podem ser operacionalizados através de gestores responsáveis pela gestão da segurança da Informação no espaço cibernético governamental. As minutas de procedimentos estão diretamente relacionadas com os papéis organizacionais desempenhados pelo agente público que atua na gestão corporativa da segurança da Informação e podem ser

[15] Considera-se como evento de segurança qualquer indício, fato, relato, comprovado ou não, que possa ser relacionado à segurança do espaço cibernético.

grupados em três grandes áreas ou perfis de atuação: nível operacional, nível estratégico e nível tático.

6.1 Minuta de procedimentos de Nível operacional em segurança cibernética

Abrange as atividades técnicas que asseguram o correto funcionamento dos recursos de TIC da Organização. O agente público, inserido no nível operacional, lida mais estreitamente com atividades típicas da segurança cibernética, como pode ser percebido na listagem a seguir:

a) contato direto com sistemas computacionais, de controle ou rede de computadores;

b) configuração, operação, manutenção e monitoramento das aplicações e infraestruturas de TIC (incluindo as redes internas e o acesso à Internet);

c) tratamento (correção e mitigação) de vulnerabilidades de TIC;

d) suporte e configuração de ferramentas de segurança;

e) planejamento de treinamento modularizado por assunto/tecnologia e diversificado por níveis de compreensão e áreas de atuação;

f) implementação de controle de acesso à informação aos recursos e serviços de TI;

g) gerenciamento de cópias de segurança (*backup*);

h) composição de estatísticas para apoio à decisão;

i) levantamento de tendências com dados oriundos dos sistemas e das redes;

j) solicitação de auditorias de dados, de adequação de *hardware*, de segurança de redes, de sistemas e aplicativos, entre outras;

k) monitoramento do tráfego das redes;

l) apoio as atividades de análise Forense;

m) avaliação de produtos, serviços e soluções das empresas nacionais e internacionais;

6.2 Minuta de procedimentos de Nível estratégico em segurança cibernética

Os agentes públicos envolvidos neste nível tratam das ações corporativas e dos cuidados necessários com a segurança da informação institucional, na sua expressão mais abrangente, incluindo pessoas, processos e tecnologia. São responsáveis por coordenar a segurança dos ativos de informação, visando assegurar ou garantir a continuidade das atividades institucionais. Consideram-se como principais procedimentos:

a) coordenação, planejamento e gestão de alto nível para alcançar resultados de longo prazo;

b) implementação da gestão de riscos, da gestão de continuidade do negócio e da recuperação de desastres;

c) formulação e implantação da Política de Segurança da Informação;

d) disseminação de informações relacionadas à segurança da informação;

e) estímulo à construção de consciência quanto a importância da segurança da Informação, por meio de ações de sensibilização, educação e treinamento;

f) manutenção de atividades e programas que estimulem a conscientização da alta administração acerca dos conceitos, objetivos, indicadores, ações e infraestruturas de segurança da informação;

g) apoio à estruturação da área operacional de TIC e da ETIR;

h) planejamento da classificação e do tratamento de informações;

i) cooperação com os órgãos nacionais e internacionais, públicos e privados, envolvidos na segurança da informação;

j) articulação com os órgão responsáveis pela segurança e defesa do setor cibernético no país e no exterior.

6.3 Minuta de procedimentos de Nível tático em segurança cibernética

Nesta perspectiva, são desenvolvidas ações de gerenciamento de incidentes de segurança em redes de computadores, ou seja, as mesmas relacionam-se diretamente com as atividades desenvolvidas por uma ETIR (Brasil 2009), onde pode ser percebido forte viés colaborativo e de compartilhamento de informações. Procedimentos típicos:

a) tratamento de incidentes (detecção, triagem, análise, resposta);

b) análise e tratamento de artefatos maliciosos;

c) recebimento e envio de notificações sobre incidentes de segurança nacionais e internacionais;

d) realização de análise computacional (forense);

e) realização de alertas e notificações;

f) realização de vistorias técnicas, avaliação de segurança e auditorias;

g) disponibilização de correções de segurança em *softwares* de desenvolvimento de sítios e sistemas, particularmente para linguagens *Web*;

