SENADO FEDERAL
SECRETARIA-GERAL DA MESA
SECRETARIA DE REGISTRO E REDAÇÃO PARLAMENTAR

REUNIÃO
26/09/2019 - 52ª - Comissão de Relações Exteriores e Defesa Nacional

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Invocando a proteção de Deus, declaro aberta a 52ª Reunião, Extraordinária, da Comissão de Relações Exteriores e Defesa Nacional da Primeira Sessão Legislativa da 56ª Legislatura do Senado da República.

Abreviando o início dos nossos trabalhos, eu solicito ao Sr. Secretário que já conduza, para integrarem a Mesa, os quatro participantes da 1ª rodada da nossa Reunião.

A presente Audiência Pública tem por objetivo debater o Programa de Defesa Cibernética, em atendimento ao Requerimento nº 24, de 2019-CRE, conforme os temas do item 5 do cronograma do Plano de Trabalho de Avaliação de Políticas Públicas:

I - Planejamento estratégico do setor cibernético;

II - Avaliação do planejamento e da execução orçamentária relacionadas ao setor cibernético;

III - Necessidades e cenários orçamentários relacionados ao setor cibernético; IV - Debate sobre a implementação das medidas definidas em 2014 e as frentes de atuação que se delineiam a partir dos resultados já verificados;

V - Apontamento das ameaças e as atualizações do cenário do ambiente cibernético.

Participam como palestrantes e debatedores o Sr. Marcelo Buz, Diretor-Presidente do Instituto Nacional de Tecnologia da Informação; o Sr. Fabio Reis Côrtes, já presente aqui à mesa, Gerente de Arquitetura e Segurança de Tecnologia da Informação do Operador Nacional do Sistema Elétrico, o Sr. Marcos Allemand Lopes, também já à mesa, Gerente do Departamento de Gestão da Segurança da Informação e da Continuidade de Negócios do Serviço Federal de Processamento de Dados (Serpro); o Sr. Ricardo Felipe Custódio, nosso coestaduano, Professor-Supervisor de Laboratório em Segurança da Computação da Universidade Federal de Santa Catarina, nosso LabSEC/UFSC. São os integrantes da primeira Mesa composta.

Igualmente participarão Sra. Cristine Hoepers, que será convidada para a segunda Mesa, Gerente Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (Cert.br); o Sr. Márcio da Silva Nunes, Vice-Presidente da Associação Nacional de Certificação Digital; o Sr. Ilton Duccini, Diretor de Segurança Digital na Empresa Telefônica Brasil e professor da Universidade Estadual de Campinas - Unicamp; o Sr. Eduardo Bergo, Diretor Setorial da Comissão Executiva de Segurança Cibernética da Febraban junto ao Banco do Brasil, os quais eu gostaria de cumprimentar e convidar para, esses últimos, fazerem parte da Mesa na segunda rodada.

Desejo, em primeiro lugar, agradecer a presença de todos os senhores e registrar com grande satisfação a presença do ilustre General de Divisão, Gen. Guido Amin Naves, Comandante de Defesa Cibernética, que é um dos padrinhos deste nosso programa; o General de Brigada Ivan de Sousa Corrêa Filho, Chefe do Centro de Defesa Cibernética do Comando de Defesa Cibernética; o Brigadeiro do Ar Marco Aurélio Martins Gabriel, Chefe do Departamento de Estratégia do Comando de Defesa Cibernética; o Contra-Almirante Marcio Tadeu Francisco das Neves, Chefe do Estado-Maior Conjunto do Comando de Defesa Cibernética; e os Srs. Cels. Edson Ribeiro dos Santos Junior, André Luís Nogueira Terra e Antonio Rocca de Andrade.

Esta audiência pública é realizada em caráter interativo com transmissão pelos canais de comunicação do Senado Federal. A população pode participar enviando observações e perguntas aos palestrantes por meio da internet, do Portal e-Cidadania, no endereço www.12.senado.leg.br/ecidadania.

A participação dos internautas é de extrema valia para os nossos trabalhos.

Como nós temos oito debatedores previstos, número superior aos assentos, já foi disponibilizado para o primeiro grupo os que integram a primeira Mesa que eu já mencionei.

Pela ordem estabelecida, o primeiro a se manifestar será o Sr. Fabio Reis Cortes.

Eu desejo esclarecer aos senhores palestrantes que será concedida a palavra por 15 minutos a cada um, com possibilidade de prorrogação para a conclusão de suas exposições. Em seguida, abriremos a fase de interpelações aos Senadores e demais inscritos, incluindo, pelo menos em parte, o que nós tivermos de participação através dos meios de comunicação.

Para dar início à audiência pública, eu concedo então a palavra ao Sr. Fabio Reis Cortes, Gerente de Arquitetura e Segurança de Tecnologia da Informação do ONS.

O SR. FABIO REIS CÔRTES (Para exposição de convidado.) - Bom dia, Senador Esperidião Amin; bom dia, senhoras e senhores. Primeiramente eu gostaria de agradecer o convite, feito através do Comando de Defesa Cibernética, em nome do Gen. Amin, para contribuir com essa audiência pública e trazer para discussão um pouco da visão de uma empresa, uma visão empresarial sobre o tema.

Então, apenas para relembrar a importância e relevância do tema, no início de setembro, o regulador americano do setor elétrico americano divulgou um reporte detalhando algumas informações sobre um incidente cibernético que ocorreu em algumas instalações, em algumas salas de controle de empresas do setor elétrico norte-americano, em que alguns equipamentos de segurança, *firewalls* foram afetados por um ataque, que explorou uma vulnerabilidade desses equipamentos. Isso não gerou nenhum impacto no suprimento de energia elétrica, mas afetou o recebimento de informações e aquisição de dados pelas salas de controle, momentaneamente. Relembrando sempre que esse é um assunto presente e que pode afetar severamente as infraestruturas críticas dos nossos países.

Bom, especificamente sobre segurança cibernética, eu gostaria de relembrar os nossos grandes desafios que passam sempre por prevenir, detectar e responder. Esses três pilares fazem parte das nossas iniciativas diárias de tratamento do tema e de proteção de nossas empresas: evitar que ameaças comprometam a operação dos nossos negócios; monitorar proativamente vulnerabilidades e ameaças para identificar invasões; e, uma vez identificadas invasões - ninguém está livre de ser atacado, de tentativas de invasão -, responder imediata e efetivamente a esses ataques.

Aqui eu trago um conceito com que nós, no setor elétrico, principalmente com pares do ONS, operadores de sistemas elétricos no mundo, temos trabalhado, principalmente este ano, que é o conceito de resiliência cibernética. Tomando emprestado lá da minha formação de engenharia o conceito de resiliência de materiais e considerando os três desafios de que eu falei há pouco, nós entendemos que essa resiliência passa por ser a capacidade de antecipar, preparar, responder e adaptar-se a tudo, desde pequenos eventos do dia a dia a incidentes mais severos, mudanças abruptas ou incrementais, devido, especificamente, a ataques cibernéticos ou eventos cibernéticos.

E nunca é demais lembrar o nosso foco de atuação. Historicamente, investimos sempre muito em tecnologia: em equipamentos, em *softwares*, sistemas, como detectar e como bloquear ameaças e invasões. Mas a gente não pode se esquecer nunca dos nossos processos e de, talvez, um dos elos mais importantes nessa corrente, que são as pessoas, o ser humano, que não necessariamente está acostumado a esse ambiente, não necessariamente está aculturado com o tema e, muitas vezes, nem sabe que está tomando uma ação que possa fragilizar a operação do negócio da sua empresa ou do País.

E, pensando sempre nos três desafios - de prevenir, responder e detectar, no foco de atuação sobre pessoas, tecnologia e processos -, a nossa atuação passa por quatro conjuntos de iniciativas: o primeiro, de gestão interna das nossas empresas; o segundo, com um foco muito importante em pessoas e processos, é a conscientização sobre o tema e como agir nesse ambiente conectado e, naturalmente, onerável; e o terceiro, evolução contínua: não adianta fazer uma análise estática, traçar planos de evolução, e não voltar a esse plano, não revisitar esse plano continuamente, porque as ameaças mudam, as tecnologias mudam, os *hackers* evoluem, o dia a dia continua, e nós precisamos continuamente revisitar nossos processos, nossas tecnologias e como devemos atuar; e um quarto, talvez dos mais relevantes de todos, a colaboração: quanto mais colaborarmos, mais teremos chances de, juntos, atuarmos na prevenção, na detecção e no tratamento desses incidentes; sozinhos, temos limites de atuação, mas, dentro dos nossos setores ou dentro do nosso País, poderemos, colaborando, compartilhando informações e formas diferentes de tratar o tema, evoluir de forma mais eficaz e efetiva.

Bom, falando um pouco agora da prática: como uma empresa - e aí eu estou trazendo o meu exemplo no Operador Nacional -, como nós tratamos essa questão.

Bom, falarei de gestão interna, tendo sempre os três pilares de desafios como objeto de atuação: prevenção, detecção e resposta. Não vou entrar em cada uma dessas caixas, mas só relembrando que devemos tratar e devemos utilizar todas as tecnologias disponíveis: *firewall*, anti-*spam*, filtro de conteúdo, aplicação de *patches* de correção, VPN's, *one-time password (*OTP), senhas de uso único e específico, demais tecnologias de prevenção ou intrusão (IPS, WAF, DLP - previsão de vazamento de dados).

Aqui é um tema muito importante e relevante, dado à Lei Geral de Proteção de Dados Pessoais, que vai entrar em vigência no ano que vem.

Processos e tecnologias de análise de vulnerabilidades, SOC, de monitoramento de segurança; Siem, inteligência, correlação de eventos, inteligência artificial, *ethical hacking*, simulações e exercícios de invasão, teste de invasão; e, na resposta: procedimentos, listas de acionamento, simulações para treinar os nossos planos de resposta, CSIRT.

Na componente de conscientização, o objetivo é levar o conhecimento e criar uma cultura de segurança da informação em nossas empresas, nas nossas organizações, em nossos colaboradores, seja através de simulações de *phishing* ou até mesmo de campanhas mais objetivas de conscientização.

