DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

COMISSÃO DE CIÊNCIA E TECNOLOGIA, COMUNICAÇÃO E INFORMÁTICA			
EVENTO: Audiência Pública	REUNIÃO Nº: 1289/2014		DATA: 3/12/2014
LOCAL: Plenário 13 das Comissões	INÍCIO: 9h51min	TÉRMINO: 11h37min	PÁGINAS: 40

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

JOSÉ NEY DE OLIVEIRA LIMA - Coordenador-Geral de Segurança da Informação, do Ministério do Planejamento, Orçamento e Gestão.
JOSÉ GUSTAVO SAMPAIO GONTIJO - Diretor do Departamento de Ciência, Indústria e Tecnologia, da Secretaria de Telecomunicações, do Ministério das Comunicações.
VIRGÍLIO AUGUSTO FERNANDES ALMEIDA - Secretário de Políticas de Informação, do Ministério da Ciência e Tecnologia.
TAKAHARU UCHINO - Diretor do Departamento de Tecnologia da Informação, do Ministério da Defesa.
MARCONI DOS REIS BEZERRA - Coordenador-Geral do Sistema se Segurança e Credenciamento, do Departamento de Segurança da Informação e Comunicações, da Secretaria-Executiva do Gabinete de Segurança Institucional da Presidência da República.
CRISTINE HOEPERS - Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil — CERT.
RODOLFO FUCHER - Diretor de Relacionamento Institucional da Associação Brasileira das Empresas de *Software* — ABES.

SUMÁRIO

Debate sobre o Plano de Ação de Políticas de Segurança da Informação do Governo Federal, em especial o disposto no Decreto nº 8.135, de 2013.

OBSERVAÇÕES

Houve exibição de imagens.

O SR. PRESIDENTE (Deputado Ricardo Tripoli) - Havendo número regimental, declaro aberta a presente reunião. Leitura e votação da Ata da 25º reunião.

O SR. DEPUTADO BILAC PINTO - Sr. Presidente, peço a dispensa da leitura da ata.

O SR. PRESIDENTE (Deputado Ricardo Tripoli) - O Deputado Bilac Pinto solicita a dispensa da leitura da ata.

Em discussão a ata. *(Pausa.)*

Não havendo quem queira discutir, se os Deputados estiverem de acordo, permaneçam como se encontram.

Estão aprovadas as atas da sessão anterior. *(Pausa)*

A presente audiência pública é fruto dos Requerimentos de nºs 337, de 2014, de iniciativa do nobre Deputado Bilac Pinto e 338, de 2014, de iniciativa do nobre Deputado Paulo Abi-Ackel.

Debaterão o Plano de Ação de Políticas de Segurança da Informação do Governo Federal, em especial o disposto no Decreto 8.135, de 2013.

Expositores. Julgo dispensável a leitura dos nomes dos convidados, já amplamente divulgados pela Comissão.

Sendo assim, justificaram a ausência o Exmo. Sr. Ministro-Chefe da Casa Civil da Presidência da República, Aloizio Mercadante; a Exma. Sra. Ministra de Estado do Planejamento, Orçamento e Gestão, Miriam Belchior, que encaminhou o representante Sr. José Ney de Oliveira Lima, Coordenador-Geral de Segurança da Informação; o Exmo. Sr. Ministro de Estado das Comunicações, Paulo Bernardo Silva, que será representado pelo Sr. José Gustavo Sampaio Gontijo, Diretor do Departamento de Ciência, Indústria e Tecnologia; o Exmo. Sr. Ministro de Estado da Ciência, Tecnologia e Inovação, Clelio Campolina Diniz, que será representado pelo Sr. Vírgilio Almeida, Secretário de Política de Informática; o Exmo. Sr. Ministro de Estado da Defesa, Celso Amorim, que será representado pelo Sr. Takaharu Uchino, Diretor do Departamento de Tecnologia de Informação; o Exmo. Sr. Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República, General de Exército José Elito Carvalho Siqueira, que será representado pelo Exmo. Sr. General de Brigada Marconi dos Reis Bezerra, Diretor substituto do Departamento de

Segurança da Informação e Comunicações; o Sr. Demi Getschko, Conselheiro do Comitê Gestor da Internet no Brasil, que terá como representante a Sra. Cristine Hoepers, Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil; o Sr. Manoel Antonio dos Santos, Diretor Jurídico da Associação Brasileira das Empresas de *Software* — ABES, que será representado pelo Sr. Rodolfo Fucher, Diretor-Adjunto; o Sr. Jeovani Salomão, Vice-Presidente de Articulação Política da Associação das Empresas Brasileiras de Tecnologia da Informação.

Nós dividiremos em duas composições, pelo volume de expositores que temos. Desde já convido a tomarem assento os Srs. José Ney de Oliveira Lima, do Ministério do Planejamento, por gentileza; o Sr. José Gustavo Sampaio Gontijo, do Ministério das Comunicações; e o Sr. Virgílio Almeida, do Ministério da Ciência, Tecnologia e Inovação.

Gostaria, primeiro, de agradecer imensamente a todos a presença. Com certeza irão enriquecer a Câmara Federal. Obviamente esta reunião dá oportunidade àqueles Parlamentares que estão e passarão neste plenário. Mas é sempre bom informar que, como temos a Internet à disposição, os Parlamentares, muitas vezes, acompanham, nos seus gabinetes ou no plenário. Estamos tendo sessão hoje, agora, às 10 horas da manhã, uma continuidade da sessão de ontem. Por conta de um problema ocorrido no plenário, o Presidente do Congresso Nacional suspendeu a sessão, que continua hoje, às 10 horas. Obviamente, isso não implica que não possamos fazer nossa reunião, mas teremos um fluxo de Parlamentares que estarão passando durante todo esse período. Vários demonstraram um grande interesse por essa matéria.

Eu queria louvar a iniciativa do nobre Deputado Bilac por ter proposto e aprovado esta matéria, com a sustentação que fez, obviamente aprovada por todos os pares da Comissão. Eu diria que é uma das matérias mais importantes que esta Comissão tem discutido, algo que a população cobra muito do Congresso Nacional.

Os Parlamentares, quando verificaram a iniciativa do nobre Deputado Bilac Pinto, imediatamente fizeram gestão no sentido de aprovar e realizar uma lista de pessoas que tivessem envolvimento com a causa e que pudessem, com certeza, colaborar com os procedimentos que estão em tramitação na Comissão de Ciência e

Tecnologia. Obviamente, algumas iniciativas virão a partir das informações obtidas com os senhores. Isso dará um grande alento ao nosso segmento.

Então, cumprimento inicialmente o nobre Deputado Bilac pela iniciativa e o convido para que venha presidir e reunião.

Interrompo a reunião por um minuto para que possa fazer a transição com o nobre Deputado Bilac Pinto.

Muito obrigado a todos. Estarei atento a todas as movimentações que advirão desta reunião. *(Pausa)*

O SR. PRESIDENTE (Deputado Bilac Pinto) - Bom dia a todos. Obrigado pela presença na Comissão de Ciência e Tecnologia, Comunicação e Informática.

Vamos dar início à nossa audiência pública, agradecendo mais uma vez a todos que aceitaram o convite e compareceram para subsidiar um tema que consideramos extremamente relevante.

Fiz algumas anotações.

Desde já, gostaria de estipular o tempo de 10 minutos para cada um dos senhores convidados, prorrogável por mais 5 minutos. Fiquem à vontade se precisarem efetivamente ultrapassar o tempo da exposição.

O tema, como já disse o Presidente Ricardo Tripoli, é de extrema relevância para todos nós do Congresso Nacional. Com certeza, vocês subsidiarão uma Comissão que trata do tema com muita objetividade, para que possamos dar nossa contribuição nesta Casa no sentido de aperfeiçoar nossas instituições.

Então, começo com algo que considero extremamente relevante.

Quero agradecer, além dos nossos convidados, que já foram citados, a participação do Sr. Rodolfo Fucher, da ABES, e também do Sr. Sérgio Paulo Gallindo, Presidente da BRASSCON.

Eu diria que com esse crescente aumento da tecnologia de informação, comunicação e com a rápida disseminação, crescem também os problemas advindos dela e relacionados a ela. Surgem necessidades que eram restritas ao universo real e agora são transpostas para o virtual, potencializando nossos riscos, perigos e vulnerabilidades dos nossos dados e, por consequência, das nossas informações.

A tecnologia da informação e comunicação nos propicia inúmeras oportunidades, diferentes tipos de negócios, novos mercados, conectando as pessoas ao redor do mundo, superando fronteiras, disseminando a informação e o vasto conhecimento, irrestrito, amplo e de grande valor, impactando nos hábitos e no comportamento das pessoas e sendo a força motriz da sociedade moderna. Mas esses mesmos sistemas que nos conectam, propiciando benefícios imensuráveis, são os que nos tornam sensíveis, vulneráveis e, também, expostos aos riscos.

A questão que se coloca é como manter esse dinamismo proporcionado por essas interconexões, preservando dados, informações capitais e a própria inviolabilidade da privacidade? É um desafio complexo, denso, com variáveis, muitas vezes, incontroláveis, mas que está exposto no presente, no nosso cotidiano.

A experiência ao longo de toda a história nos mostra que proteções não são invioláveis, porque os sistemas não são estáticos, mas dinâmicos, sujeitos à intervenção humana para o bem ou para o mal.

A garantia de sistemas robustos é baseada numa arquitetura integrada, que leve em consideração os pontos de maior fragilidade do nosso sistema, por meio dos quais se quebra a segurança da informação.

A consistência do sistema implica uma solução integrada composta por, entre outros, arquitetura adequada, linguagens, processos, procedimentos de desenvolvimento, codificações, qualificações e criptografia.

As possibilidades de ataques aos sistemas ocorrem em múltiplas situações e não apenas porque neles sejam inseridos premeditadamente recursos lógicos ou físicos para a espionagem.

A segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações coorporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode ser guardada para uso restrito ou exposta ao público para consulta e aquisição. A tríade: confidencialidade, integridade e disponibilidade, segundo os padrões internacionais, representa os principais atributos que, atualmente, orientam a análise do planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger.

Com a evolução do comércio eletrônico, dos meios de troca e do compartilhamento dos dados, a privacidade da nossa sociedade de informação passou a ser também a nossa preocupação. O nível de segurança desejado pode se consubstanciar em uma política de segurança que seja seguida pela organização ou pela pessoa para garantir que, uma vez estabelecidos os princípios, aquele nível desejado seja perseguido e mantido. A constituição dessa política deve levar em conta riscos associados à falta de segurança, benefícios e custos de implementação dos mecanismos.