h) realização de análise de vulnerabilidades na infraestrutura de TIC da organização;

i) desenvolvimento de ferramentas de apoio à segurança;

j) certificação ou avaliação de produtos e serviços;

k) acompanhamento de novas ameaças cibernéticas e de possíveis explorações de vulnerabilidades, bem como das ações dos principais grupos de ativistas *Hackers;*

l) estabelecimento de parcerias com centros de tratamento de incidentes nacionais e internacionais;

m) articulação com órgãos de inteligência e policiais, em caso de ataques múltiplos e em grande escala;

n) acompanhamento do desenvolvimento do arcabouço jurídico nacional e das normas internacionais relacionados a incidentes de segurança cibernéticos.

7 CONSIDERAÇÕES FINAIS

Observa-se uma crescente dependência das organizações governamentais em relação aos sistemas computacionais e a progressiva integração desses sistemas por intermédio das redes de computadores. Aflora a inexorabilidade do espaço cibernético para o desenvolvimento de um Estado-nação, como pode ser constatado no Programa Nacional de Segurança Cibernética do Reino Unido (NCSP-UK).

Independente de uma estratégia ou de um programa nacional para a segurança do espaço cibernético brasileiro, os Grandes Eventos vêm contribuindo para evidenciar a importância e a necessidade da segurança e da defesa cibernéticas como vetor de sustentabilidade e progresso do País.

Segundo o TCU (2014), o uso cada vez mais crescente das TICs na execução dos processos organizacionais, em especial dos finalísticos, vem acompanhado do aumento do risco de segurança da informação, requerendo maior atenção da APF no estabelecimento dos processos e controles voltados à proteção das informações. Neste contexto, para a maioria das instituições da APF, a informação e a tecnologia são ativos críticos interdependentes que representam os seus bens mais valiosos, mas em muitas situações transparecem como pouco compreendidas e apoiadas pela alta administração.

A segurança do governo eletrônico brasileiro é testada cotidianamente e deve ser constantemente aprimorada pelos órgãos da Administração Pública que disponibilizam as informações. Assim sendo, assegurar um patamar aceitável de Segurança da Informação, no ambiente cibernético (ou Segurança Cibernética), é algo que viabiliza e agrega valor aos serviços e aplicações, sustentando e garantindo a credibilidade da Instituição, na proporção em que possibilita a satisfação dos cidadãos, a produtividade de seus colaboradores e mantém a imagem que a Instituição constituiu na sociedade.

A segurança da informação, no espaço cibernético, ultrapassa as fronteiras tecnológicas, não se limitando às soluções de segurança de TIC e torna-se primordial avançar em conceitos mais abrangentes e complexos, como promover o debate e o desenvolvimento de procedimentos de Segurança Cibernética, contemplando as pessoas e os processos inerentes.

Dessa forma, buscou-se ampliar a discussão sobre o tema, analisando os procedimentos peculiares à segurança cibernética realizados pelos agentes públicos nacionais, e estratificá-los em três perspectivas de atuação ou papéis organizacionais desempenhados: nível operacional, nível estratégico e nível tático. Na sequência, entende-se que o tema deva ser aprofundado como, por exemplo, com o mapeamento das necessidades informacionais dos agentes públicos no seu ambiente de trabalho e de acordo com as tarefas realizadas.

Concluindo, os procedimentos e suas perspectivas de atuação devem ser adaptados para que estejam perfeitamente alinhados com a Política de Segurança da Informação de cada órgão ou Instituição da Administração Pública, bem como podem ser consolidados como instrumentos norteadores de desempenho das pessoas, processos e serviços intrínsecos à gestão da segurança da cibernética em organizações públicas e privadas.

REFERÊNCIAS

Academia Latino-Americana de Segurança da Informação. 2006. *Introdução à Segurança da Informação*. Microsoft TechNet. http://www.nerdbb.com/download/file.php?id=2618.