Na componente de colaboração: estabelecer uma relação estratégica com as entidades envolvidas em segurança cibernética, sejam dentro do nosso setor, envolvendo o Governo e até mesmo outros países que tenham relações conosco e outras empresas e setores estrangeiros que se relacionam com nossas organizações.

Aqui eu cito a colaboração bastante efetiva com ComDCiber, que culminou este ano com a participação do setor elétrico no Guardião Cibernético, envolvendo ao todo, nos quatro setores envolvidos, mais de 200 pessoas, mais de 40 empresas. Foi uma experiência bastante válida, de vários ensinamentos que nós podemos trazer, especificamente para o setor elétrico.

E não adianta, como eu falei, parar, tirar uma foto e achar que aquilo está resolvido. Nós temos que continuamente evoluir sobre esse assunto.

Especificamente no setor elétrico, trazendo algumas iniciativas que vêm sendo executadas e trabalhadas desde o ano passado, para trazer um horizonte mais recente, as associações de agentes têm conduzido discussões bastante relevantes sobre o tema. No ano passado, também tivemos oportunidade de participar do Brazil Cyber Defence Summit, promovido pelas Forças Armadas. Nesse evento, foram apresentados os resultados do Guardião Cibernético 1.

Ainda no meio do ano a Abrage (Associação dos Geradores de Energia) e Itaipu Binacional promoveram o primeiro Colóquio Técnico de Segurança Cibernética para o Sistema Elétrico, do qual nós tivemos oportunidade de participar também.

Mais para o final do ano, o Cigré, também na linha de promover esse tema no nosso País, realizou aqui em Brasília o I Workshop de Segurança Cibernética.

A Abrate, a associação das transmissoras de energia, desenvolveu uma proposta de um *framework* de segurança cibernética bastante interessante para seus associados, baseado em *frameworks* bastante já consolidados no mundo e com foco de recomendação para suas empresas. A Cier, Comissão de Integração Energética Regional, promoveu em Montevidéu um *workshop* sobre segurança cibernética no setor elétrico da América Latina, apresentando também um trabalho em conjunto com o BID sobre esse tema.

Já para este ano, a execução do Guardião Cibernético 2.0, que envolveu, além dos setores nuclear e financeiro - participaram do primeiro telecom e elétrico. Parece pouco três dias de execução, mas esses três dias, por trás deles, tem um ano de planejamento, de discussões e de tratamento. Em junho, nós no ONS, por conta da relevância do tema, promovemos um seminário sobre segurança cibernética especificamente para operação do Sistema Interligado Nacional, com a participação de entidades governamentais, academia e agentes do setor elétrico.

E, para dar continuidade ao trabalho, considerando de novo a relevância, a importância, a criticidade do tema...

Senador Esperidião Amin, na última audiência pública, no dia 5 de setembro, um ponto que o senhor destacou foi a necessidade de um normativo mais homogêneo sobre o tema. E essa iniciativa do setor elétrico de definição nos nossos procedimentos de rede, para quem não conhece as nossas regras de operação do Sistema Interligado Nacional, nós, os agentes e a Aneel, agência reguladora, estamos trabalhando para estabelecer dentro dos procedimentos de rede requisitos mínimos, controles mínimos para a segurança cibernética na operação de nossas instalações.

Não tive a pretensão aqui de dar uma aula de segurança cibernética, até porque o tempo não comporta, mas de trazer um pouco do que uma empresa, que faz parte de um ecossistema em uma infraestrutura crítica, tem atuado internamente e junto aos seus pares, no sentido de evoluir a nossa capacidade de prevenir, detectar e responder.

Muito obrigado a todos. Bom dia.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Eu que agradeço e cumprimento pelo cumprimento do prazo estabelecido.

Reitero a sua observação, que foi consenso na reunião do dia 5 de setembro, sobre a necessidade de um apurado arcabouço legal para esse conjunto de necessidades.

Já entre nós o Sr. Marcelo Buz, Diretor-presidente do Instituto Nacional de Tecnologia da Informação.

Retomamos a ordem preestabelecida e concedo igualmente a palavra pelo prazo de 15 minutos.

O SR. MARCELO BUZ (Para exposição de convidado.) - Bom dia, Senador Esperidião Amin. Bom dia a todos os componentes da mesa, aos palestrantes e a quem nos assiste também pelos meios digitais.

Eu peço escusas pelo meu breve atraso. Hoje nós estamos realizando o 17º CertForum, que o fórum da certificação digital. Incumbe a mim abrir os trabalhos, como Diretor-Presidente de ITI, então o deslocamento de lá até aqui me tomou um pouquinho de tempo.

Mas acho muito importante e relevante, Senador, a sua proposição desta audiência pública para que a gente possa debater os aspectos de segurança cibernética.

Esses aspectos são, muitos deles, condições *sine qua non*, para que a gente possa ter uma nação realmente endereçada para o futuro e com soberania nacional.

O ITI, Instituto Nacional de Tecnologia da Informação, é vinculado à Casa Civil da Presidência da República e incumbe a nós o mandato do País de desenvolver e ser o proponente das criptografias das chaves públicas brasileiras.

Eu tenho uma breve apresentação para que a gente possa guiar um pouco e, ao cabo dela, eu pretendo falar um pouquinho sobre um projeto de lei que tramita no Congresso Nacional, para que a gente possa avançar e modernizar a Infraestrutura de Chaves Públicas Brasileira, que é uma infraestrutura. Conforme o próprio nome diz, Infraestrutura de Chaves Públicas é uma infraestrutura agnóstica, à disposição de governo e também dos atores da economia, para fazerem uso do certificado digital.

Neste mundo em que nós vivemos, onde os documentos passam a ser nato-digitais, onde há as relações entre pessoas, entre artefatos, entre coisas, com a Internet das Coisas, nós precisamos preservar a integridade, a autenticidade e a autoria, com plena validade jurídica. E quem fez a criptografia endereçada no País é a ICP-Brasil. Por isso, eu venho difundindo, cada vez mais, esse padrão tecnológico que nós temos no País.

Primeira situação que é importante nós ressaltarmos a respeito da ICP-Brasil, Senador Esperidião, é que nós estamos diante de um padrão tecnológico cuja lei que o estabelece é datada de 2001. Isso nos traz sérios limites de desenvolver e adaptar às novas tecnologias existentes, em que pese, na Medida Provisória 2.200-2, de 24 de agosto de 2001, tenha sido instituído, junto com a Infraestrutura de Chaves Públicas Brasileira, a Autoridade Certificadora Raiz e o ITI, um comitê gestor, que desenvolve, que efetivamente faz as regras e regulamenta o setor de infraestrutura. Então, muitas das situações nós conseguimos endereçar através do nosso comitê gestor, porém vale lembrar que a nossa lei é de 2001 e não está muito adequada para os dias de hoje.

É interessante nós falarmos também que a ICP-Brasil é uma infraestrutura organizada pelo Estado, que fiscaliza, credencia e audita essa infraestrutura, que é o papel do ITI. O ITI, por estar vinculado à Casa Civil da Presidência da República, nunca teve um concurso público, nós nos valemos da prerrogativa da requisição. Então, o corpo técnico do ITI é composto pelas mais variadas instituições e órgãos deste País. Cito aqui a Agência Brasileira de Inteligência, o Exército, a Polícia Federal, só para que a gente possa ter um pouco de ideia do conteúdo intelectual sobre criptografia que nós temos embarcado dentro do ITI. Nós temos muito mais proveito para poder entregar à Nação em termos de defesa cibernética.

É uma autarquia, então tem autonomia administrativa e independência financeira. As funções que ao ITI se colocam, que o ITI tem: nós somos a operadora da Autoridade Certificadora Raiz, que fisicamente é uma sala-cofre, com todos os conceitos de sala-cofre, nos mais altos níveis de segurança. Fica na Presidência da República. Nós cumprimos o papel de uma agência executiva dos padrões de certificação digital, somos a entidade que administra todo este credenciamento dos entes, autoridades certificadoras, autoridades de registro e ainda somos a entidade que fomenta e cria padrões de assinaturas digitais, cria o padrão da nossa criptografia. Diga-se de passagem, a criptografia do ITI para os artefatos das coisas, que é algo muito importante em termos de defesa cibernética, é a E-521, que depois eu acho que o Prof. Custódio pode até referendar, que é uma das mais seguras, uma das criptografias mais seguras, e nós já a implementamos aqui no Brasil em nossos *hardwares*, em nossas HSMs. Então, é uma criptografia muito forte.

Temos a presença forte da iniciativa privada, que produz, gera emprego, lucra, gera impostos. A iniciativa privada, que são as autoridades certificadoras e autoridades de registro.

Aqui na tela, a gente pode ver um pouquinho da nossa infraestrutura. São 17 autoridades certificadoras de primeiro nível, normativas; a principal delas é a Receita Federal. Então, vale lembrar que a ICP-Brasil é a grande garantidora do sigilo fiscal brasileiro no que tange ao relacionamento do cidadão para com a Receita Federal brasileira. Ontem mesmo, anteontem, assinamos um protocolo de intenções com o Inmetro por meio do qual o Inmetro passa a se credenciar como autoridade certificadora de primeiro nível e fará a normatização de toda o regramento da criptografia das coisas, dos artefatos. E isso é um avanço fantástico para o nosso País, porque nós vamos ter as transações, as relações entre objetos metrológicos principais primeiramente e, depois de tudo que se possa falar, com plena validade jurídica e não repúdio dessas informações.

Depois nós temos na nossa infraestrutura também carimbos de tempo. O ITI é possuidor de dois relógios de césio, e nós estamos, com a instalação deles, nos credenciando para ser membros da UTC e passar a ser um dos fornecedores da unidade de tempo universal. Aqui no Brasil nós vamos ter mais um laboratório: no caso, a sala cofre do ITI com dois relógios de césio. Já é uma realidade, nós já o temos funcionando, e ele está a serviço para carimbar o tempo das informações as quais os certificados digitais transacionam no mundo digital.