O assunto em debate é estratégico e de vital importância para qualquer organização ou pessoa, e a segurança digital torna-se um desafio para as sociedades modernas. Envolver os atores relevantes à sociedade civil organizada, o Legislativo, o Executivo e as forças vivas da sociedade, em que pese o alongamento do tempo para encontrarmos um caminho, será, com certeza, a nossa alternativa mais recomendada.

Diante da minha exposição, gostaria muito que iniciássemos essa audiência pública. Com certeza, o depoimento — com objetividade — de cada um dos senhores que foram convidados será para nós de grande valia, para que possamos aperfeiçoar e construir o nosso caminho, com o intuito de termos realmente uma legislação forte, duradoura, segura, transparente e que tenha a confiança da sociedade.

Então, para iniciar sua exposição, passo a palavra ao Sr. José Ney de Oliveira Lima.

O SR. JOSÉ NEY DE OLIVEIRA LIMA - Senhores, bom dia.

Sou representante do Ministério do Planejamento, Orçamento e Gestão, que tem atribuição de definir, através da Secretaria de Logística e Tecnologia da Informação, políticas e diretrizes da informatização pública federal.

Eu trouxe aqui uma proposta bem rápida, uma apresentação talvez de 10 minutos, que eu acho que define uma visão estratégica de como o Ministério do Planejamento tem trabalhado persistentemente em conjunto com o Gabinete de Segurança Institucional, o Ministério da Ciência, Tecnologia e Inovação, o Ministério das Comunicações e os nossos provedores de serviços, dos quais eu destacaria o

SERPRO, a TELEBRAS e a DATAPREV. Temos, ainda, uma parceria com o MCTI através do Centro de Tecnologia da Informação.

Então, farei minha apresentação rapidamente.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Se o senhor quiser se levantar, ali fica mais fácil para o senhor. *(Pausa.)*

O SR. JOSÉ NEY DE OLIVEIRA LIMA - Quem somos. A missão do Ministério do Planejamento, Orçamento e Gestão — acabei de falar — é promover o planejamento participativo e a melhoria da gestão pública para o desenvolvimento sustentável e socialmente includente do País. Essa é a missão do Ministério do Planejamento, representado aqui por nós, eu e o Leonardo Boselli, Diretor do Departamento de Infraestrutura de Serviços de Rede, representando a Ministra Miriam Belchior.

(Segue-se exibição de imagens.)

Essa é a missão da Secretaria de Logística e Tecnologia da Informação — SLTI, que eu já falei: planejar, coordenar, supervisionar e orientar normativamente as atividades da administração de recursos de informação e informática, de serviços gerais — e nós temos também uma linha de logística — e de gestão de convênios e contratos, de repasse, bem como propor políticas e diretrizes a elas relativas.

Nossa Secretária Loreni Foresti tem uma agenda de compromissos hoje e não pôde participar.

Nós temos aqui a definição do Tribunal de Contas da União, que caracteriza o Ministério do Planejamento como Organização Governante Superior — OGS. Ele tem a responsabilidade de normatizar e fiscalizar o uso e a gestão de TI em seus respectivos segmentos da administração pública federal (Voto do Acórdão 1.145/11 — TCU — Plenário).

Em seguida, tem o decreto do Sistema de Administração dos Recursos de Tecnologia da Informação — SISP, que nos dá a atribuição de definir essas políticas de TI para toda a administração pública federal direta, indireta, autárquica e fundacional, sendo opcional ao Ministério da Defesa, com os comandos: Marinha, Exército e Aeronáutica.

Esses são os nossos eixos temáticos. A ePING são Padrões de Interoperabilidade de Governo Eletrônico, que estão constantemente em dinâmica e

submetidos à consulta pública anualmente. Então, há uma participação muito efetiva da sociedade, das academias. Neste momento ela está com mais 15 dias em consulta pública, incluindo o Decreto nº 8.135/13. Os outros eixos são a governança, a padronização tecnológica, o *software* público, as contratações, os serviços de rede, a segurança da informação — que estou aqui representando — e o governo eletrônico. Esses são nossos eixos ou as nossas dimensões.

Os conceitos. Todos esses conceitos estão devidamente divulgados através das normas do Gabinete de Segurança Institucional, que nós representamos na Presidência da República — na presença do General Marconi. Nós temos lá um trabalho já de alguns anos na elaboração dessas normas, que são praticamente definidas para toda a administração pública federal. Aí cabe ao General depois falar sobre elas.

O arcabouço normativo. Eu falei agora: o Gabinete de Segurança Institucional da Presidência da República e como organização governante superior.

As de leis são essas:

- Lei nº 12.527/11, que tem total aderência à Lei de Acesso à Informação — LAI;

- Lei nº 9.983/00, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 — Código Penal e dá outras providências.

O Decreto nº 3.505/00 também é de origem do Gabinete de Segurança Institucional e participamos efetivamente da sua construção. Desse decreto derivou a infraestrutura de chaves públicas. Nós participamos do projeto e o coordenamos, hoje sob a governança da Casa Civil. O órgão que tem sob sua garantia é o Instituto de Tecnologia da Informação, da Presidência da República.

O Decreto 7.724 regulamenta a LAI e o 7.845 diz respeito a credenciamento de segurança e tratamento das informações, ao qual nós também aderimos através do Gabinete de Segurança Institucional da Presidência da República.

Aí estão as nossas instruções normativas, a gestão da segurança também do Gabinete de Segurança Institucional.

Todo o nosso trabalho tem total convergência com as normas instituídas pelo Gabinete de Segurança Institucional. Elas vêm do Decreto 3.505 e da Instrução

Normativa nº 1, de 2008. As seguintes são as Instruções Normativas 2 e a 3, que estabelecem criptografia baseada em algoritmo de Estado.

Nossos projetos. Nós temos uma estratégia nacional de segurança cibernética sobre a qual vou discorrer, instituída pela Portaria 124/2013, da Secretaria de Assuntos Estratégicos. Esse grupo está ativo e tem como objetivo definir uma estratégia de segurança para o Estado brasileiro. Está ainda em estágio de desenvolvimento e definição dos eixos temáticos, que são a governança, a educação e a segurança da informação, infraestrutura, pesquisa, desenvolvimento e outros eixos.

Nós entramos exatamente no domínio que cabe ao Ministério do Planejamento através do SISP, que é o Decreto 7.579 do qual já falei: definir padronizações.

Os desafios que temos. Aumento da exposição e transparência das informações — essa é uma demanda social —; aumento da demanda pelos cidadãos; aumento exponencial do compartilhamento; fragilidade de identificação de usuário, que são os acessos; compartilhamento de informação e ferramentas de ataque cada vez mais sofisticadas; crescimento exponencial do crime cibernético; dependência tecnológica de recursos de TIC — isso daí é irreversível; interdependência entre os ativos de informação; tecnologias proprietárias, um grande desafio; e outros desafios que nós temos.

Aí entra praticamente o que seria o nosso portfólio de projeto: o mapeamento de ativos, aderência ao Gabinete de Segurança Institucional, à norma, uma metodologia geral de risco para a administração pública federal, o DATAGOV, que seria a nuvem de governo. Nós teríamos já uma infraestrutura montada entre SERPRO, TELEBRAS e DATAPREV.

Possivelmente, vamos fazer um acordo de cooperação e trabalhar com essas infraestruturas, definindo um ambiente único de governo sob a gestão do Estado brasileiro.

Gerenciamento de identidade, sobre o qual falamos numa grande federação de identidade, cabendo ao Ministério do Planejamento, como organização governante superior em recursos humanos de toda a administração pública federal,

ativos, inativos e pensionistas, da ordem de 2,1 milhões de servidores. Nós vamos criar essa federação, que seria um controle único de acesso.

Não confundir o Centro de Tratamento de Resposta com o SETIGOV, que está no GSI. Aquele é para dentro da administração pública federal, sob a governança do Planejamento. A educação em SIC, a gestão de continuidade e o gerenciamento de operações e comunicações.

Nós já temos nosso projeto de INFOVIA. O Coordenador desse projeto está presente, Leonardo Boselli. Eu diria que é um projeto de sucesso, com ampla redução de custos e definições de padrões para toda a administração pública federal. Um canal seguro de comunicação na administração pública federal.

Ofereço uma ideia de como seriam esses projetos: um mapeamento de ativos, aderência à norma do GSI 10, DSIC/GSI/PR, uma metodologia de risco aderente à Norma 4, já publicada e devidamente divulgada.

Em seguida, nós teríamos uma ferramenta para toda a administração pública federal em todas as estações de trabalho, que seria desenvolvida em *software* público ou arquitetura aberta. Redução de custo e interoperável entre os demais componentes.

Aqui é o nosso DATAGOV, nossa nuvem, sobre a qual eu já falei, também aderente à Norma 14 do GSI e que deverá suportar a recuperação dessa infraestrutura em caso de desastres, fazendo com que os órgãos e entidades continuem a funcionar sem interrupção.

Computação distribuída, *hardware,* tecnologias/Internet e gerenciamento de sistema. Essa é a nuvem.

Essa seria uma proposta de estrutura de comitê.

Esses seriam os patrocinadores: Planejamento; o Gabinete de Segurança Institucional; o Ministério da Defesa; o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil — CERTBR, aqui representado pela Cristine Munique; o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal — CTIR Gov, normatizador; a Rede Nacional de Ensino e Pesquisa — RNP; e ali os nossos clientes: toda a Administração Pública Federal e os nossos provedores, SERPRO, DATAPREV, TELEBRAS, a ANATEL, regulamentadora de comunicações, e outros órgãos.

Aqui também nós vamos colocar as empresas que queiram participar desse *pool* de desenvolvimento. Isso é um esforço coletivo do Governo.

O gerenciamento de identidade, de que já falei, também aderente à Norma 7. Essas normas devem ser de conhecimento de todos os senhores. São normas muito bem-feitas, macrodiretrizes.

Sobre o projeto em desenvolvimento, nós já estamos fazendo um piloto dentro do Ministério do Planejamento com o SERPRO e a DATAPREV, com o novo sistema de pagamento da União. O projeto está bom. Eu acho que, em seguida, nós vamos exportar esse piloto para os demais órgãos da administração.

Estou falando praticamente de uma base de dados sob a custódia do Estado da ordem de 105 sistemas estruturantes críticos, desde o sistema de arrecadação, sistema de saúde, DATASUS, previdenciários, coisas dessa ordem.

São sistemas que, no arco da administração pública federal, capilarizam todo o território nacional e alguns até Estados e Municípios.

Nós podemos citar entre eles o COMPRASNET, o SICONV e outros. Dos aproximadamente 600 mil servidores ativos da União, nós temos em torno de 80% nessas estações de trabalho. São apoiadores desses 105 sistemas. É algo colossal que merece uma atenção muito especial. É essa ideia que nós estamos trazendo para cá.