Associação Brasileira de Normas Técnicas. 2013. *NBR ISO/IEC 27002:2013: Tecnologia da informação: Técnicas de segurança: Código de prática para controles de segurança da informação*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

Brasil. Gabinete de Segurança Institucional da Presidência da República. 2008. “Instrução Normativa GSIPR n. 1, de 13 de junho de 2008.” Disciplina a gestão da segurança da informação e comunicações na administração pública federal, direta e indireta e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, (115) junho. Seção 1.

Brasil. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. 2009. “Norma Complementar n. 05/IN01/DSIC /GSIPR.” Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. *Diário Oficial [da] República Federativa do Brasil* (156), agosto. Seção 1.

Brasil. Tribunal de Contas da União. 2014. *Acórdão n. 3117/2014 – TCU – Plenário*. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU.

http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141114/AC_3117_45_14_P.doc.

Brasil. Tribunal de Contas da União. 2012. *Acórdão n. 2585/2012 – TCU – Plenário*. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU. http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367.

Brasil. Tribunal de Contas da União. 2010. *Acórdão n. 2308/2010 – TCU – Plenário*. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU. http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500E3BC0A19993DE040010A8900136B.

Camelo, J. R. de S., J. M. E. Carneiro. 2014. “A atuação do Centro de Defesa Cibernética na Copa das Confederações FIFA/2013.” In *Segurança e defesa cibernética: da fronteira física aos muros virtuais*, organizado por Oscar Medeiros Filho, Walfredo Bento Ferreira Neto, e Selma Lúcia de Moura Gonzáles, 149-74. Recife: Editora UFPE.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. 2012. *Cartilha de segurança para a Internet*. São Paulo: Comitê Gestor da Internet no Brasil. http://cartilha.cert.br/.

Fernandes, Jorge H. C. 2013. “Ciência, tecnologia e inovação no setor cibernético: Desafios e oportunidades (Painel 5).” In *Encontro Nacional de Estudos Estratégicos, Rio de Janeiro, setembro 25-27 2013, Ministério de Assuntos Estratégicos.* http://pt.slideshare.net/saepr/apresentao-cincia-tecnologia-e-inovao-no-setor-ciberntico-desafios-e-oportunidades.

Fernandes, Jorge H. C. 2012. *Segurança e defesa cibernéticas para reduzir vulnerabilidades nas infraestruturas críticas nacionais (Relatório Técnico)*. Brasília: Núcleo de Estudos Prospectivos do Exército Brasileiro. http://www.eme.eb.mil.br/ceeex/public/arquivos/nep2012/NEP_CEEEx_Jorge_Fernandes_2012.pdf.

International Organization for Standardization. 2012. *ISO/IEC 27032: Information technology: Security techniques: Guidelines for cybersecurity*. Geneva: ISO/IEC.

International Organization for Standardization. 2014. *ISO/IEC 27000: Information technology: Security techniques: Information security management systems: Overview and vocabulary*. Geneva: ISO/IEC.

Klimburg, Alexander. 2012. *National cyber security framework manual*. Talinn: NATO CCD COE Publication.

Núcleo de Informação e Coordenação do Ponto br. 2010. *Dimensões e características da web brasileira: um estudo do gov.br.* Brasília: Núcleo de Informação e Coordenação do Ponto br. http://www.cgi.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-da-informacao-e-da-comunicacao-no-brasil-tic-governo-eletronico-2010/.

Revista Brasileira de Inteligência. 2007. Brasília: Abin, 3(4), September.

Senado Federal. 2014. “Espionagem cibernética.” *Em Discussão!* 21, July. http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/.

Wallier Vianna, Eduardo. 2013. “A segurança cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável.” In: *Ciência, tecnologia e inovação: Pontes para a segurança pública*, organizado por M. K. Nakaiama, 127-56. Florianópolis: FUNJAB.

Wallier Vianna, Eduardo. 2011. “Procedimentos para a gestão de incidentes de segurança nas redes de computadores da Administração Pública Federal.” Monografia de Especialização, Universidade de Brasília. http://dsic.planalto.gov.br/documentos/cegsic/monografias_2009_2011/16_Eduardo_Wallier.pdf.

WIENER, Norbert. 1995. *Cybernetics: Or the control and Communication in the animal and the machine*. 2nd ed. EUA: MIT Press. 1995.