Temos mais de 1,2 mil autoridades de registros que fazem a verificação do cidadão lá na ponta, garantido que uma criptografia esteja sendo endereçada efetivamente para aquele cidadão. E por que isso é tão importante, minha gente? Porque nós não podemos, num mundo tão digital como no qual vivemos, correr o risco de termos falsas pessoas acessando os nossos sistemas. Os riscos são enormes, e, em épocas em que nós estamos fazendo a convergência desses serviços para portais únicos ou em que nós temos todos os documentos que lá, ao cabo, serão assinados por um ministro de Estado ou, quem sabe, lá, ao cabo, culminarão com uma assinatura que, de praxe, acaba sendo de próprio punho da Presidência da República, nós temos que reconhecer que todo o trâmite desses processos transaciona hoje por meio digital. Então, eu fico imaginando a relevância e a importância que nós temos que dar para estes sistemas que fazem esse intermédio entre o nascedouro de uma ideia até ela virar um despacho oficial, seja um decreto, uma lei, uma sanção.

Nesse ínterim, nós temos todas as decisões do País - evidentemente que não as decisões de cunho de defesa nacional que acabam tendo um outro caminho -, todas as decisões do dia a dia, do cotidiano que, no seu compilado, passam a ser de uma importância muito grande, talvez expostas a ataques se nós não estivermos prestando muita atenção, Senador, de como nós estamos fazendo o *login* de acesso a esses sistemas.

Nós temos também os prestadores de serviços de suporte, que são credenciados, fiscalizados e auditados, como toda nossa cadeia é; os prestadores de serviços de biometria, que, ao fazerem a coleta - e isto é muito interessante, porque, ao se fazer a emissão de um certificado digital, nós fazemos a coleta das biometrias, armazenamos, e os nossos PSBios são interoperáveis. Então, a gente tem, toda autoridade de registro passa a ter acesso às informações uma das outras de forma criptografada e anonimizada, o que nos permite garantir que uma pessoa não passe dentro do ICP-Brasil por dois CPFs. É impossível isso acontecer, e, se porventura essa tentativa ocorrer, uma vez identificada através dos padrões geométricos, o padrão da ICP-Brasil é revogar ambos os certificados digitais: o primeiro e o segundo, porque a gente passa a não ter certeza de quem é o verdadeiro e de quem é o fraudador.

Temos também os prestadores de serviço de confiança que endereçam toda essa solução para a nuvem, e nós passamos a ter, então, o certificado digital na palma da mão, no celular e mais instalações técnicas, e instalações técnicas secundárias aqui que ainda constam, mas que nós extinguimos ao longo do Governo Bolsonaro na minha gestão para que nós pudéssemos dar um pouquinho mais de dinamismo à nossa infraestrutura.

Hoje está quase chegando a oito milhões de certificados digitais ativos, e isso nós precisamos endereçar de forma muito veemente. Nós precisamos encontrar ao menos o censo da população economicamente ativa. Nós temos que encontrar maneiras de desentravar o certificado digital para que cada cidadão economicamente ativo possa ter acesso ao que eu chamo de plena segurança, direito à legítima defesa cibernética, que é isso que o certificado digital faz. O certificado digital dá ao cidadão a sensação de plena defesa no mundo cibernético. Isso é extremamente relevante.

O Comitê Gestor, que regulamenta e normatiza, que é formado tanto pelo Estado quanto pela iniciativa privada.

Então, essa é a imagem com que nós podemos resumir a Infraestrutura de Chaves Públicas Brasileira.

Meu tempo vai passando, e eu vou tentar ser muito coeso com ele para respeitar o tempo dos demais.

Eu acho que é muito importante, pessoal, nesta minha fala, que a gente possa entender, endereçar que realmente, no que tange a todos os documentos que nós estamos tramitando no mundo digital, nós não podemos falhar nos nossos *logins* de acesso aos nossos sistemas, nós não podemos mais no mundo de hoje discutir e debater a probabilidade de dar integridade e autenticidade por força de lei a *login* e senha; a lei não pode refletir algo que tecnicamente não seja possível entregar, não pode. Então, quando nós temos às vezes tramitando pelo Congresso Nacional leis que vão ao encontro de flexibilizar,

por ser talvez mais fácil, por ser talvez mais acessível - permita-me aqui dizer, Esperidião -, é um barato que pode custar muito caro para a Nação.

E, se nós pensarmos em uma estratégia de massificação do certificado digital, a escalabilidade pode remeter o certificado digital a custos muito mais baixos. Então, quando nós falamos de defesa cibernética, é irrefutável que nós falemos da criptografia. E essa criptografia, no Brasil, quem mais fala sobre isso, quem mais tem estudos sobre isso, é o Instituto Nacional de Tecnologia da Informação, composto por diversos entes, inclusive de segurança, como Polícia Federal, Exército e Agência Brasileira de Inteligência.

Nesse sentido, Esperidião, eu coloco o Instituto Nacional de Tecnologia da Informação totalmente à disposição tanto do Senado quanto do Congresso, como de todos os atores da nossa Esplanada, para que a gente possa cada vez mais endereçar soluções que culminem com o aumento da segurança cibernética do País. Eu reitero que talvez um processo, um procedimento possa não ser algo de extrema relevância, porém o conteúdo de todos...

(Soa a campainha.)

O SR. MARCELO BUZ - ... a soma de todos os despachos que nós temos tramitando hoje via cibernética oficialmente nos sistemas dos nossos governos precisam ser olhados com outra atenção, para evitar fraudes, evitar corrupções e mitigar, sem sombra de dúvida, todos os riscos a que o Brasil e todas as nações estão expostos no mundo digital.

Vale lembrar também que nós temos ciência de que se debate muito que *hackers* hoje continuam sugando dados para que, lá no futuro, eles possam descriptografar. Então, nós não temos que pensar só na criptografia de hoje; nós temos que pensar em modelos e padrões que nós possamos, de alguma forma, recriptografar no futuro. E aí vêm questões de padrões, questões de regulamentação que o ITI está acostumado a fazer há 18 anos.

Obrigado, Senador.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Muito bem. Cumprimentos pela precisão micrométrica.

Eu vou deixar pendurada uma indagação: o Sr. Marcelo Buz nos diz qual a providência que o instituto toma em caso de duplicidade. Já deixo encomendada a pergunta. O senhor informou qual é a primeira providência - eliminar os dois -, e a seguinte é a pergunta que fica para depois.

Eu vou me inserir na condição de, um pouco privilegiado, mas, um dos internautas, que faz a pergunta. Eu acho que a providência está certa: exclui os dois e depois procura saber quem é o verdadeiro e quem é o *hacker*, que nome tem.

Por uma questão de afinidade e até de citação, eu concedo a palavra ao Sr. Ricardo Felipe Custódio, Professor-Supervisor do Laboratório em Segurança da Computação da Universidade Federal de Santa Catarina, que tem, portanto, afinidade direta com o exposto pelo Sr. Marcelo Buz. O seguinte será o Sr. Marcos Allemand Lopes.

Com a palavra, portanto, o Prof. Ricardo Felipe Custódio.

Eu gostaria de saudar a presença do nosso querido Senador Chico Rodrigues, que, a seguir, presidirá a nossa reunião, juntamente com o Senador Marcos do Val.

Registro que já esteve conosco o nosso Presidente da Comissão de Relações Exteriores e Defesa Nacional, Senador Nelsinho Trad, que está em outro compromisso neste momento, mas também retornará.

Com a palavra, portanto, o Prof. Ricardo Felipe Custódio.

O SR. RICARDO FELIPE CUSTÓDIO (Para exposição de convidado.) - Bom dia a todos.

Quero agradecer ao Senador Amin, na pessoa de quem cumprimento todos os presentes na Mesa, o público, o pessoal do Exército, general.

Muito obrigado.

A minha fala vai ser breve. A intenção aqui não é repetir a apresentação dos demais, não é conceituar, apesar de ser professor de universidade, meu ímpeto seria dar uma aula sobre o que é segurança da informação, política de segurança, norma, mas eu não vou fazer isso. O meu objetivo será rápido no sentido de mostrar o passado, o que foi feito...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Eu interrompo o Prof. Ricardo para passar a Presidência para o nosso querido Senador Chico Rodrigues, uma vez que tenho que me ausentar e retornarei daqui a pouquinho.

Continua com a palavra.

O SR. RICARDO FELIPE CUSTÓDIO - Obrigado. Então, eu vou fazer uma incursão pela história, o que aconteceu no passado, por que estamos criando no Brasil toda essa preocupação com uma Política Nacional de Defesa Cibernética e tentar, com uma bola de cristal, prever o futuro, o que vai acontecer no futuro, de forma muito rápida. Eu vou colocar em seguida um eslaide em que eu coloquei datas, mas essas datas são muito aproximadas, podem variar muito, dependendo da fonte em que a informação foi obtida. É só para ter uma ideia, uma noção, um esqueleto do que de fato aconteceu e do que pode acontecer no futuro.

Podia passar para o segundo eslaide?

Na linha de cima, temos o passado até o presente; na linha de baixo, temos o futuro, aquilo que a gente espera que possa acontecer em termos de segurança da informação, em termos de defesa cibernética.

Na linha de cima, nós vemos que o computador surgiu aproximadamente em 1950, logo após a Segunda Guerra Mundial, nós começamos a ter computador disponível, e aí começaram os problemas cibernéticos.

Em 1969, foi inventada a internet, começou a surgir a internet no mundo. Lá no início, no comecinho, os computadores começaram a se interligar, principalmente nos Estados Unidos, Europa, alguns países asiáticos.

Em 1971, primeiro vírus, primeiro *malware*, primeiro *software* que tentou atacar, roubar, dar algum prejuízo para alguém.

Em 1975, temos um marco muito importante relacionado ao ITI, que foi a criação da assinatura digital. A partir de 1975, então, foi possível, nós conseguimos conceber tecnologia, ferramenta para possibilitar a assinatura digital de um documento eletrônico e, a partir disso, saber quem assinou, quando assinou, por que assinou, enfim, tudo que é necessário saber em termos de segurança de documentos eletrônicos.

Em 1994, com ajuda da RNP, a internet chegou ao Brasil definitivamente. Então, foi instalada a internet no Brasil e nós começamos a criar provedores de acesso à internet, o pessoal começou a acessar rede de computadores.

Em 2000, surgiram as redes sociais, que é uma coisa bastante preocupante hoje em termos de *fake news*, informações falsas, divulgação de informações, roubo de informações, ataques.