O piloto é o sistema de pagamento da União, da ordem de quase 300 bilhões por ano, envolvendo 2,1 milhões de servidores.

O Centro de Tratamento de Respostas aderente à Norma do GSI 5 e 8, que define as políticas, as diretrizes e os procedimentos para o tratamento de incidentes em segurança.

Este também seria um modelo de governança desse Centro de Tratamento.

Aqui o GSI/Presidência da República, órgão normatizador.

Aqui nós estaríamos para dentro e, aderente à Norma 5 do GSI, as equipes de tratamento de respostas.

Nós não estamos construindo nada, inventando nada. Estamos apenas tentando monitorar, mapear o que já existe e definindo uma nova arquitetura de TI para o Governo. Isso remete ao que está exatamente disposto no Decreto nº 8.135.

Aqui estão os eixos que nós pretendemos. Nesse centro de tratamento, outros países, mas aí a questão é o CTIR Gov, do GSI, os cidadãos, o setor privado, as Forças Armadas, com o CDCIBER, os Estados e Municípios, o Legislativo e aqui toda a administração pública federal. Isso é uma visão de futuro.

Padrões de Auditoria — Decreto nº 8.135. Esse é o objeto da audiência pública. Nós já produzimos um documento que está em consulta pública há mais de 20 dias e o estendemos por mais 15 dias.

Eu acredito que nós vamos receber algumas propostas ou proposições de alteração do que nós estabelecemos lá.

Eu gostaria de citar que até hoje não tivemos nada no nosso portal, nenhuma proposição. Aqui tem a representação da ABES — Associação Brasileira das Empresas de Software, e já conversamos bastante. Mas nós esperamos contribuições para que exatamente o Decreto nº 8.135, de 2013, reduza ao máximo a incerteza na sua implementação. É esse o nosso propósito: reduzir as incertezas entre Governo, sociedade e os nossos provedores de serviço e fornecedores. Então, temos mais 15 dias de consulta pública.

Este aqui é um modelo de governança desse padrão que nós estamos definindo do Decreto nº 8.135, de 2013, com o crivo de segurança nacional, ouvido o Conselho de Defesa Nacional.

Aqui participa quem quiser. Nós vamos convidar quem quiser. É apenas uma ideia do que seria esse modelo de governança. Será muito dinâmico entre nós, Governo e sociedade.

A gestão de continuidade, aderente também à norma do GSI — Gabinete de Segurança Institucional da Presidência da República.

Muito obrigado, em nome da nossa Secretária Loreni.

Essa apresentação foi feita semana passada em Angola, nos países de Língua Portuguesa, e praticamente foi bem aceita pelos representantes desses países.

Muito obrigado.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Esta Presidência agradece a exposição ao Sr. José Ney de Oliveira.

Dando continuidade à nossa audiência pública, passo a palavra ao Sr. José Gustavo Sampaio Gontijo, para que faça a sua apresentação.

Agradeço a presença aos Parlamentares que compõem conosco esta Comissão.

Muito obrigado a V.Exas. pela presença.

Com a palavra o Sr. José Gustavo Sampaio Gontijo.

O SR. JOSÉ GUSTAVO SAMPAIO GONTIJO - Obrigado, Deputado Bilac Pinto. Gostaria de cumprimentar V.Exa. e todos os Parlamentares aqui presentes.

Quero agradecer, primeiro, a oportunidade de expor a visão que nós temos no Ministério das Comunicações sobre o tema.

Começarei falando um pouco do histórico, do porquê isso aconteceu. Acho que isso é um bom início para a gente entender aonde estamos chegando.

(Segue-se exibição de imagem)

Todo mundo sabe o que aconteceu em 2013. Surgiu um escândalo com denúncias sobre uma grande rede de espionagem em todos os níveis de chefes de governo, inclusive da Presidente Dilma Rousseff. Possivelmente a PETROBRAS também tenha sido interpelada de alguma maneira não convencional. De lá para cá, o Governo reagiu. E será que aquilo era verdade? Uma demonstração de que isso aconteceu é que agora, em 2014, a pessoa que denunciou, o Sr. Edward Snowden, recebeu um prêmio de direitos humanos sueco pelas denúncias que ele fez para mostrar ao mundo o que estava acontecendo.

Em 2014, o Terceiro Comitê da Assembleia Geral da Organização das Nações Unidas — ONU aprovou por unanimidade a Resolução do Brasil e da Alemanha, defendendo o direito à privacidade em caso de procedimento ilegal de espionagem.

A gente tem que entender — apenas adicionando ao que o meu colega do Ministério do Planejamento falou — que a ePING não trata só de segurança. Segurança é um dos itens da ePING. Ela trata de interconexão, meios de acesso, organização, áreas de interação do Governo. Então já existia um trabalho sendo feito e, em face do fato que ocorreu, deu-se uma ênfase em como atuar nesse sentido de proteger as redes de governo.

A gente sabe que o GSI — Gabinete de Segurança Institucional da Presidência da República vem trabalhando isso há bastante tempo, tem regulamentações desde 2000 até agora. São 4 decretos, 3 instruções normativas, 21 normas de segurança da informação e comunicação, 1 norma de credenciamento de segurança.

Isso não está acontecendo agora porque ocorreu a espionagem. O GSI trabalha com contraofensiva e sabia muito bem o que estava fazendo. Junto com os outros órgãos de Governo já vinha trabalhando com diversas normas há mais de 10 anos.

Em relação ao Decreto 8.135, de 2013, o que a gente pode apresentar — e que já foi bastante ilustrado pelo colega do Planejamento — é que as comunicações de dados da administração pública federal precisam de maior proteção. Isso é claro. O que o decreto está fazendo é regulamentando a Lei 8.666, de 1993, que diz que é dispensável a licitação quando houver possibilidade de comprometimento da segurança nacional, nos casos estabelecidos em decreto do Presidente da República, ouvido o Conselho de Defesa Nacional. Então, estamos atuando com base na regulamentação que já existia.

Devem ser adotados meios para que os serviços de correio eletrônico e funcionalidades complementares por órgãos e entidades da administração pública federal sejam protegidos, que esses programas e equipamentos tenham características que permitam uma auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações e o armazenamento e recuperação de dados de *backup*.

Isso por quê? Eu não estou falando que vou querer ver o código-fonte antes de usar o aplicativo. Mas eu quero uma garantia de que não houve alteração no processo do código que ele me entregou, se houver um vazamento de informação — corrija-me depois o pessoal especialista da área —, como aconteceu, por exemplo, nas usinas do Irã, que compraram um sistema que em algum momento foi alterado.

O órgão gerenciador das regulamentações das contratações de compras públicas no Governo Federal é o Ministério do Planejamento, por meio da Secretária de Logística e Tecnologia da Informação — SLTI.

A abrangência que se deu nessa portaria interministerial são os correios eletrônicos, óbvio. Compartilhamento e sincronização de arquivos. Uma prática muito comum tanto no setor privado quanto no setor público é a utilização de Dropbox, Google Drive. A gente sabe que isso facilita muito a nossa vida, mas cria uma vulnerabilidade gigantesca.

No Ministério das Comunicações a gente encerrou as atividades desses aplicativos e está utilizando uma solução própria do Governo. E funciona. Você cria uma VPN — Virtual Private Network , você cria uma porta. Assim, eu tenho acesso a todas as minhas pastas remotamente. O que eu alterar nela num lugar eu vejo noutro. Então, não há necessidade de utilização de Dropbox e Google Drive. São medidas pequenas que resolvem grandes situações de vulnerabilidade.

O prazo é de 24 meses para questões de serviços de TI. Para os serviços de redes de telecomunicações, o prazo é de 24 meses nas capitais e regiões metropolitanas e de 60 meses nas demais localidades para as redes do Governo Federal. Isso se dará em maio de 2016 e maio de 2019, se não me engano.

A portaria interministerial ainda falou de vários critérios de comprovação, atendimento a normas e possibilidade de realização de auditoria.

Em relação à auditoria, um exemplo do que poderia ser feito — e que é feito por algumas privadas quando se contrata algum serviço — é abrir o *software* junto com a empresa vendedora e pedir que gerem o código *hash*. Para quem não sabe, o *hash* é como se fosse a identidade digital do software. Se ele colocar um espaço dentro daquele código, muda completamente. Gerado o código *hash*, lacra-se o *software* e o entrego à empresa para guardá-lo. Se em algum momento acontecer um incidente, pode-se checar se foi alterado: *"O que você me vendeu é o que você instalou nas minhas máquinas?"* É uma forma de você comparar, é algo que me veio à mente e é simples de ser feito. Existem vários outros métodos. Esse é um deles.

Além disso, esses serviços são prestados, nos casos de redes do Governo, pela TELEBRAS, pelo SERPRO. Mas se essas instituições não tiverem o serviço necessário para o Governo, quem vai prestá-lo? Há exceção. Se o setor público não atender às condições do Governo, o privado também pode fazê-lo.

Então, não é uma coisa que se restringe exclusivamente ao setor público.

A consulta pública eu acho que não preciso passar, pois o nosso colega do Planejamento já falou bastante sobre os documentos que estão em consulta por mais 15 dias.

Eu queria ressaltar, então, que já existem várias normas. Existe o Common Criteria, sobre o qual vocês já devem ter ouvido falar. É o critério comum de avaliação de vulnerabilidade de equipamentos e sistemas. Por que o Brasil não adere a esse critério e simplesmente segue o que existe?

Se vocês olharem bem, verão que isso aqui é um certificado retirado do *site* da Common Criteria, dando um atestado de que o equipamento está o.k., com nível de proteção X. Mas se vocês virem quem assina...

A pessoa que foi acusada, que originou todo esse movimento de holofote em cima do que já vinha sendo feito, é o tipo de pessoa que, em determinados países, olha se o equipamento é seguro ou não. É a raposa cuidando do galinheiro. É um negócio meio...

Minha opinião pessoal: não sei se devemos fazer 100% sozinhos, mas devemos talvez ter um laboratório para nós certificarmos, usando o Common Criteria ou algo equivalente no País.

Por fim, eu coloco que a dúvida foi instaurada num escândalo, e essa dúvida não foi colocada sobre o Governo, mas sobre o setor privado. É fundamental o setor privado participar. Por isso a consulta pública, que serve para isso. A consulta pública não é lei preto no branco. Ela serve para o setor privado contribuir e trazer sugestões.

Considerando tudo isso que aconteceu, como o setor privado pode contribuir com o Governo para tornar as redes mais confiáveis, para tornar as redes mais seguras, para que o Governo possa efetivamente confiar nos sistemas de serviços e equipamentos providos para ele?

Obrigado.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Quero agradecer mais uma vez a apresentação ao Sr. José Gustavo Gontijo. Esta Comissão lhe agradece sensibilizada a contribuição a esta audiência pública.

Dando sequência aos trabalhos, eu vou passar a palavra ao Sr. Virgílio Almeida, para que faça sua apresentação. Desde já quero agradecer muito, Virgílio, a sua contribuição e participação nesta audiência pública.

Muito obrigado. Estenda o nosso agradecimento ao Ministro, por gentileza.

O SR. VIRGÍLIO AUGUSTO FERNANDES ALMEIDA - Bom dia a todas e a todos. Eu queria primeiramente agradecer à Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados o convite para participar desta Mesa. Eu queria agradecer em especial ao Deputado Bilac Pinto, autor do requerimento, em nome do qual eu cumprimento e saúdo todos os Deputados aqui presentes.

Além disso, quero me congratular com a Câmara dos Deputados por colocar na agenda de discussões o tópico de segurança da informação. Este é um tópico estratégico que o País tem que construir olhando o futuro. Hoje nós vivemos em um mundo conectado à Internet. Nós temos algo em torno de 3 bilhões de usuários, pessoas, empresas e governos.

Nós podemos falar em uma economia digital. Hoje, o Brasil digital tem o setor de Tecnologia da Informação e Comunicação, que representa algo em torno de 7% do PIB, do Produto Interno Bruto brasileiro. No futuro, isso deve crescer. A chamada economia digital cresce a taxas muito maiores do que a da economia tradicional. Por exemplo, o setor de TIC cresceu nos últimos 5 anos a uma taxa de aproximadamente 9% a 10% quando comparado a 1%, 2% ou 3% da economia tradicional.

Esse é um setor-chave para o Brasil, não só pelo tamanho que representa em termos da economia, 7% e pouco do PIB, mas também porque esse é o setor que leva a inovação aos demais setores da economia, da sociedade e do Governo também. Nós estamos falando de um setor essencial, estratégico. O Brasil tem que se preparar para o futuro. Nós não podemos chegar 10 anos a frente e dizer que não nos preparamos de maneira adequada para defender o País.

Como o meu colega do Ministério das Comunicações mostrou, ano passado houve a revelação, pelo Edward Snowden, do processo de espionagem, do monitoramento dos cidadãos e autoridades brasileiras. O que ficou claro após todas essas discussões referentes ao monitoramento pelos Estados Unidos é que o Brasil

tem que fazer o dever de casa. O Brasil tem que criar estruturas seguras. O Brasil tem que criar mecanismos para diminuir suas vulnerabilidades. É isso que todos os países fazem.

Nesse contexto do ciberespaço — espaço criado pelas redes de informação, pela Internet, que interliga as pessoas, os governos e as empresas —, o Brasil tem que criar os seus mecanismos de defesa e de minimização das vulnerabilidades.

Se nós olharmos esses mecanismos, veremos que há três eixos importantes a considerar: primeiro, a estratégia nacional de defesa, já estabelecida, que coloca o Exército como o responsável pela defesa cibernética. Mas nós temos que pensar em medidas adicionais. Temos que pensar em politicas públicas que criem mecanismos de segurança. O Decreto nº 8.135, de 2013, é um exemplo dessas politicas públicas. Nós temos que, antes de tudo, pensar em desenvolver tecnologias nacionais. O País deve ter controle sobre elas, porque sem isso o Brasil fica em uma dependência aguda de um setor estratégico em termos de defesa. Naturalmente que isso não exclui a participação e a interação do País com outros países na troca de informações e de conhecimentos científicos. O Brasil tem que ter a sua tecnologia para a defesa cibernética e para a segurança do espaço cibernético.

Se nós olharmos, nesse contexto da preparação do País, para os anos que virão, nos quais o Brasil digital vai se tornar cada vez mais presente, veremos que nós temos várias unidades e órgãos do Governo encarregados da execução dessas políticas. O Ministério da Defesa, o Gabinete de Segurança Institucional, o Ministério do Planejamento, Orçamento e Gestão e o Ministério das Comunicações são órgãos que executam as políticas que põem em prática a execução das ações de segurança e de defesa. No nosso caso, o Ministério da Ciência, Tecnologia e Inovação é responsável por fomentar o desenvolvimento de tecnologias brasileiras nesse setor.

Eu chamo a atenção para uma ação do Ministro da Ciência, Tecnologia e Inovação, Clélio Campolina, que criou, por meio do Decreto nº 8.269, de 2014, o Programa Nacional de Plataformas do Conhecimento, que associa ações de longo prazo, relativas a problemas de interesse nacional, ao desenvolvimento científico e tecnológico.

Entre essas plataformas já escolhidas estão: saúde; fármacos; vacinas; energia; agricultura; aeronáutica, com o avião verde; e uma delas é segurança e defesa cibernética.

Então nós teremos ações de médio e longo prazo visando desenvolver no País não só universidades ou governos, mas principalmente empresas. As empresas têm que se desenvolver para criarmos no mercado ferramentas, tecnologias e instrumentos para segurança e defesa cibernética. Essa é a nossa participação nesse processo como um todo.

Eu vou rapidamente apresentar alguns pontos. Mas eu queria chamar a atenção para o porquê a ciência e a tecnologia são importantes nesse setor. Quando trabalhamos com as questões de defesa e segurança cibernética, trabalhamos protegendo contra vírus, contra elementos chamados de *malware,* etc. Geralmente, esse trabalho é feito como se olhássemos no retrovisor quais foram as ameaças e os ataques do passado.

Nós estamos trabalhando em um mundo em que a evolução tecnológica é muito rápida. Principalmente, estamos trabalhando em um mundo assimétrico, no qual *hackers* — jovens rapazes e moças que têm um conhecimento tecnológico — podem ameaçar Estados e grandes empresas com um custo muito pequeno. A defesa disso é assimétrica, porque ela requer investimentos de longo prazo. Esse é um mundo novo, para o qual o Brasil tem que se preparar, dada a dimensão do seu mercado e do seu país. Rapidamente eu vou mostrar alguns pontos.

(*Segue-se exibição de imagem.*)

Nesse caso específico da discussão do Decreto nº 8.135, de 2013, nós temos dois pontos: a questão do armazenamento das informações e a questão da transmissão das informações no País. São dois os focos vigentes: armazenamento e equipamentos de *hardware* e *software*. Se nós não tivermos maneiras de garantir que esses equipamentos, *softwares* e programas tenham como criar mecanismos para verificar quais são suas vulnerabilidades... Eles hoje constituem a infraestrutura com que nós todos trabalhamos hoje. São os roteadores e os equipamentos de rede que transmitem, são os programas que controlam os *e-mails* e os acessos à base de dados. Com tudo isso, nós não temos certeza de que eles não possuem vulnerabilidades explícitas.

Vou dar um exemplo: uma empresa chinesa que recentemente cresceu muito, chamada Xiaomi, tomou rapidamente o mercado de celulares na China. Outro dia, os jornais noticiaram que o Governo indiano havia entrado com uma determinação para que os telefones da Xiaomi não fossem usados no governo, porque todas as informações que passavam por esses telefones eram transmitidas para servidores na China. Então o Governo indiano sentiu: *"Há uma brecha no sistema de segurança*".

São esses exemplos com que nós temos que trabalhar. O Brasil é uma das seis ou sete maiores economias do mundo e precisa ter uma infraestrutura tecnológica adequada a esse porte. Nós temos que investir para criamos isso no País.

O Decreto nº 8.135, de 2013, determina que esses programas e esses equipamentos sejam passíveis de auditoria no que se refere à confidencialidade, integridade, disponibilidade e autenticidade.

A Portaria nº 141, de 5 de maio de 2014, dá ao Ministério do Planejamento, Orçamento e Gestão essa atribuição. É uma portaria do MP, do Ministério das Comunicações e do Ministério da Defesa. Mas a questão é: como verificar isso? Então surge essa questão prática.

A necessidade de normas específicas. Já foram mencionadas pelo colega do Ministério do Planejamento as normas existentes, mas nós temos que trabalhar com tecnologias que possam nos permitir verificar quais são as vulnerabilidades. Isso não se faz mais só com pessoas. Nós precisamos de tecnologias sofisticadas para isso. É com esse desenvolvimento tecnológico que nós temos que trabalhar.

As contribuições que a Secretaria de Política de Informática e o Ministério da Ciência, Tecnologia e Inovação podem dar são: a participação da SEPIN nas discussões do tema; a disponibilização de pesquisadores do CTI, o Centro de Tecnologia da Informação Renato Archer, do MCTI, localizado em Campinas; a redução de parte das vulnerabilidades existentes por meio de uma ação conjunta do MCTI com o Ministério da Defesa — eu vou mostrar qual é essa ação em andamento —; uma capacidade de resposta que dependerá da definição de prioridades e maiores investimentos em recursos humanos; uma experiência adquirida na formulação e implantação de uma política pública chamada CERTICS,

para a certificação de tecnologia nacional de *software* e a implantação de um ecossistema Defesa/MCTI/Empresas e ICTs, para o desenvolvimento de tecnologias para a cibersegurança e a ciberdefesa.

Eu vou mostrar rapidamente quais são os pontos principais, as ações do MCTI que vão levar a essa plataforma do conhecimento em ciência e tecnologia na área de segurança e defesa cibernética.

A segurança está ligada à questão da nuvem. Hoje cedo o *The New York Times* publicou um artigo intitulado *Os países movem-se para as nuvens de computação: o crime também.* Então nós temos que nos preparar para que lá na frente a sociedade não se lamente: *"Olha, nós não nos preparamos da maneira adequada"*. É esse o ponto e a importância desta reunião de hoje, requerida pelo Deputado.

Próximo. Precisamos ter o domínio de tecnologias, não só de nuvens, mas também tecnologias de comunicação.

Algumas das medidas de curto prazo foram discutidas aqui, tal como o Decreto nº 8.135, de 2013, mas existem as medidas de médio e longo prazo, que são: capacitação, desenvolvimento de tecnologia no País, etc.

Os objetivos principais desse programa do MCTI são: estruturar um ambiente digital seguro. Por exemplo: o Reino Unido diz que, como estratégia de governo, quer ter um ambiente do ciberespaço o mais seguro possível para a sociedade e paras as empresas fazerem negócio. Nós precisamos olhar o Brasil com uma visão estratégica. Precisamos parar de olhar 6 meses à frente, só reagindo a um episódio. Nós temos que criar uma linha. Daí o papel e a importância de a Comissão de Ciência e Tecnologia, Comunicação e Informática trazer essa temática para a discussão.

Então nós estamos trabalhando em identificação de temas e tecnologias críticas que permitam a segurança, a rastreabilidade dessas ações no ciberespaço.