Em 2001, por uma vontade da Organização das Nações Unidas, o Brasil criou a Infraestrutura de Chaves Pública Brasileira (ICP-Brasil), que o Marcelo Buz já colocou que foi criada a partir da Medida Provisória nº 2.200/2001.

No ano de 2010, mais ou menos, começou o que a gente chama de guerra cibernética, os primeiros ataques cibernéticos feitos por países contra outros países, empresas contra outras empresas. Ficou patente que isso estava acontecendo e acontece até hoje.

Em 2011, foi criado, a partir da END, o Centro de Defesa Cibernética do Exército, que é uma coisa muito boa, muito bem-vinda no Brasil, que foi um alento, uma coisa importante para a Nação brasileira.

Em 2003, apareceu o Snowden, que provou que existia guerra cibernética, que o Brasil estava sendo vigiado, a Presidência vigiada, que as nossas redes são vigiadas, que as redes do mundo inteiro são vigiadas. Então, ele provou com documentos essa questão. O mundo todo ficou sabendo: "Opa, estamos sendo vigiados". Tínhamos inclusive no Brasil padrões de criptografia que eram baseados em normas controladas pelo NSA, agência de segurança americana, que tínhamos que revogar porque estávamos sendo vigiados pelos nossos próprios padrões.

Em 2014, temos a Política Nacional de Defesa Cibernética, que foi implantada e que é alvo desta reunião aqui para discutir a efetividade dessa política, o que está acontecendo.

Em 2019, com a entrada do novo ITI no Brasil, houve uma mudança, um redirecionamento muito bom, muito importante do ITI, que eu chamo de nova ICP-Brasil. Então, na medida do possível, o ITI fez algumas modificações muito boas, mas precisa de mais, como foi colocado pelo Marcelo Buz. O Senado, o Congresso precisa realmente, nós precisamos de uma nova lei, um novo regramento, um novo marco regulatório para permitir o uso da criptografia. A Infraestrutura de Chaves Pública, na realidade, permite um bom uso da criptografia, em geral.

Hoje estamos aqui avaliando a Política Nacional de Defesa Cibernética, o que a gente fez, o que está sendo feito, o que foi trabalhado. Temos uma série de iniciativas, uma série de entidades propondo políticas de segurança cibernética, uma série de empresas, grupo de empresas, órgãos de Governo trabalhando nesse sentido, então, muitas coisas acontecendo no Brasil. Precisamos coordenar melhor essas iniciativas todas, juntar isso e talvez criar um marco de Política Nacional de Defesa Cibernética.

Futuro. O que precisamos trabalhar, o que falta? Nós não cuidamos das nossas âncoras de confiança do mundo cibernético. Nós não temos controle do que o povo brasileiro, do que podemos confiar. Hoje esse controle é feito por outras nações e por empresas estrangeiras, nós não temos o menor controle. Hoje, se uma empresa americana quiser, ela desativa o sistema bancário brasileiro, basta revogar os certificados raiz das ACs que emitem os certificados digitais dos bancos brasileiros. Então, nós não temos esse controle.

Como isso é feito na Europa? Na Europa, as nações, os países têm a lista de serviços eletrônicos confiáveis. Todo Estado publica essa lista de forma constante e indica em que serviços o povo pode confiar. Isso falta no Brasil, nós não temos.

Nós não temos interoperabilidade das aplicações. Nossos padrões de interoperabilidade, apesar de termos o programa ePING, ele ainda é muito incipiente, deveria ser mais bem tratado. Nós deveríamos criar padrões efetivos de interoperabilidade não digo semântica, mas pelo menos sintática, para permitir que todas as aplicações possam se comunicar, se integrar, evitar retrabalho e que efetivamente a gente possa fazer a defesa cibernética do nosso sistema de informação.

Nós não temos um barramento brasileiro, um barramento de Nação, para garantir uma integração dos sistemas de informação, como existem em vários países. Então, sisteminhas que precisam se comunicar, trocar informação, nós hoje estamos dependendo totalmente de padrões privados, padrões que não são padrões, são privados.

O relógio. Apesar da iniciativa do ITI de ter um relógio atômico e permitir que certificados digitais sejam emitidos nas datas corretas, nós não cuidamos bem do nosso relógio. O que significa cuidar do relógio? Os relógios de todas as máquinas, de todos os equipamentos, são sincronizados em algum lugar via satélite, via GPS, via Network Time Protocol, via protocolos de rede para fazer isso no relógio, mas hoje é possível controlar os relógios das máquinas e fazer ataques. Então, nós temos que cuidar melhor do nosso relógio. Hoje nós temos duas fontes de hora no Brasil, que é o Observatório Nacional, no Rio de Janeiro, e o ITI, mas nós, povo, não temos acesso a um relógio confiável.

Gerador de números aleatórios. Nós tivemos uma iniciativa muito boa da Abin no passado para criar um *chip* para fazer a geração realmente confiável de números aleatórios, porque todas as chaves criptográficas, todas as chaves públicas, tudo que nós precisamos de segurança da informação depende dos geradores de números aleatórios, depende de um gerador de números aleatórios confiável, e nós temos hoje pouco acesso a isso.

Do 5G, está todo mundo falando, 5G vai acontecer. Na China, já está espalhado; nos Estados Unidos, está se tentando controlar, e vai entrar no Brasil forte, ou seja, todos os equipamentos, sistemas, vão poder se comunicar de forma muito rápida e a defesa cibernética vai se tornar muito mais difícil, nós vamos ter que ter muito mais ferramentas, muito mais sistemas, muito mais processos para cuidar bem dos nossos sistemas de informação.

Hardware. Há muitos anos se fala dos *chips*, circuitos integrados, que a gente não produz no Brasil. Então, hoje nós não cuidamos muito bem disso, porque é difícil de cuidar, é muito caro criar uma fábrica de *chip*, é muito caro ter produção de equipamentos de *hardware*, mas, em alguns sistemas, em alguns ambientes, nós precisaríamos realmente ter o controle, o domínio tecnológico de criar alguns *chips*, alguns circuitos integrados, alguns equipamentos que seriam colocados em pontos estratégicos, principalmente em ambientes de infraestrutura crítica, para que efetivamente o Estado brasileiro tenha condição de controlar. Nós não podemos pensar que vamos poder ter controle cibernético, de segurança cibernética em todo o sistema, não tem como, mas em alguns sisteminhas nós poderíamos ter.

E o futuro, o que está vindo aí, gente? Com o que o mundo está preocupado? Com o computador quântico, que vai quebrar toda a criptografia que temos hoje no Brasil. Toda a segurança, o mínimo de segurança que nós temos hoje não vai existir mais. O RCA vai ser quebrado, curva elíptica vai ser quebrada. E o que nós estamos fazendo nessa seara? Praticamente nada. Nos Estados Unidos, por exemplo, o Nist (National Institute of Standards and Technology) está criando padrões de assinatura digital, padrões de fazer acordo de chave, os protocolos de acordo de chave, padrões de comunicação já quânticos, tanto usando técnicas de criptografia pós-quântica quanto algoritmos quânticos. Nós precisamos cuidar com carinho dessa questão da computação quântica no Brasil.

É isso, não vou falar mais.

Muito obrigado. Fico à disposição para qualquer dúvida.

O SR. PRESIDENTE (Chico Rodrigues. Bloco Parlamentar Vanguarda/DEM - RR) - Dando continuidade à audiência pública, eu concedo a palavra ao Sr. Marcos Allemand Lopes, gerente do Departamento de Gestão da Segurança da Informação e da Continuidade de Negócios do Serviço Federal de Processamento de Dados (Serpro).

V. Sa. tem 15 minutos.

O SR. MARCOS ALLEMAND LOPES (Para exposição de convidado.) - Bom dia, Senador Chico Rodrigues, colegas de Mesa, senhores e senhoras. Eu gostaria de começar a minha fala aqui pegando uma palavra do que o Fabio colocou, que foi a colaboração. Então, esta apresentação está centrada nessa questão da colaboração. Fiz também uma linha de tempo, como o Prof. Custódio, mas não vou...

Vamos lá.

Eu detalhei aqui alguns principais marcos em que o Serpro esteve envolvido com vários órgãos de Governo. Essa questão da colaboração, essa questão da confiança, tem estado presente desde 1999, quando a gente sentou em conjunto e começou a elaborar o Decreto nº 3.505 que foi a Política de Segurança da Informação da Administração Pública Federal. E aí a gente chega até 2019. Eu vou detalhar essas etapas rapidamente. São poucos eslaides.

Como marcos, eu coloquei ali a própria política, a questão dos grandes eventos e, por fim, a proteção das infraestruturas críticas.

Em termos da política, como eu falei, o início da elaboração do Decreto nº 3.505 foi em 1999. Em 2000, ele entrou em vigência. Foi criado o Comitê Gestor de Segurança da Informação; foi criado o Departamento de Segurança da Informação e Comunicação, hoje o DSI; houve, lá na política, o direcionamento para a criação da ICP-Brasil. O Serpro participou ativamente. Quando o Senador Esperidião Amin falou que a próxima ligação seria com o Prof. Custódio, ligado com o ITI, a gente teve muita interação com essa questão de ICP. Não existia nem ITI na época, no ano 2000, quando a gente começou isso. Houve a criação do CTIR Gov, também, de que a gente participou em conjunto. A elaboração de normas complementares, várias ações de conscientização de segurança para a PF, em conjunto com o Comando do Exército, o Comando da Marinha, o Casnav. E também um curso de pós-graduação na UnB, para 40 pessoas, com foco em gestão de segurança. Essa ação foi tão legal, tão importante, que o próprio DSI resolveu fazer três turmas, também com a UnB, nesse tema. Foram três turmas presenciais, depois foram elaboradas mais três turmas de ensino à distância para ampliar essa capacitação da Administração Pública Federal.

Esse foi o primeiro marco, que eu destaquei. O segundo, já chegando mais para perto, agora, foram os grandes eventos. Aí sim, a gente começou a ter um contato maior com o CDCiber. A gente teve participação junto lá na Rio+20, depois outros grandes eventos. Na época era o CDCiber, e logo em seguida foi criado o Comando de Defesa Cibernética. Então, foram várias reuniões de planejamento, um detalhamento muito grande, um profissionalismo enorme. Nada podia falhar. Na ação operacional conjunta também estávamos lá, na Rio+20 e em outras atividades também. E é importante a reunião de avaliação pós-ação, ou seja, fez a missão, voltou, avaliou, vamos nos preparar para a próxima.

Nós assinamos um acordo de cooperação com o CDCiber, se não me engano em 2014, Serpro e CDCiber, justamente por causa desses grandes eventos. O próximo ponto aqui tem a ver com um momento mais recente, com relação a essa questão da proteção das infraestruturas críticas. Por volta de 2006, com o DSIC, hoje DSI, a gente elaborou um guia de referência para a segurança das infraestruturas críticas. É interessante que, para todas essas ações, a gente tinha componentes nos grupos que... Nessa época nem tinha sido criado ainda o ComDCiber, mas havia pessoas lá que eram como se fosse o DNA do ComDCiber porque no final, ao longo dos anos, eles acabaram indo para o ComDCiber. Então, na época da política de segurança, do Decreto nº 3.505, havia um oficial do Exército, que era um capitão, que estava lá discutindo a política e depois, no grande evento Rio+20, ele também estava lá discutindo as ações da Rio+20. É interessante essa questão de trabalhar junto, a questão da confiança, aquele negócio de estar junto há muito tempo, que só de olhar já sabem o que fazer.

Houve a questão de um grupo de trabalho voltado para a segurança da infraestrutura crítica e finanças. A gente participa disso já há bastante tempo. É um grupo lá no GSI, no Departamento de Assuntos de Defesa Nacional. Existem outros grupos de infraestrutura crítica também, de água, transportes, telecomunicações, mas o Serpro está nesse de finanças, justamente por causa da interação com sistemas críticos que a gente desenvolve e produz, como o Siafi, que serve para o Tesouro Nacional e para a Receita Federal.

Participamos também da elaboração da Política Nacional de Segurança das Infraestruturas Críticas, que foi publicada agora no final de 2018. Agora, está sendo desdobrada na Estratégia Nacional de Segurança das Infraestruturas Críticas. Da mesma forma, a publicação da PNSI (Política Nacional de Segurança da Informação) também saiu no final de 2018. Estávamos lá presentes também. Na Estratégia Nacional de Segurança, que é consequência da política, participamos também. Inclusive, ela está em consulta pública até o dia 2 de outubro.

Fechando esse bloco de proteção de infraestruturas críticas, não poderia deixar de citar a questão do exercício cibernético: o ciclo de 2018, que foi o Guardião I; e agora, em 2019, o Guardião II. Como o Fabio adiantou aqui, foi um sucesso, realmente. Os dois setores que participaram no primeiro evento não queriam deixar de participar, e aí ampliou para mais dois. Foi muito importante essa questão desse exercício.

Finalmente, aqui, alguns pontos fundamentais. Participando nesses 20 anos em grupos de Governo, o que a gente vê é que é fundamental essa questão de capacitação. A gente sabe que, sem capacitação, fica difícil a gente ter uma boa resposta em termos de segurança e defesa cibernética.

A questão de confiança e colaboração é fundamental. É a palavra inicial aqui. A gente, do Serpro, tem essa real visão de que essa questão de colaboração é fundamental. Por isso, a gente sente que tem essa responsabilidade de repassar os nossos conhecimentos e também absorver conhecimentos dos outros grupos de órgãos de Governo. É fundamental essa

questão de coordenação setorial para as infraestruturas críticas e também uma nacional, ou seja, se a gente está falando de segurança na parte de energia, é importante que o setor se cuide, que ele tenha um tratamento, processos definidos e as questões tratadas ali, o que não impede, e é necessário, que haja essa coordenação nacional também. A questão da infraestrutura adequada é fundamental. Sem isso, a gente não consegue, realmente, dar respostas adequadas e efetivas. Quando se trata de infraestrutura crítica, isso é *top*, é fundamental. E há a questão do tal envelhecimento da infraestrutura. A gente às vezes implanta alguma coisa muito boa, mas com o passar do tempo isso vai ficando esquecido, e isso às vezes não é um ataque, mas é uma falha que ocorre por causa desse envelhecimento. Finalmente, ali, há a questão de ações preventivas e reativas. Ou seja, não adianta a gente focar só em preventivas, porque a gente vai precisar reagir de alguma forma. Por mais que a gente imagine as situações todas de ameaças, de vulnerabilidades, a gente sempre vai esquecer de alguma, ou vai surgir uma nova e a gente não vai saber responder se não estiver preparado. É nessa hora que entra a questão da resiliência, que é um tema importante. Alguns países, após o ataque terrorista de 2001, resolveram alterar a estratégia de infraestrutura crítica. Antes se falava em proteção das infraestruturas críticas, e a partir desse evento começou a se falar em resiliência das infraestruturas críticas, porque elas não podem parar, ou não podem se degradar no total. Pelo menos um nível mínimo de serviço tem que estar disponível, já que ela é uma infraestrutura crítica.

É isso que eu queria falar rapidamente. Não falei do Serpro. Falei mais dessa parte de colaboração, que é fundamental, e a gente entende assim lá no Serpro.

Muito obrigado.

O SR. PRESIDENTE (Chico Rodrigues. Bloco Parlamentar Vanguarda/DEM - RR) - Eu quero agradecer a participação do Sr. Marcelo Buz, Diretor-Presidente do Instituto Nacional de Tecnologia da Informação (ITI); ao Sr. Fabio Reis Côrtes, Gerente de Arquitetura e Segurança de Tecnologia da Informação de Operador Nacional do Sistema Elétrico; ao Sr. Marcos Allemand Lopes, Gerente do Departamento de Gestão da Segurança da Informação e da Continuidade de Negócios do Serviço Federal de Processamento de Dados (Serpro); e ao Sr. Ricardo Felipe Custódio, Professor-Supervisor do Laboratório em Segurança da Computação da Universidade Federal de Santa Catarina.

Eu gostaria de suspender a reunião por alguns minutos, enquanto outro Senador assume a Presidência, porque estou na Presidência também da medida provisória do FGTS, e vence prazo na próxima semana. Nós estamos no limite exatamente da aprovação da medida provisória, para que ela possa realmente manter a sua validade. Então, gostaria de pedir a paciência de vocês, dos participantes desta audiência pública, para que aguardassem mais um pouco enquanto nós temos a presença de um Senador para continuar presidindo a sessão.

Então, suspendo a reunião por alguns minutos.

Muito obrigado.

(Suspensa às 10 horas e 27 minutos, a reunião é reaberta às 10 horas e 52 minutos.)

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Declaro reaberta a reunião.

Tenho a honra de convidar, para compor a segunda Mesa de debatedores, a Sra. Cristine Hoepers, Gerente Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil; o Sr. Márcio da Silva Nunes, Vice-Presidente da Associação Nacional de Certificação Digital; Sr. Ilton Duccini, Diretor de Segurança Digital na Empresa Telefônica Brasil e Professor da Universidade Estadual de Campinas; Sr. Eduardo Bergo, Diretor Setorial da Comissão Executiva de Segurança Cibernética da Febraban, junto ao Banco do Brasil.

Então, eu concedo a palavra à Sra. Cristine, Gerente Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

A SRA. CRISTINE HOEPERS (Para exposição de convidado.) - Prezado Senador Marcos, muito obrigada pelo convite. Agradeço e agradeço às autoridades em nome do General Amin, do almirante, do brigadeiro.

Desculpem todos pela voz; estou com uma crise alérgica um pouco severa. Se eu começar a tossir, não se assustem.

O que eu queria conversar um pouco hoje, dentro dos tópicos de pauta que eu acho que estão mais adequados à atuação do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), é um pouco sobre ameaças e o cenário cibernético brasileiro. O CERT.br foi criado em 1997. Nós estamos com 22 anos de atuação; desses 22 anos, eu estou lá há 20. Ele foi criado através de um diagnóstico do Comitê Gestor da Internet no Brasil, que é uma entidade multissetorial, coordenada pelo MCTIC, que é responsável por coordenar e integrar todas as iniciativas de internet, do que seria necessário para a gente aumentar os níveis de segurança da internet no Brasil.

As pontuações que eu vou fazer são muito em cima de todas as fases de trabalho que nós temos, do tratamento de incidentes aí por esses 20 anos, dos problemas e de onde nós estamos vendo algumas das causas raízes dos problemas e de projetos que nós temos, de analisar tendências e sensores - desde 2001 nós temos trabalhado com isso.

Gostaria até de atualizar um pouco. Não sei se ficou claro para todo mundo o último painel. Houve o comentário sobre hora oficial, talvez confiança. Eu só queria reforçar que o Comitê Gestor da Internet, desde o final dos anos 90, mantém uma infraestrutura de hora oficial do Brasil junto com o Observatório Nacional, em que a gente tem quatro relógios de césio, um GPS, e são todos acessíveis para serem utilizados via protocolo NTP, bem como eles também podem ser usados para carimbo de tempo, e hoje já são, por exemplo, usados pelas instituições financeiras para carimbar tempo de transações.

Uma coisa que eu acho que, antes de a gente falar de problemas, a gente deve falar é do tamanho da internet brasileira. A internet brasileira, sem dúvida, é uma das maiores do mundo. O gráfico à esquerda mostra que nós somos 70% de todas as redes autônomas da América Latina e do Caribe. Então, hoje, em todos os sistemas autônomos, a segunda maior é a Argentina, apesar de o México ser sempre visto como um dos maiores em usuários, eles têm poucas redes autônomas. Hoje a gente tem - no último trabalho do Cetic, que é também uma instituição do Comitê Gestor da Internet, que faz todo o mapeamento de internet - mais de 6 mil provedores de acesso no País. Embora a gente sempre lembre muito dos grandes provedores, a gente tem muitos, e 75% deles têm mil clientes ou menos.