Quantas às ações de curto prazo, algumas delas já foram mencionadas aqui.

Nós estamos trabalhando com os instrumentos legais de fomento à inovação, como, por exemplo, a Lei do Bem e a Lei de Informática. O Brasil tem um conjunto de leis que permitem incentivos a vários setores. Precisamos orquestrar essas leis nesses objetivos nacionais, como, por exemplo, ter um ciberespaço seguro.

Uso do poder de compra. Nós temos uma lei de poder de compra que dá preferência a tecnologias desenvolvidas no País. Isso não exclui as empresas estrangeiras. Pelo contrário. Nós queremos que as empresas estrangeiras que estão no Brasil desenvolvam parte dessas tecnologias avançadas aqui no País e façam uso, também, do poder de compra.

Só para concluir: temos a estruturação desse núcleo de pesquisa, desenvolvimento e inovação, junto com o Ministério da Defesa, para o desenvolvimento de antivírus nacionais e também de ferramentas para defesa perimetral; temos essa estratégia colocada pelo Ministro Clélio Campolina, juntamente com a Presidente, de criar as plataformas nacionais do conhecimento científico e tecnológico — sendo que uma delas é Segurança e Defesa Cibernética —, e temos a possibilidade de usar o poder de compra para garantirmos que os equipamentos e as tecnologias compradas deem ao País uma segurança quanto àquilo que vem sendo executado.

Com isso, eu concluo a minha observação, dizendo o seguinte: queria, mais uma vez, congratular e louvar a Câmara dos Deputados por trazer este debate, que não é só em função do episódio de Edward Snowden, mas é em função do País, que tem de se preparar para uma situação em que a vida nesse ciberespaço vai ser tão crescente e importante no dia a dia, quanto é a vida no ambiente físico.

O Brasil digital é uma realidade; basta nós olharmos. As pessoas todas hoje usam a Internet. O Governo usa a Internet, a política está em cima da Internet, a economia, tudo. Então, o País tem que se preparar — como outros países estão se preparando — para essa garantia estratégica de um ciberespaço seguro.

Deputado, agradeço, mais uma vez, o convite.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Eu é que quero agradecer ao Dr. Virgílio Almeida, que representa aqui o Ministro da Ciência, Tecnologia e Inovação, a exposição.

De uma certa forma, nós estamos agora encerrando o primeiro bloco das apresentações.

Vou agradecer aos Deputados que estão aqui conosco: Jorge Bittar, Dr. Adilson Soares, Arolde de Oliveira, Oziel Oliveira — que esteve aqui, mas que já saiu —, Fábio Ramalho — que também já saiu —, Duarte Nogueira, Chico das

Verduras — que está aqui conosco também —, e a Iara Bernardi, que está tentando dar presença ali. *(Risos.)*

A tecnologia é boa quando funciona, ouviu, Deputada? *(Risos.)*

Eu vou pedir aos expositores que retornem aos seus lugares de origem — nós vamos deixar que levem as placas com vocês — e que nos aguardem porque nós vamos agora convocar o segundo bloco da nossa audiência, para que depois os Parlamentares possam, de uma certa forma, fazer perguntas e esclarecer as suas dúvidas.

Dando continuidade à nossa audiência pública, quero convidar, para tomar assento aqui conosco, o Sr. Takaharu Uchino, Diretor do Departamento de Tecnologia da Informação, do Ministério da Defesa; o Exmo. Sr. General-de-Brigada Marconi dos Reis Bezerra, Diretor-Substituto do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República; a Sra. Cristine Hoepers, Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil; e também o Sr. Rodolfo Fucher, Diretor-Adjunto da Associação Brasileira das Empresas de Software — ABES.

Mais uma vez, só relembrando: os senhores convidados têm o tempo de 10 minutos para fazer a exposição, prorrogáveis por mais 5 minutos. Fiquem à vontade se, porventura, precisarem se estender mais.

Então, dando sequência, eu quero passar a palavra ao Sr. Takaharu Uchino, para que faça a sua apresentação.

O SR. TAKAHARU UCHINO - Bom dia, Srs. Deputados e demais representantes! Minha fala vai ser bastante rápida porque não há nenhuma apresentação específica para este evento. No entanto, eu gostaria de posicionar o Ministério da Defesa como o que foi parte integrante na formulação da regulamentação da Portaria nº 141; e nós fomos convidados exatamente para trabalhar por essa portaria, em função do impacto que o Decreto nº 8.135 poderia ocasionar em cima da estrutura de comunicação militar.

Os senhores todos devem saber que o Ministério da Defesa é um Ministério civil que abrange as Forças Armadas, com sua independência administrativa. Quando se fala em rede militar, uma rede extensa, enorme, que alcança os rincões

no Brasil todo, afora o espaço aéreo, na defesa das fronteiras, enfim, existe toda uma estrutura especificamente montada que requer certa autonomia e gestão independente das restrições ou das regulamentações que foram impostas através do Decreto nº 8.135.

Eu sou Diretor de Tecnologia da Administração Central do Ministério da Defesa e, portanto, não faço parte e não tenho autoridade nem competência para discursar sobre o lado militar. Para responder pela vertente militar do Ministério da Defesa está aqui presente o Comandante Fábio Martins Raymundo da Silva, que trabalha no Comando e Controle do Estado-Maior das Forças Armadas e que, posteriormente à minha fala, pode dar uma percepção aos senhores sobre essa estrutura militar existente. Enquanto lado civil do Ministério da Defesa, nós somos um órgão setorial do SISP, e, portanto, a gente segue a todas as normas do Ministério do Planejamento e também do Gabinete da Segurança Institucional, no que se refere à política de segurança.

Falar de segurança é um assunto extremamente apaixonante. No entanto, ele é recheado de uma série de questões que foram levantadas até agora aqui por aqueles que já se pronunciaram sobre o assunto. O Dr. Virgílio citou, agora há pouco inclusive, que temos 3 bilhões de usuários da Internet no momento. Pois há pouco tempo participei de um evento, onde se discutiu muito a questão da computação em nuvens, computação distribuída, Internet das coisas, *Internet of Things,* e soube que existe inclusive uma estatística que diz que em 2020 haverá cerca de 70 bilhões de coisas conectadas à Internet.

Hoje, cada um de nós, se olharmos para nós mesmos, a gente vê que tem pelo menos três ou quatro aparelhos que nós utilizamos. Cito o nosso *notebook*, *o tablet*, o telefone celular, entre outros. Acho que a maioria dos senhores deve ter pelo menos dois celulares, e todos se conectando à Internet. Afora isso, existem na Internet sensores que vão se ligar a todas essas questões. Toda essa infraestrutura da Internet vai requerer uma percepção, uma necessidade de se ter uma infraestrutura de preparo e segurança tão alta que, em determinados *gadgets*, pode-se estar transmitindo informações, rastreando a posição de pessoas, buscando informações por meio de várias técnicas de captação de informações.

Então, essa segurança não é muito diferente daquilo que a gente tem em casa. A gente sabe quanto segura a nossa casa ou nosso apartamento é. Mas existe toda uma preocupação dentro das instituições no sentido de, vamos dizer assim, preparar a sua casa para aquilo que é possível, utilizando um conjunto de pessoas capacitadas, processos e tecnologias para diminuir a vulnerabilidade.

Outra questão que se discute muito em segurança é o que se fala como apetite pelo risco; quer dizer, a área de segurança não é uma área que define qual deve ser o nível de segurança. A segurança é um assunto que deve ser definido pela governança corporativa das instituições. São essas que têm que definir qual é o apetite de risco que estão dispostas a assumir

Evidentemente, o apetite de risco de uma instituição bancária vai ser diferente do de uma instituição que não seja tão crítica, porque segurança total todos nós sabemos que não existe. Não existe 100% de segurança. É necessário a gente conciliar o grau de segurança requerido com o grau de negócio em que a gente esteja trabalhando.

Estendendo isso a nível de país, nós dependemos sempre dessas tecnologias. Como já foi dito aqui por várias pessoas, vários representantes, o Brasil já oferece incentivos fiscais. No Ministério da Defesa, por exemplo, existe uma Secretaria de Produtos da Defesa que incentiva o fomento à indústria nacional de produtos e de defesa, concedendo inclusive incentivo fiscal para se fortalecer a indústria nacional. Outras instituições, quer dizer, outras iniciativas também propiciam exatamente essa evolução.

Gostaria de finalizar, dizendo que segurança, acima de tudo, é um estado de espírito. A gente tem que estar preparado para isso, porque, repito, segurança total não existe. A gente tem que reunir esforços de todas as maneiras, segundo as tecnologias disponíveis, para diminuir as nossas vulnerabilidades.

O SR. PRESIDENTE (Deputado Ricardo Tripoli) - Com a palavra o Capitão de Mar e Guerra Fábio Martins Raymundo da Silva para fazer o complemento da apresentação do Sr. Takaharu Uchino.

O SR. FÁBIO MARTINS RAYMUNDO SILVA - Muito obrigado, Sr. Deputado. Bom dia a todos.

Sou o Capitão de Mar e Guerra Fábio Silva, Chefe da Seção Técnica de Comando e Controle do Ministério da Defesa. Como já foi dito, participei da elaboração do Decreto nº 8.135.

O que é importante da parte de comunicações militares é o entendimento de que elas estão dentro de um sistema, devidamente colocado na portaria de regulamentação, que é o sistema militar de comando do controle.

As comunicações militares, por suas características, existem basicamente para prover o que é chamado por nós de consciência situacional de qualquer operação militar, na parte da operação que esteja acontecendo. Para isso, ela se utiliza de diversos protocolos.

No caso das comunicações de dados, de que se fala aqui, está-se falando do IP — *Internet Protocol*, que é um dos protocolos utilizados nas comunicações militares. Mas existem outros protocolos que, apesar de serem de tecnologia da informação, não estão dentro desse universo de que se fala, que é o básico do Decreto nº 8.135. São protocolos que permitem, por exemplo, ao sistema de armas de um navio repassar informações para outro sistema de armas de outro navio. São protocolos que permitem a comunicação entre computadores de sistemas de tiro, etc. Então, não fazem parte desse universo que se pretende. Mas, obviamente, na parte de consciência situacional, o IP é muito importante.

As Forças Armadas trabalham em níveis de comando: o nível estratégico, o operacional e o tático. O tático é o nível mais baixo; é o nível ali da tropa. Mas no nível operacional e no estratégico há necessidade de coordenação. Para isso são utilizadas redes de dados IP, nesse caso, para que essas informações fluam.