Então, esse é um cenário com que também é difícil de lidar, porque você tem uma pulverização grande de empresas, você tem que atingir todas essas empresas com mensagens de segurança, boas práticas, e o Brasil também, hoje, tem um dos maiores pontos de interconexão de tráfego no mundo, que é o ponto de interconexão de São Paulo. Ele é o nº 1 do mundo em número de participantes, com mais de 1,7 mil - 1,7 mil redes autônomas se conectam lá. O segundo maior do mundo é o de Amsterdã, e tem só 800 membros. Então, hoje, a gente, em número de participantes, realmente é o líder mundial, e é o nº 3 do mundo em tráfego. Então, a nossa internet não é desprezível; ela é grande e ela cresceu muito com todo esse esforço de governança de internet no País, de você ter esse modelo multissetorial e de implementação de boas práticas.

Um outro ponto também que eu queria trazer, de que eu acho que a gente não pode sair, por mais que a gente esteja pensando em segurança das nossas empresas, é que a gente tem que pensar na segurança do cidadão. Hoje, nós temos que 70% da população respondeu, na última pesquisa feita em domicílios no Brasil, que utilizou a internet há menos de três meses. Então, isso é considerado, inclusive nos padrões da Eurostat, do ITU, que é um usuário de internet: você usou pelo menos nos últimos três meses.

E o que eu acho que também não pode ser deixado de lado é o crescimento do uso de telefone celular e televisão. Hoje a gente tem que 97% da população acessa via celular, e só 43% via computador. Eu acho que a gente precisa prestar atenção nesse ecossistema, porque hoje, no ecossistema de celulares, a gente sabe que as empresas que vendem aparelhos têm políticas de atualização e *upgrades* diferentes para a região da América Latina. Então, a maioria desses aparelhos é de baixo custo e é política da empresa não atualizar o telefone, inclusive para questões de segurança. Então, a gente tem que assumir que a população vai estar vulnerável, vai estar acessando isso desse tipo de dispositivo. Eu acho que esse cenário não pode ser tirado do nosso norte. E eu acho que uma das coisas que também todo mundo fala muito é que a IoT vai ser o problema do futuro, mas ela já é o problema há muito tempo. Hoje, a gente tem várias categorias, tem ataques de negação de serviço, fraude, mas todos eles têm algum componente de Internet das Coisas. Hoje a maior parte das negações de serviço que nós vemos saindo de redes brasileiras estão sendo feitas via câmeras de TV, roteadores de banda larga, TVs, as *smart TVs*, toda sorte de *smartphones.* Isso a gente está vendo tanto em notificações de incidentes quanto na nossa rede de sensores.

E são os mais diversos tipos de ataques: mineração de criptomoedas, ataques a terceiros, fraudes. E as tentativas de fraudes contra o cidadão também são muito prevalentes via meios falsos ou de infecção dos dispositivos, e isso está migrando para celulares. Por quê? Porque a gente está vendo a população migrando para celulares, os negócios estão migrando para celulares, e o acesso a serviços de governo eletrônico também vão migrar para celulares, se já não migraram totalmente. Então, acho que a gente não pode perder isso de vista.

E acho que o principal que a gente tem que ver é que o ecossistema é muito complexo, ele é interdependente. Eu fiz essa pirâmide. Ela não é uma pirâmide de importância dos atores, mas ela é uma pirâmide que reflete, no seu tamanho, a quantidade de profissionais que a gente tem hoje em cada uma dessas áreas. A maioria das pessoas que se formam em computação, sistemas de informação, engenharia da computação acabam trabalhando em projetos de desenvolvimento de sistemas, e a gente precisa de segurança lá, porque hoje o maior problema que a gente tem é que os sistemas já chegam inseguros, e aí o primeiro ponto acima dos desenvolvedores, que são aqueles que implantam os sistemas, administram os sistemas e aplicações, é que eles estão lidando com sistemas vulneráveis, que têm problemas, eles estão tentando configurar da melhor maneira possível. Acima disso, a gente tem profissionais de segurança, que é onde a gente começa a

ter a inserção de ferramentas de segurança, de *firewalls* e tudo o mais, mas vejam que isso é um remendo para o que há de errado, que está vindo debaixo dessa rede, e cada vez que a gente vai subindo a gente tem menos profissionais preparados, a gente tem mais falta de mão de obra qualificada.

A área de tratamento de incidentes depende de todas as outras, a área em que eu atuo. Quer dizer, nós estamos lá, tentando resolver problemas que foram criados na base dessa pirâmide, em sistemas desenvolvidos sem se pensar em segurança, que foram implantados também sem muito foco em segurança e que as ferramentas de segurança não estão dando conta de proteger. Então, a gente tem isso, e, no topo disso, a gente tem todo o trabalho de defesa cibernética, que está tendo que lidar com algo muito mais especializado, com menos gente ainda e dependendo de tudo o que está sendo feito por todas as outras áreas também para ser efetivo.

Então, isso eu acho que é muito importante a gente pensar e lembrar que hoje praticamente tudo é *software*: carros são *softwares*, eletrodomésticos são *softwares*, o celular... Então, tudo tem algum componente de *software*, e esse *software* está sendo feito sem se pensar em segurança. E eu diria que uma das coisas que é urgente é a gente tentar envolver atores de engenharia de *software* e desenvolvimento para nos criar menos problemas. Então, esse é um problema, é um desafio grande que a gente tem hoje. A gente precisa envolver a Sociedade Brasileira de Computação, precisa repensar toda a parte de currículos de universidades, o que Capes e CNPq estão demandando como métrica. Eu teria que ter como métrica sistemas mais seguros; não necessariamente só mais sistemas. Eu teria que mudar o sistema de incentivos. A gente teria que tentar definir requisitos mínimos de segurança. Eu acho que, nessa área de segurança, certificações estacionam, são muito boas para algo que é mecânico, mas se você tem algo que, para se manter seguro tem que ser atualizado constantemente, você não consegue certificar. A gente precisa mover para a maturidade. Eu quero certificar que uma determinada empresa tem maturidade e desenvolvimento, eu quero certificar que uma determinada organização tem processos maduros, mas eu não posso certificar um pequeno *software* e achar que ele, quando for interagir com outros *softwares*, vai continuar com a mesma integridade. Então, é um sistema complexo o que a gente tem. Outra coisa que em que a gente precisa atuar muito é quem está administrando sistemas e aplicações na internet. Hoje nós temos esses sistemas com muitos problemas já vindo da outra área. Temos poucos profissionais no mercado - e isso em nível global; não estou falando só de Brasil - com conhecimentos sólidos de protocolos de internet. Então, volta o problema da questão educacional, da questão de formação.

A internet é um bem global, e ela tem esse valor porque ela tem interconexão, porque você tem a economia girando, porque você tem inovação, tem desenvolvimento. Então, tudo o que você precisa implementar em segurança precisa seguir boas práticas globais. Você não consegue fazer isso localmente.

Na área de segurança, a gente tem profissionais tentando implementar ferramentas, soluções, mas eles dependem muito do sucesso dessas ferramentas e soluções, da base que eles estão recebendo. Você precisa ter cooperação. Cooperação já foi destacada pelos outros palestrantes; eu não vou nem reforçar muito mais isso, mas o que a gente precisa reforçar é que, mesmo que a gente tenha *software* desenvolvido com a maior segurança possível, tenha pessoas colocando isso para funcionar, fazendo o melhor que elas podem de boas práticas, que a gente tenha as melhores ferramentas, é impossível fazer 100% de segurança nessa área, porque a complexidade é muito grande.

Então, incidentes de segurança vão acontecer, ou seja, a gente vai ter ataques. Haverá ataques que terão sucesso. E como é que a gente torna o País mais resiliente? Detectando rápido e respondendo rápido, porque, se você detecta adequadamente, você reduz o dano, você tem agilidade. Então, acho que a gente precisa pensar nisso. Eu preciso ter essa base toda. É o foco do CERT.br, a gente tem tentado focar. Foi o primeiro grupo criado no País em 1997, e o foco, desde o início, foi aumentar o número de grupos de tratamento de incidentes, treinar profissionais - a gente já treinou mais de mil profissionais nessa área de tratamento de incidentes, não é segurança como um todo - e principalmente criar massa crítica e influenciar padrões globais, porque se a gente quer ter coisas melhores, a gente tem que tentar influenciar ao máximo os fóruns mundiais que estão definindo padrões.

A minha especialidade, obviamente, não é defesa cibernética; essa é a especialidade do comando de defesa. E eu acho que uma das coisas mais valiosas que eles têm no cerne deles é a importância da cooperação, de os atores estarem envolvidos, e de que tudo depende de que todos façam a sua parte, mas você tem as pontas, que são quem está lá, podendo instalar uma atualização de *software*, é a ponta, é a empresa, é o cidadão, que consegue botar o antivírus, é ele que tem que fazer a parte dele, mas nenhum de nós, que estamos nas pontas, podemos fazer as questões importantes e estratégicas de inteligência e defesa.

Eu acho que tudo isso tem que ser um sistema que se coordena e que funciona em conjunto. Eu acho que a gente está movendo para isso, com todas essas reuniões, com exercícios, com todo esse trabalho de todo mundo interagir.

A nossa atuação lá no NIC.br e no Comitê Gestor é mais nessas áreas entre a segurança de administração de sistemas, segurança cibernética e tratamento de incidentes. É um dos princípios de governança no Brasil de que você precisa ter

estabilidade, segurança e funcionalidade caminhando juntas. Eu não posso ter uma rede segura desconectada. Eu não posso ter uma rede funcional, mas que não me permita fazer nada de negócios ou de Governo eletrônico. E a gente precisa ter padrões internacionais e boas práticas, acho que isso é muito chave.

A gente hoje está levando a cabo um programa, que é o Programa por uma Internet mais segura, que é uma iniciativa conjunta de várias associações de provedores, associações de indústrias de *software* e *hardware*, e todo esse trabalho é um trabalho colaborativo de como sair da infraestrutura de internet e ir até uma infraestrutura mais segura. Isto é muito importante para nós, quer dizer, é você ter uma rede que tem ataques, que tem problemas, que tem vulnerabilidades, e colocar todos os provedores de acesso, operadoras de telecom, sistemas autônomos, todos juntos, trabalhando para um sistema mais seguro. Então, hoje o nosso foco tem sido produzir material educacional livre, dar treinamento pelo Brasil. Nós temos ido a todas as reuniões regionais de provedores de acesso e universidades para dar treinamento em boas práticas. Estamos tentando gerar o máximo possível de indicadores de segurança para poder ver a melhora e poder ver esse impacto. E aí o que a gente espera é que a gente chegue a uma internet mais resiliente, mais segura.