Entretanto, desde muito tempo, desde praticamente o início do uso da TI no País, as Forças Armadas já investem em redes privadas próprias para essa comunicação operacional, e já há muito tempo se preocupa com isso, que é já uma doutrina, é mesmo chamado de doutrina. É uma doutrina de segurança que permite que todas as informações que trafeguem por essa rede — apesar de já trafegarem em uma rede segregada, própria, com enlaces próprios — tenham um tratamento conforme seu grau de sigilo e o grau de necessidade. Então, isso já é feito normalmente. Isso já é feito nas Forças Armadas, e que, obviamente, pode ser

incrementado. E é incrementado dentro das condições e necessidades operacionais que acontecem.

Nesse sentido, o sistema tático de comando e controle abrange todos os serviços que nós utilizamos. Por exemplo, comunicação por satélite faz parte do sistema de tática de comando e controle, e tem os seus protocolos próprios, utiliza esses equipamentos e tem as suas características de segurança

Então, nesse sentido, o Sistema Militar de Comando e Controle abrange todos os serviços que nós utilizamos. A comunicação satelital faz parte do Sistema Militar de Comando e Controle, tem os seus protocolos próprios, utiliza esses equipamentos e tem as suas características de segurança preservadas dentro do processo.

Agora, existem outras tarefas que as Forças Armadas possuem e que também precisam ser levadas em conta quando trabalhamos. Por exemplo, todo o controle aéreo nacional é feito por meio dessa rede segregada, que utiliza inclusive a comunicação satelital, enlaces digitais de longa distância que têm as suas características próprias de disponibilidade e que, muitas vezes, precisam ter um tratamento diferenciado, como existem os sistemas de controle de tráfego marítimo, de tráfego naval e, futuramente — estão sendo colocados —, o SISFRON, o SISGAAZ e o SISDABRA, este último da Força Aérea, que já existe, está montado. Eles se utilizam dessa tecnologia e estão totalmente preocupados em manter a segurança da informação, em fazer com que essa ou aquela informação esteja devidamente tratada e também devidamente protegida nas comunicações.

Nesse sentido, esses foram os motivos por que, na Lei nº 8.135, em alguns pontos, foi dado tratamento diferenciado às comunicações militares.

É só isso.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Eu quero agradecer mais uma vez ao Sr. Takaharu Uchino, que é Diretor do Departamento de Tecnologia da Informação, do Ministério da Defesa, assim como ao Capitão de Mar e Guerra Fabio Martins Raymundo da Silva, que fizeram aqui, agora há pouco, a sua exposição.

Dando continuidade, vou pedir ao Sr. General de Brigada Marconi dos Reis Bezerra, que é Diretor Substituto do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da

República, que faça também sua exposição, relembrando que o senhor tem 10 minutos para fazê-la, mais 5 minutos de tempo prorrogável.

O SR. MARCONI DOS REIS BEZERRA - Exmo. Sr. Deputado Bilac Pinto, autor do requerimento em pauta, na pessoa de quem eu cumprimento os demais Parlamentares aqui presentes, os representantes dos órgãos que foram convidados e a distinta audiência, eu aqui represento o Ministro-Chefe do Gabinete de Segurança Institucional — GSI, General Elito Siqueira, e, atendendo ao que foi solicitado no Requerimento nº 337, do Deputado Bilac Pinto, e desde já agradecendo o convite que nos foi formulado, vou repassar aos senhores algumas informações relacionadas ao Plano de Ação de Políticas de Segurança da Informação do Governo Federal e alguns relacionamentos desse Plano com o Decreto nº 835 e a Portaria nº 141 que regulamentou esse decreto.

(Segue-se exibição de imagens.)

Aqui eu coloquei, para nos situarmos no contexto, onde estamos no Gabinete de Segurança Institucional. Eu quero destacar apenas alguns pontos onde, no Gabinete, são tratadas as questões de segurança da informação.

Ali em cima está uma competência diretamente atribuída ao Ministro pela lei de acesso. Ele exerce a função de Autoridade Nacional de Segurança — aquele ANS ali em cima — para fins de tratados e acordos internacionais com outros países que envolvam o tratamento da informação classificada e o credenciamento de pessoas no território nacional que precisem ter acesso a informação classificada.

Então, o nosso Ministro exerce essa função de Autoridade Nacional de Segurança.

Ele também é o Secretário-Executivo do Conselho de Defesa Nacional, e é com esse chapéu que ele assina as normas, que eu vou comentar lá na frente, aprovadas pelo Comitê Gestor de Segurança da Informação e Comunicações. O Ministro assina, então, como Secretário-Executivo do Conselho de Defesa Nacional.

Ele também é o Presidente da Câmara de Relações Exteriores e Defesa Nacional — CREDEN, do Poder Executivo, que também tem uma competência de segurança da informação.

O nosso Ministro é assessorado pelo Comitê Gestor de Segurança da Informação para essa assessoria, tanto ao CDN quanto ao CREDEN, nas questões de segurança da informação.

E ali vemos o nosso Departamento de Segurança da Informação e Comunicações, ligado diretamente à Secretaria-Executiva.

Aqui, uma estrutura um pouco mais detalhada, onde todo o Departamento trata, direta ou indiretamente, de segurança da informação, que é o nosso foco principal.

Temos um vínculo técnico com o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações — CEPESC, para fins de pesquisa e desenvolvimento de recursos criptográficos, algoritmos de Estado, como temos um vínculo técnico também com o Comitê Gestor de Segurança da Informação.

Vou comentar alguns detalhes mais à frente sobre o Comitê Gestor de Segurança. Ele é coordenado pelo Diretor desse Departamento. Então, o Diretor desse Departamento coordena as reuniões do Comitê Gestor de Segurança da Informação.

Aqui estão apenas alguns *flashes* sobre as reuniões desse Comitê, que são realizadas mensalmente no Anexo I do Palácio do Planalto. Às segundas e quartas-feiras de todos os meses, religiosamente, essas reuniões são realizadas com a presença de 17 Ministérios, que são os titulares e os suplentes designados, mais uma quantidade de cerca de 70 órgãos colaboradores, que têm participado conosco da elaboração dessas normas.

Aqui eu coloquei alguma legislação relacionada ao tema que nós estamos abordando aqui, que é a segurança da informação. A Lei nº 12.462/11 definiu a estrutura do GSI e ali, no seu art. 6º... Essa é uma lei de 2011 que vem sendo atualizada desde a criação do GSI, em 2003. Essa competência vem sendo atualizada com vistas a coordenar as atividades de inteligência federal que o GSI realiza por intermédio da ABIN e as de segurança da informação, realizadas por intermédio do Departamento de Segurança da Informação.

O Decreto nº 8.100, de 2013, que é o último que atualiza a estrutura de governo, também atualiza as competências do GSI e do DSIC. Estão ali elencadas todas as atividades que nós realizamos no dia a dia no Departamento.

Aqui o Decreto nº 3.505, de 2000, já foi citado aqui pelo Ministério do Planejamento. Na ementa do decreto já consta lá que ele institui a Política de Segurança da Informação nos órgãos da administração pública federal e institui também o Comitê Gestor de Segurança da Informação, com atribuição de assessorar a Secretaria Executiva do Conselho de Defesa Nacional na consecução das diretrizes da política de segurança da informação dos órgãos da APF.

Então, isso foi criado lá em 2000. O GSI veio a ser criado depois de 2003; e, posteriormente, foi criado o DSIC, em 2006. A partir daí, as normas começaram a ser elaboradas por todos os órgãos que compõem o Comitê.

Aqui, meus senhores, começamos a falar a respeito do Plano de Ação, do que nós temos feito em termos de política de segurança da informação no âmbito do Governo Federal.

Ali eu coloquei uma ação bastante desenvolvida no nosso Departamento, que são os normativos, que já foram bastante citados aqui e que estão publicados na Internet. E tem sido cobrado pelo TCU o cumprimento de todos eles.

Ali a primeira publicação: a Instrução Normativa nº 1, que teve como tema principal a gestão e o planejamento de segurança da informação no âmbito da APF. Complementares a essa normativa, nós já temos 21 normativas em vigor. A primeira normativa é de 2008, e as complementares datam de 2008 a 2014. Já foram 21, as duas primeiras publicadas no mesmo ano, em 2008.

Temos também, em termos de normativos para a administração pública, do *Guia de Referência de Segurança das Infraestruturas Críticas da Informação*, publicado em 2010, como também o *Livro Verde: Segurança Cibernética no Brasil*, também publicado em 2010.

Os senhores reparem que todas essas iniciativas são anteriores à questão do Snowden e de uma série de outras questões que vieram posteriormente. O DSIC já vem pensando nessa questão de segurança desde a sua criação.

Aqui um *flash* geral, para os senhores terem ideia, dos temas que são abordados nessas normativas. Esses são temas todos estratégicos, decididos no âmbito do Comitê Gestor. Nós teremos, na próxima semana, a última reunião do ano do Comitê Gestor de Segurança, ocasião em que faremos um balanço das normas que foram aprovadas neste ano e de alguns temas que foram levantados e cujos

estudos prosseguirão no ano que vem. E já vamos começar a levantar temas agora, neste mês, sugeridos pelos integrantes do Comitê, temas a serem normatizados no próximo ano.

Ali, as outras restantes, de 12 a 21. Todas as Normas, cada uma, abordam um tema específico e estratégico normatizada pelo Gabinete.

Senhores, falando em normas, é inevitável falarmos na cobrança das normas, porque não adianta fazermos uma norma que não seja cumprida. Essa é uma preocupação constante do Comitê, quando produz uma norma: produzir algo que não será cumprido. As normas são muito bem elaboradas, discutidas amplamente no âmbito do Comitê, e o TCU tem colaborado bastante nessa questão da cobrança de norma. O Comitê aprova, o Ministro assina, publicamos no *Diário Oficial*, e o Tribunal de Contas da União, em todas as suas auditorias, tem usado essas normas como referência para a cobrança das questões de segurança digital de todos os órgãos da administração pública federal.

Cito ali apenas alguns. Existem vários acórdãos do TCU que levantam essa questão do cumprimento das normas do GSI. Coloco ali o Acórdão nº 1.233, do TCU, de 2012. Naquela ocasião, ele dizia que a adoção dos normativos do DSIC e do GSI não são facultativos, mas, sim, obrigação da alta administração. Naquela oportunidade, em 2012, o nosso Ministro deu um aviso a todos os Ministros do Poder Executivo, passando essa recomendação que o TCU nos deu. Agora, no corrente ano, o TCU fez um balanço acerca do que era em 2012 e como está agora, em 2014. O TCU concluiu que a situação melhorou muito. A POSIC era dotada por 26%, e hoje está dotada por 54% dos órgãos. Então, em vários aspectos de segurança os órgãos melhoraram. Porém, no Acórdão nº 3.117, ali embaixo, o TCU conclui que a situação não está no ideal ainda, que há muito o que fazer, há muito o que evoluir em termos de segurança de dados da administração pública.