Uma outra parte que a gente foca desde 2000 é a criação de materiais educativos de uso livre - e eles são todos de uso livre mesmo. Então, hoje, a gente tem escolas utilizando esse material, tem empresas. E ele é um material para que todos possam usar, quer dizer, para quem precise conscientizar e aculturar, que já tenhamos isso feito, isso pronto, e você só precise fazer a última milha, como a gente comenta tecnicamente, que é ir até a ponta e conversar com as crianças - nós temos material para crianças, para adultos, para terceira idade. Então, são materiais que a gente está vendo muita gente adotando.

E eu queria só agradecer - eu falei brevemente aqui - novamente o convite do ComDCiber, o convite do Senado, pela importância da reunião.

Muito obrigada.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Agradeço as palavras da Sra. Cristine.

Concedo a palavra ao Sr. Márcio da Silva Nunes, Vice-Presidente da Associação Nacional de Certificação Digital.

O SR. MÁRCIO DA SILVA NUNES (Para exposição de convidado.) - Obrigado, Senador.

Primeiramente, eu gostaria de cumprimentar a Mesa, na pessoa do Presidente da Mesa; registrar o agradecimento ao Senador Esperidião Amin pelo convite da ANCD; cumprimentar as autoridades das Forças Armadas, da sociedade civil, as senhoras e os senhores.

Tentando não ser repetitivo na apresentação, até porque especialistas já vêm falando sobre vários aspectos, o meu desafio aqui foi tentar criar uma apresentação mais de contextualização propriamente dita. *(Pausa.)*

Agora que a tecnologia voltou a funcionar, vou tentar cumprir o meu prazo ainda em cima disso.

Representando a ANCD, quem é a ANCD? Associação Nacional de Certificação Digital, que eu aqui estou representando, sou Vice-Presidente do Conselho.

Somos uma associação civil sem fins lucrativos, e o nosso desafio é desenvolver e massificar o uso da certificação digital no nosso País.

Aqui somos representados por sete associados que operam três infraestruturas completas. E quando a gente fala de três infraestruturas completas de infraestrutura de chaves públicas, a gente está falando de centenas de profissionais de desenvolvimento de *softwares* de segurança da informação que trabalham justamente para poder manter os padrões de funcionamento e garantir que a inovação tecnológica não sejam, na verdade, gatilhos também de crescimento de vulnerabilidades.

Ao mesmo tempo, quando a gente fala disso, a gente fala de fato de um Sistema Nacional de Certificação Digital, baseado na ICP-Brasil, como foi comentado pelo Presidente do ITI na última Mesa, o objetivo é realmente massificar o uso da certificação, usando, como elemento de segurança, um elemento de desenvolvimento econômico, mas que ao mesmo tempo seja de segurança; promover o uso do certificado propriamente dito na forma da sua assinatura como está regulamentada para que efetivamente a gente possa ter uma equivalência jurídica baseada num elemento seguro que traga este tipo de suporte; promover a conscientização coletiva - para que serve o certificado? Como utilizá-lo? Como tirar vantagem? Por que, de fato, ele é importante na sociedade? -, a substituição do papel, enfim.

Além disso, o nosso desafio é desenvolver, evoluir e apoiar padrões. Então, a medida - como o próprio Prof. Custódio mencionou na primeira parte -, a própria linha de tempo sobre a evolução da tecnologia e os desafios que tem, o nosso desafio também é desenvolver essas tecnologias, apoiar padrões e colocar essa implementação para que possamos promover um aspecto bastante importante, que é a interoperabilidade.

Quando a gente fala sobre cibersegurança, efetivamente sobre os ataques, qual é o desafio? O desafio é que a gente não consegue, de fato, lidar com todos os desafios que chegam, porque os desafios crescem todo dia. A gente fala de tecnologias disruptivas. E, aí, quando a gente pensa em guerra cibernética, é, engraçado não, mas é interessante a troca de palavras ali, quer dizer, é uma guerra silenciosa, mas, ao mesmo tempo, a gente está trocando armamentos, metralhadoras por *malwares*, por *softwares*, defesas por *firewalls* e, de fato, a gente está trocando os alvos: no lugar de serem elementos físicos, a gente está trocando por computadores, bancos de dados, equipamentos - como foi mencionado -, câmeras de vídeo, enfim, todo tipo de ataque para obter algum tipo de vantagem, algum tipo de espionagem ou vantagem competitiva.

Mas o que está mudando, de fato? Tudo. Tudo está mudando, e muda o tempo inteiro, e tudo o que afeta é afetado. Toda vez em que a gente coloca uma tecnologia, essa tecnologia sofre também alterações ao longo do tempo, e ela é afetada pelas novas inovações. Então, como garantir a resiliência dessas tecnologias da infraestrutura que você opera e ao mesmo tempo continuar inovando? Esse é o grande desafio de quem lida com tecnologia e com segurança.

Então, qual é a próxima curva da inovação? A gente vive falando sobre inovação, e inovação, na verdade, além de uma aliada da evolução da economia e da sociedade como um todo, também é um desafio. Interessante é que 65% das crianças que hoje estão no primeiro ano não vão trabalhar em atividades que a gente conhece hoje, o que vai criar novas vulnerabilidades, novas situações, novas narrativas de uso da tecnologia para o desenvolvimento social pela própria sociedade.

A gente fala sobre os 6 Ds das tecnologias. Como é que vai ser esse processo? Sai pelo processo de digitalização, há uma expectativa, você começa a entrar na disruptura disso e, no final, você está falando em desmonetização e democratização da tecnologia.

Como democratizar a tecnologia quando princípios importantes de segurança da informação precisam estar inseridos na própria cultura? Esse também é o desafio.

Se a gente for levar em consideração que, nos últimos 150 mil anos, o desenvolvimento humano se baseou de forma local e linear, hoje ele é exponencial e global. Então, a todo tempo, em qualquer lugar, você tem um desenvolvimento da tecnologia, um *software* novo, um ataque novo, que cria, na verdade, situações nas quais você tem que trabalhar a prevenção. Esse é o grande desafio. Então, a todo tempo, em qualquer lugar, você tem um desenvolvimento da tecnologia, um *software* novo, um ataque novo, que cria, na verdade, situações em relação às quais você tem que trabalhar a prevenção. Esse é o grande desafio.

A gente volta 20 anos como era, quer dizer, a quantidade de dispositivos e tecnologias que se tinha, mais analógicos ou menos digitais, e hoje se carregam todas elas no bolso e com muito maior capacidade de processamento. O futuro em perspectiva: quando a gente olha, a gente imagina que, na própria era da indústria 4.0, você envolve estratégia de competitividade das empresas, desenvolvimento de negócios, tecnologia em si, cada vez mais disruptiva, pessoas interagindo com essa tecnologia e a sociedade. É que, à medida que você vai evoluindo isso, você começa a imaginar outros ambientes.

Então, não é só o ambiente no nosso mundo, a gente começa a falar agora em como sair do nosso mundo e ir para outros lugares; começa a usar a inteligência artificial cada vez mais intensamente, quer seja para ataque ou para defesa - e é defesa sim. Então, trata-se de saber como atacar ou como se defender de um ataque quando ele está baseado em inteligência artificial. Então, a defesa também tem que fazer uso da própria inteligência artificial como elemento. Sistemas estáticos estão fadados a terem maior dificuldade para poderem, justamente, combater sistemas que são baseados nisso.

E, cada vez mais, a gente consegue transportar o bem e o mal de forma muito mais simples. Através de um *drone*, eu consigo transportar qualquer tipo de efeito, para o bem ou para o mal. Então, a segurança do espaço aéreo, a forma como esses *drones* são disponibilizados, como eles são utilizados, a tecnologia embarcada e qual o objetivo deles, tudo isso também faz parte desse ataque, que é físico e digital ao mesmo tempo.

Há a própria identificação das pessoas. Então, trata-se da capacidade de poder identificar. A gente tem casos bastante... A China consegue identificar em 3 segundos 1,3 bilhão de cidadãos através de uma análise facial. Então, como fazer isso? Até que ponto isso é importante, ou crucial, para o desenvolvimento da sociedade e para garantir segurança nos ambientes?

Você começa a ter assistentes virtuais que têm a capacidade de se passar por pessoas de fato e, dependendo do tipo de público-alvo, você tem a interpretação e o entendimento de estar lidando com uma pessoa, mas, de fato, é um robô digital. Você consegue hoje trocar um conteúdo de *streaming* de um vídeo por um conteúdo pelo qual você não é quem está dizendo e nem exatamente o que você está falando, justamente como forma de ludibriar as pessoas e poder tirar vantagem sobre isso.

A própria impressão 3D, ou seja, a capacidade de você construir componentes baseados... Então, você começa a ter espionagem e formas de obter acesso a informações e como criar aquilo justamente com fins não de desenvolvimento, mas

como ataque. Você começa a passar por toda uma geração de especulações sobre o desenvolvimento da melhor tecnologia para poder embarcar e levar pessoas e outras coisas para outros mundos. Até o carro foi para lá, né? Então, assim, o carro também já está viajando por lá.

Mas, no final das contas, o que conta aí é que o *software* está comendo o mundo. Se a gente for observar, como foi dito anteriormente pela colega, o grande desafio é como a gente engenhar os *softwares* adequadamente para que tenham os elementos de segurança adequados para que, de fato, você estabeleça um equilíbrio entre a conveniência e a segurança. É que esse é o desafio, né? Segurança demais gera pouca conveniência; conveniência demais normalmente fragiliza a segurança. Então, achar esse equilíbrio de fato é o desafio para a sociedade que temos.

Aqui, como exemplo, é um tipo de carro e aqui mostra a linha evolutiva do processo de evolução de *software*. Na década de 70, *software* representava quase nada nesse carro. Quando a gente vai no começo dos anos 2010 ali, ele já representava 30% dos componentes do veículo, ou seja, *software* é manipulável, *software* é acessível e manipulável à medida que você tenha capacidade de fazer isso.