Destaco também o Acórdão nº 3.051, também de 2.014, que recomenda ao TCI alertar os órgãos da administração pública federal que a elaboração periódica de planejamento de ações é obrigação expressa na Norma Complementar nº 2. Aqui a de nº 1, aquela publicada em 2008, em que o TCU recomenda a toda a administração pública que aquela ordem é expressa na norma publicada em 2008.

Em outro local também do Acórdão nº 3.051, o próprio TCU colocou no seu Relatório Final um comentário de que, no âmbito do Poder Executivo, o GSI tem desempenhado papel preponderante na regulamentação do setor e na promoção de ações de capacitação a que temos realizado.

Aqui, falando em capacitação, temos desenvolvido algumas ações no âmbito de toda a administração pública federal. Temos realizado curso de especialização e gestão DCIC, que este ano, na sua quarta edição, é um curso exclusivo para a administração pública federal, para formarmos Gestores de Segurança da Informação, o que é feito em parceria com a UNB. Aliás, uma formatura já está marcada. Essa última edição está terminando agora, ao final do ano. Com essa formatura, teremos em torno de 330 especialistas já formados, nessa parceria do GSI com a Universidade de Brasília.

Realizamos nove oficinas técnicas sobre temas específicos das normas complementares. Divulgamos na Internet essas oficinas. Os órgãos se inscrevem e realizamos ali, todos os meses, também oficinas, que já atenderam a um público de 429 servidores. Essa iniciativa começou há um pouco mais de 1 ano e já atendemos a 85 órgãos da administração pública em todo o Brasil; órgãos de todos os Estados têm comparecido aqui, em Brasília, para participar dessas oficinas. Já realizamos sete colóquios técnicos.

Aqui, temas mais ligados ao tratamento de incidente de rede. Já atendemos também a 600 servidores, e cerca de 75 órgãos já estiveram conosco discutindo essas questões de tratamento de incidente de rede.

Em 2014 surge uma outra Coordenação nossa dentro do Departamento, que é o CTIR Gov, que processou cerca de 16 mil notificações incidentes de segurança em redes do Governo em contato com mais de 200 equipes de tratamento de incidentes de redes em toda a administração pública federal. E esse trabalho é feito visando mitigar riscos de incidentes de segurança e combater as vulnerabilidades das grandes redes corporativas da administração pública federal.

Outra ação que nós temos realizado em prol da administração pública é o credenciamento de segurança. Ele foi instituído pela Lei de Acesso à Informação e, atendendo ao que foi previsto na lei, foram publicadas pelo GSI duas Instruções Normativas, as de nºs 02 e 03, e uma complementar à de nº 02, falando dessas

questões de credenciamento para o tratamento da informação classificada, montando toda a estrutura de credenciamento — órgãos nível 1 seriam os Ministérios; nível 2... etc. Toda essa estrutura está definida nessa Instrução Normativa, com a sua complementar. E a Instrução Normativa nº 03, também cumprindo determinação da Lei de Acesso, definiu os parâmetros e os padrões mínimos dos recursos criptográficos baseados em algoritmo de Estado para a criptografia da informação classificada.

No tema criptografia nós contamos com alguns pesquisadores, cientistas e estudiosos da ABIN, que já vêm estudando esse assunto há em torno de 30 anos. Temos uma equipe bastante reforçada, da qual já participaram mais de 20 servidores, e atualmente são muitos os pesquisadores que vêm estudando essa questão da criptografia com algoritmo de Estado.

Ainda falando do credenciamento de segurança, o Núcleo de Segurança e Credenciamento, uma das coordenações do DSIC, credenciou gestores de segurança e credenciamento no escopo do processo de habilitação dos órgãos de registro, que foram definidos pela Lei de Acesso, e já emitiu credenciais de segurança para pessoas que têm necessidade de tratar a informação classificada. Esse trabalho começou com a Lei de Acesso, em 2011, e vem sendo incrementado agora.

Bom, senhores, já chegando ao final, faço agora o vínculo do Decreto nº 8.135, de 2013, com a Portaria Interministerial nº 141, de 2014. Esse plano de ação que nós temos feito, as ações que temos desenvolvido em termos de capacitação, normas, etc., que repercussão têm Decreto nº 8.135 e na Portaria Interministerial nº 141?

Embora o GSI não tenha assinado esses instrumentos, ele foi citado nos arts. 5º, 9º e 12 da portaria que regulamentou o decreto, onde constam disposições relativas ao cumprimento de todo o arcabouço normativo do DSIC. Aqui eu destaco apenas os pontos em que foi citado o GSI na Portaria.

No art. 5º, § 1º, consta o seguinte:

"Art. 5º. .....

§ 1º A contratação dos serviços de que trata o caput será efetuada em conformidade com as normas e

> *os procedimentos estabelecidos pelo órgão gerenciador, observadas as disposições relativas à segurança da informação e comunicações fixadas pelo Gabinete de Segurança Institucional da Presidência da República."*

O art. 9º diz que o termo de referência ou projeto e o contrato deverão conter obrigações de comprovação da disponibilidade, integridade, confidencialidade e autenticidade. São termos que já foram até citados aqui e aparecem em várias instruções normativas. Eles começaram a ser citados na Instrução Normativa nº 01, primeiro instrumento normativo do GSI, do Comitê Gestor, publicado em 2008.

Outra obrigação que ele impõe é a apresentação da política de segurança de dados e o detalhamento das ações do DSIC. São focos das Normas Complementares nºs 02 e 03, também já citadas.

O art. 12 dessa mesma portaria diz que:

> *"Sem prejuízo dos requisitos previstos nos arts. 8º e 9º, os serviços de tecnologia da informação de que trata esta Portaria devem adotar os seguintes critérios mínimos de segurança da informação e comunicações (...)"*

Ele cita o uso de criptografia — como já vimos, nós temos uma norma específica que trata disso, que é a Norma Complementar nº 09, que foi atualizada recentemente, após a Lei de Acesso — e o uso de ferramenta de controle de acesso, a Norma Complementar nº 07, também revisada este ano, em 2014, onde já se incluem, inclusive, as questões de controle de acesso biométrico, como impressão digital, identificação de íris, etc. Uma série de recomendações atualizadas é passada nessa norma de controle de acesso.

Bom, senhores, dentro do tempo previsto, eu espero ter passado aos senhores algumas informações que fazem esse vínculo do plano de ação que o GSI tem realizado com o Decreto nº 8.135 e a Portaria nº 141.

É um trabalho nosso que ainda não é conclusivo. Temos muito a fazer. Como o próprio TCU vem dizendo, o GSI tem desempenhado seu papel normativo, etc., mas ainda há muito a fazer. O próprio atendimento da administração pública ele conclui que melhorou, mas ainda não chegou ao ideal. As normas estão publicadas, novas normas, como eu já disse, virão no próximo ano, outros temas estão sendo

levantados por órgãos públicos e privados, que nós estamos sugerindo, e o Comitê vai estudar esses novos temas para serem debatidos.

Muito obrigado a todos.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Eu quero agradecer ao General de Brigada Marconi dos Reis Bezerra a exposição.

Ao mesmo tempo, registro que esta Comissão acaba de ser informada de que, pelo Regimento da Casa, quando se inicia a Ordem do Dia nas sessões do Congresso Nacional, da Câmara ou do Senado, nós temos que, infelizmente, encerrar os nossos trabalhos.

Eu quero pedir desculpas ao Dr. Rodolfo Fucher, da ABES, que tão gentilmente aceitou o nosso convite e não teve a oportunidade de fazer a sua exposição, assim como à Sra. Cristine Hoepers. Ela esteve aqui conosco, se preparou para fazer a sua exposição, e não poderá fazê-la.

Quero agradecer muito a presença de todos que aceitaram o convite para participar desta audiência pública, cujo tema é extremamente relevante para a Câmara dos Deputados, principalmente para a Comissão de Ciência e Tecnologia, Comunicação e Informática, na pessoa do Sr. José Ney de Oliveira Lima; do Sr. José Gustavo Sampaio Gontijo; do Sr. Virgílio Almeida, nosso conterrâneo, que veio aqui representar o Ministro de Ciência e Tecnologia; do Sr. Takaharu Uchino; e do General Marconi dos Reis Bezerra.

Lamentavelmente, como disse, a Sra. Cristine Hoepers e o Sr. Rodolfo Fucher não puderam fazer as suas apresentações. Quero, então, pedir-lhes desculpas, pois, pelo Regimento da Casa, infelizmente, nós não podemos dar sequência à nossa audiência pública.

Com a palavra o ilustre Deputado Jorge Bittar.

O SR. DEPUTADO JORGE BITTAR - Sr. Presidente, senhores convidados, eu quero falar da importância do tema e da qualidade desta audiência pública, que consegue ter um painel bastante diversificado sobre assunto extremamente importante e estratégico para o nosso País.

Mas pergunto, Sr. Presidente, uma vez que faltam apenas dois expositores desta Mesa, se nós não poderíamos ouvi-los, até para aproveitar a viagem, ainda que a exposição seja feita de forma sintética. Mesmo transgredindo um pouquinho o

Regimento, poderíamos ouvir os nossos expositores. Ainda não começou a votação no plenário. Quando começar, vamos lá rapidamente. Nós já marcamos presença.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Eu pediria então à Myriam, nossa Secretária, que, assim que começar a votação no plenário, nos avise, e aí, sim, nós vamos encerrar os trabalhos. De certa forma, nós todos aqui...

O SR. DEPUTADO JORGE BITTAR - Como nós não estamos votando aqui, esta é uma audiência pública...

O SR. PRESIDENTE (Deputado Bilac Pinto) - ...estamos correndo um risco coletivo, em função do Regimento Interno da Casa. Mas vamos correr o risco, porque eu acho que vale a pena.

O SR. DEPUTADO JORGE BITTAR - Aceitaremos o puxão de orelha.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Vamos receber o puxão de orelha.

Dando continuidade à audiência, vou passar a palavra à Sra. Cristine Hoepers, pedindo-lhe que, por gentileza, seja sucinta na sua apresentação, para que o Sr. Rodolfo Fucher também possa fazer a sua.

A SRA. CRISTINE HOEPERS - Inicialmente, muito obrigada a todos pelo convite. Agradeço aos Srs. Deputados, em nome do Dr. Demi Getschko, que não pôde estar aqui hoje. Eu vou tentar ser mais sucinta ainda do que já pretendia.

O Comitê Gestor da Internet é um órgão multissetorial. Aliás, não é um órgão, é um comitê multissetorial formado por Governo, sociedade civil e empresas. Tem representantes de todos os órgãos do Governo — alguns estão aqui —, da indústria do *software* e de outras áreas.

Uma das áreas em que se tem investido muito, na estratégia do Comitê Gestor, que vai completar 20 anos em 2015, é a de segurança e resiliência da Internet e de infraestrutura de Internet no Brasil. O CERT.br, um dos serviços prestados pelo Núcleo de Informação e Coordenação do Ponto BR, que implementa as diretrizes do Comitê Gestor, implementa essas diretrizes na área de segurança da informação, com o auxílio de outras áreas que implementam também partes da segurança, como a parte de troca de tráfego no Brasil. Temos 26 pontos para interconexão e para maior qualidade de transmissão, para manter esse tráfego dentro do Brasil.

Hoje nós temos trabalho em várias áreas, de treinamento, de formação de pessoal, e especificamente temos visto quais são os maiores problemas no País como um todo. Eu acho que aqui foi discutido muito tudo que se tem tentado fazer em termos de medidas de segurança, que, na verdade, são as maneiras de tentar lidar com problemas mais profundos.

Eu acho que um dos problemas que têm maior impacto está na área de desenvolvimento de *software* mesmo. Até fico muito contente que tenhamos representantes aqui da indústria do *software*, porque a maior parte dos problemas que temos se devem a *softwares* desenvolvidos sem se pensar em segurança, sem se levantar risco, sem se levantar o ambiente em que eles estão sendo implantados. E o maior problema de todos é que hoje nós não temos uma força de trabalho treinada para lidar com isso.

Hoje as nossas universidades não preparam os desenvolvedores de *software* para lidar com segurança. Ainda na sexta-feira eu ouvi uma palestra de um estudante recém-formado que entrou no mestrado. Ele disse: *"Ensinaram-me cem maneiras de fazer um algoritmo para ordenar dados, mas ninguém nunca me falou que eu poderia inserir um problema de segurança no software quando o estivesse desenvolvendo."*

Esse é um depoimento muito interessante de quem está sendo introduzido. E eu acho que isso é uma coisa a se considerar. Por mais que se tenha *software* aberto ou desenvolvido pelo Governo, ou programas, ou auditorias, ainda se tem um problema mais de raiz: os *softwares* que estão sendo desenvolvidos são vulneráveis.

Hoje foram levantados aqui vários casos clássicos, como, por exemplo, o da usina do Irã, que no fundo era um programa que explorava a vulnerabilidade de *software.* Quer dizer, um *software*, mesmo sendo desenvolvido para um setor crítico, tinha um problema de segurança, que foi explorado. Hoje a complexidade do *software* é muito grande. Por mais que já se pensasse em desenvolver com segurança, é muito difícil pensar em todas as áreas.

Então, eu acho muito importante pensar que só o fato de ser um *software* aberto não quer dizer que ele vai ser seguro. Acho que um dos exemplos mais emblemáticos foi o deste ano, quando tivemos o Rabbit, que foi uma vulnerabilidade

que saiu na TV, no jornal, todo o mundo falou a respeito. Era um *software* aberto, havia gente olhando, mas ele é tão complexo que não se conseguia ver os problemas que estavam nele.

Eu acho que é importante pensar, então, que precisamos ter, acima de tudo, mais preocupação com a formação dos nossos profissionais, de maneira geral, o que envolve, acho, não só quem está trabalhando no Governo, mas também quem vai estar trabalhando nas empresas que vão fornecer *software*, quem está criando a nossa infraestrutura de Internet. Nós temos muitas organizações aqui trabalhando em várias áreas. Claro que no curto prazo precisamos ter todas as medidas de segurança, mas é exatamente pela complexidade do sistema, pelo fato de que não estamos preparados para desenvolver... — a sociedade mundial, não só a sociedade brasileira, porque esse é um problema do mundo inteiro.

E precisamos pensar que a Internet é global. Não adianta pensarmos em criar um protocolo diferente ou uma rede separada das outras. O que precisaríamos é fazer do Brasil, mesmo, um ator mais forte na Internet mundial, um ator que influenciasse os protocolos mundiais. Hoje o Comitê Gestor da Internet está ajudando nisso, está fomentando, dando bolsas para que as pessoas participem das reuniões que definem protocolos. Nós abrimos um escritório do W3C, que define os padrões da *web* no Brasil. Quer dizer, devemos pensar que nós precisamos ser influenciadores e que, se a nossa indústria de *software* estiver na frente, do ponto de vista de desenvolvimento seguro, aí sim, vamos ter uma ponta de competição global nessa área, não só mais segurança dentro do próprio Brasil.

Eu poderia ter falado de outras coisas, mas quis focar aqui pontos que acho que não tinham sido lembrados antes.

Muito obrigada.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Eu quero agradecer à Sra. Cristine Hoepers por sua apresentação e, principalmente, pela brevidade com que se pronunciou.

Dando sequência aos trabalhos, para que possamos dar oportunidade a todos os nossos convidados de se manifestarem, uma vez que a sessão do Congresso já está em andamento, passo a palavra ao Sr. Rodolfo Fucher para, em nome da ABES, fazer a sua exposição.

O SR. RODOLFO FUCHER - Bom, eu quero, inicialmente, agradecer o convite e a oportunidade de discutir esse tema extremamente importante. Muito obrigado, Deputado Bilac Pinto.

Eu iria fazer uma pequena apresentação sobre a ABES, mas vou pular essa parte. Em resumo, a ABES — Associação Brasileira das Empresas de Software tem hoje tem mais de 1.500 associados no Brasil, 86% pequenas e médias empresas; 57% desses associados faturam menos de 1 milhão de reais por ano. Então, estou aqui representando empresas pequenas.

Realmente, a minha fala é um complemento ao que a Cristine Hoepers acabou de comentar. A fala dela antes da minha ajudou bastante a reduzir a minha exposição e me ajudou a ser muito mais preciso.

Quando falamos em segurança, ela é um aspecto extremamente global, ela não é um aspecto pequeno, não se trata só de as pessoas se preocuparem com código fonte ou com criptografia. Ela vai desde a transmissão, o manuseio das informações, até a experiência e a qualificação do usuário. Hoje um funcionário que tem acesso a um *e-mail* que já vem com aquele código malicioso chamado *phishing* pode derrubar toda a segurança de um sistema. Então é um assunto muito complexo e, como já foi dito aqui, é um assunto dinâmico, não é estático.

A nossa preocupação é que exista realmente um diálogo aberto com a indústria, para buscar uma solução. Como o Secretário Virgílio comentou, a busca de fomentar a indústria local, de desenvolver soluções para atender a essa necessidade, toda essa discussão em busca da implementação de padrões, procedimentos, seja *Common Criteria*, seja não *Common Criteria*, é muito importante. Realmente se faz necessária uma discussão ampla com a indústria, porque é a indústria que vai participar e investir nessas soluções. Se não existe uma segurança por parte da indústria de qual é a direção que o Governo pretende tomar, a indústria não irá investir nessa solução. Então, é muito importante um diálogo aberto.

Ney já comentou aqui, e estivemos diversas vezes conversando com ele e com a Secretária, mas sempre foi uma ação muito mais de o setor levar algumas propostas, como foi a *Common Criteria*. Nunca houve um diálogo, uma discussão mais aprofundada de quais são as intenções. Existe uma série de documentos em

consulta pública, o que realmente é louvável, mas o tempo disponível para a indústria analisar toda essa documentação não é razoável.

Por isso a indústria vem solicitando cada vez mais que se abra um tempo razoável para que isso seja debatido; não só debatido, mas que também ocorra uma audiência pública. Ou seja, que o Governo possa vir falar à indústria e à sociedade em geral sobre os documentos propostos, qual a sua estratégia, quais são as suas políticas. Até o que foi comentado rapidamente pelo representante do MiniCom José Gontijo, que eu achei muito interessante, quando citou o ponto do *Common Criteria*. Aquilo é real? Aquilo aconteceu em algum país? Quem assinou aquele documento? Como acontece isso em outros documentos? São mais de 20 países que participam da *Common Criteria*. Ou seja, tem que haver alguma segurança lá.

Houve algum caso em que algum país o aceitou? O próprio Secretário responsável pela defesa assinou aquele documento? Ele é válido ou não? Esses são os pontos que a indústria gostaria de discutir abertamente para entender do Governo a proposta, as razões dessa proposta e como a indústria pode, de forma efetiva, participar da solução, porque é uma solução muito complexa, não é fácil.

Outro ponto importante: deve-se acessar apenas o código fonte ou pegar um código fonte instalado para a administração pública ter segurança de que aquilo que esteja rodando lá é o mesmo código fonte? Isso é praticamente inviável, porque o *software* hoje sofre atualizações a cada minuto, a cada instante. Então, um *software* estático rodando em algum lugar está totalmente vulnerável. Essa não é uma solução adequada para o mercado; seja essa solução desenvolvida pelo Governo, seja desenvolvida pela iniciativa privada.

Existem diversos pontos que estão sob consulta pública que precisam e necessitam de um diálogo mais aberto. Até iria comentar ações que existem em outros lugares do mundo, mas eu vou resumir a minha fala ao pedido da indústria: que passemos a debater isso de uma forma muito mais ampla e não numa mera consulta pública. Nós achamos que a consulta pública não dá a importância devida ao tema e não permite que a indústria realmente o debata, entenda e consiga propor uma solução em consenso para a sociedade em geral.

Muito obrigado.

O SR. PRESIDENTE (Deputado Bilac Pinto) - Eu quero agradecer ao Sr. Rodolfo Fucher pela sua apresentação e também pelo tempo em que a fez, o que nos ajudou muito.

Como já estamos com a Ordem do Dia iniciada, eu quero agradecer muito a presença dos Deputados, do Deputado Dr. Adilson, do Deputado Arolde de Oliveira, do Deputado Jorge Bittar e da Deputada Iara Bernardi.

Quero mais uma vez reiterar os meus agradecimentos a todos os expositores que aceitaram nosso convite. Com certeza, vocês deram uma grande contribuição a esta Casa para que esse tema possa ser posto e discutido pelo Poder Legislativo, pelo Poder Executivo e pela sociedade brasileira com muita propriedade e assertividade.

Eu quero agradecer mais uma vez ao Sr. José Ney de Oliveira Lima; ao Sr. José Gustavo Sampaio Gontijo; ao Sr. Virgílio Almeida; ao Sr. Takaharu Uchino; ao General Marconi dos Reis Bezerra; à Sra. Cristine Hoepers; e ao Sr. Rodolfo Fucher por atenderem ao nosso convite.

Agradeço mais uma vez aos Parlamentares pela presença.

Quero encerrar os nossos trabalhos agradecendo a cada um dos presentes, em especial a cada um dos senhores palestrantes, que deram uma grande contribuição a esta audiência pública.

Muito obrigado.

Declaro encerrada a sessão.