Outro aspecto importante é que a longevidade das pessoas está aumentando. Então, você tem pessoas com mais ou menos cultura digital lidando com uma cultura altamente disponível.

Voltamos para a quarta revolução industrial e de que forma isso afeta o nosso dia a dia, justamente por conta dessa disponibilidade e facilidade de uso da tecnologia. Ela não bem implementada ou sem os elementos de segurança cria situações de risco para a própria sociedade.

Hoje você está trabalhando em uma economia compartilhada, em que várias pessoas se juntam, em várias partes do mundo, para desenvolverem tecnologia. Essa tecnologia é para o bem ou para o mal. A gente conhece a Deep Web, conhece uma série de situações em ambientes que, na verdade, usam a tecnologia e não têm propósito positivo efetivamente. E a gente começa a imaginar como essa tecnologia vai interferindo, cada vez mais, no nosso dia a dia. Nas próprias cidades inteligentes, nas *smart cities*, a combinação de tecnologias que você tem, de *hardwares e softwares*, para poder criar conveniências e facilidades para o dia a dia do cidadão também são elementos, pontes e focos de ataque que podem, de fato, interromper o funcionamento de uma cidade, de uma operação ou de ambientes de infraestruturas altamente sensíveis a isso.

Então, a gente começa a dizer e começa a perceber, cada vez mais, o que são os *enablers*, ou seja, aqueles elementos vetores que massificam e que criam a economia colaborativa. Você tem IoT, sensores, *big data*, comunicações, pagamento *peer-to-peer*, você tem *machine-to-machine*, comunicação entre máquinas e os próprios micropagamentos. São desafios que necessariamente precisam ter elementos de segurança para suportar.

E onde isso tudo entra no contexto? A gente tem tecnologias cada vez mais virtuais, físicas, mais transparentes ou mais fáceis de serem visualizadas, mas todas elas fortemente desenvolvidas e baseadas em *softwares*, o que cria desafios para quem desenvolve *softwares* e para quem utiliza *softwares* como forma de desenvolvimento econômico.

Voltando para o nosso ponto: de que forma a gente enxerga tudo isso? De fato, a gente enxerga a ICP-Brasil como um dos pilares de sustentação do governo eletrônico, pelo qual a iniciativa privada, através da sua entidade, a Associação Nacional de Certificação Digital, vem trabalhando fortemente justamente para o desenvolvimento dessa tecnologia e massificação do seu uso. Se a gente for levar a quantidade de soluções que hoje fazem uso dos certificados, também é importante pensar na evolução do uso da tecnologia ampliando os elementos de segurança pelos quais as infraestruturas físicas e lógicas hoje são implementadas para que você possa expandir cada vez mais o uso dessa própria tecnologia e de outras que se compõem.

Na verdade, não existe uma tecnologia melhor do que a outra, o que existe é a melhor combinação delas, justamente como forma de mitigação dos seus riscos. E quando a gente pensa em por que o certificação digital, o ICP-Brasil especificamente, é importante...Na verdade, ele, sim, ajuda também a coibir, ou pelo menos a dificultar, ataques cibernéticos, garante a autenticidade em termos de autoria de documento, garante a você a integridade sobre a informação - a manipulação da informação gera dados duvidosos e críticos - , interoperabilidade e, de fato, baixa dependência sistêmica em função do tipo de infraestrutura que a gente tem hoje. Então, a gente pode dizer que, fundamentalmente, o grande desafio da certificação digital, de fato, é uma organização dos serviços públicos e da atribuição da segurança como elemento extremamente importante dentro desse processo nas transações eletrônicas.

A certificação digital garante, como a gente promove isso, a própria autenticidade dessas transações baseada nessa tecnologia. Daí a importância que enxergamos no uso da certificação também como um vetor, como um elemento, como uma infraestrutura importante na hora em que se pensa em segurança para o nosso País.

Claro que o objetivo é reduzir índices de fraudes, ter maior rastreabilidade - esse é um elemento importante da certificação. Ela afere a rastreabilidade pelo uso de uma transação. O login/senha não necessariamente têm dependência de sistemas. Quando você usa o certificado você consegue ter uma rastreabilidade sobre o uso, e isso ajuda a detectar ataques e a poder,

de alguma forma, criar políticas melhores de proteção aos dados. Obviamente, tudo isso objetivando o uso e a expansão do governo digital.

Como diria ele - apenas mais uma coisa para encerrar dentro do meu tempo -, a segurança da informação também passa pelo processo de cultura. Todas as empresas, de um jeito ou de outro, têm a sua PSI, a sua Política de Segurança da Informação. Deveriam também ter um programa de segurança para o cidadão. Como pelo colega foi mencionado, há um material que é disponível já para conhecimento, para a cultura, mas as escolas deveriam inserir a segurança da informação como um elemento importante. A gente aprende a não atravessar a rua quando tem carro, a gente aprende uma série de coisas, mas deveria aprender também a usar os recursos disponíveis de informática e de informação de forma segura para que, justamente, a gente não se torne vetores de ataques impróprios.

Mas, como tudo continua mudando, o Prof. Custódio mencionou, a próxima revolução e o grande desafio, sem dúvida alguma, é a computação quântica. Por maior criptografia que utilizemos hoje, temos que trabalhar no desenvolvimento dos algoritmos pós-quânticos, no desenvolvimento dessa criptografia, para que, de fato, a gente possa conseguir evoluir com os processos de segurança. A criptografia, hoje, tem o seu estágio de maturidade, mas efetivamente a gente tem que continuar investindo no processo para poder desenvolver elementos de segurança mais adequados para a criptografia, para a anonimização e para a garantia do direito do cidadão à privacidade. A própria Lei Geral de Proteção de Dados tem aspectos importantes que passam pelo tipo de uso da criptografia como elemento importante de segurança também.

Como diria Peter Drucker, o planejamento de longo prazo não lida com decisões futuras, mas com o futuro das decisões presentes. Então, isso é extremamente importante quando a gente pensa em um plano, de fato, de desenvolvimento e proteção da segurança cibernética.

Muito obrigado.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Agradeço as palavras proferidas pelo Sr. Márcio da Silva Nunes.

Agora concedo a palavra ao Sr. Ilton Duccini, Diretor de Segurança Digital da Empresa Telefônica Brasil e Professor da Universidade Estadual de Campinas, a Unicamp.

O SR. ILTON DUCCINI (Para exposição de convidado.) - Um bom-dia a todos!

Gostaria de agradecer o convite tanto ao Comando de Defesa Cibernética quanto ao Senado. Para mim é uma honra poder falar desse tema, um tema ao qual venho me dedicando nos últimos 15 anos.

Gostaria de ressaltar já inicialmente que também me coloco à disposição para novas rodadas de discussão sobre esse assunto, porque a segurança cibernética é um tema que requer perseverança. Na verdade, requer muita perseverança para que você consiga conscientizar as pessoas, mobilizar as pessoas e, consequentemente, os investimentos necessários para isso.

Hoje pretendo apresentar a segurança cibernética sob duas óticas.

Em primeiro lugar é preciso ter em mente que esse tema é um tema de perigo real e iminente. A gente não está falando aqui de ciência de foguete, a gente está falando de coisas que, de fato, já têm acontecido no mundo como um todo e que requerem investimentos para a mitigação desses riscos.

Um segundo viés é justamente a possibilidade de tratar esses investimentos para o desenvolvimento de novas tecnologias, de tecnologias nacionais que possam, inclusive, gerar dividas para o País. Eu tenho acompanhado muito de perto empresas e empreendedores brasileiros que têm desenvolvido tecnologias nacionais e que já têm começado a exportar essas tecnologias para outros países da América Latina, inicialmente. Então, acho que a gente tem uma grande oportunidade.

A gente tem aí, como exemplo, tudo o que Israel tem investido nesse tema de segurança cibernética e como eles têm monetizado esse aspecto. Israel tem seguido o exemplo do que os Estados Unidos já começaram a fazer desde a década de 1960, de 1970. Ainda há tempo de começarmos a investir nisso, mas tem que ser agora. *(Pausa.)*

Eu também estava acompanhando aqui os comentários das pessoas que estão acompanhando a audiência pública pela internet. Eu vejo que há um público com conhecimento bastante heterogêneo sobre esse assunto. Então, apenas para contextualizar, é importante ressaltar que algum tempo atrás o aspecto de guerra cibernética era contextualizado muito na questão de Estado-Nação contra Estado-Nação. Hoje esse conceito caiu por terra e, na verdade, aquele conceito que nós tínhamos de proteção de fronteiras, de proteção de perímetro, quando a gente fala de guerra cibernética, ele já não existe mais. Nós temos atores individuais, grupos de cibercriminosos que podem, sim, causar grande disruptura em todo o sistema de comunicação, em todo o sistema de internet de um determinado país.

Eu vou falar, inclusive, de um de um exemplo que aconteceu na Estônia e que é considerado o primeiro evento de guerra cibernética no mundo e, inclusive, a partir desse evento, foi criado o Centro de Excelência em Defesa Cibernética da Otan, o CCDCOE. Eu utilizei muito material CCDCOE para que, de uma forma pragmática - é um material de estudo que desenvolvi -, nós tenhamos uma visão clara de como devemos conduzir a nossa estratégia de defesa cibernética nacional.

Tudo o que tem sido feito hoje... Eu, inclusive, participei recentemente - tive o prazer de participar - do Exercício Guardião Cibernético, e a percepção que eu tenho é que hoje nós temos as pessoas certas no lugar certo. Então, estamos num bom caminho, estamos com a fundação começando de uma forma bem estruturada, e isso traz um certo alívio. E é uma coisa de que muitas pessoas não têm visão, do esforço que está sendo feito em relação a isso.

Mas a gente não pode parar por aqui, a gente tem que olhar para frente, e a gente também não pode cometer o erro de achar que o pior cenário que nós poderíamos sofrer é o que, por exemplo, aconteceu na Estônia. Esse foi o primeiro cenário. Nós temos outros cenários que aconteceram - vou mostrar numa linha do tempo em seguida -, mas eu diria que o pior ainda está por vir.

Aqui é um vídeo. A gente não vai ter tempo para falar, mas é um vídeo de um almirante que é o diretor responsável pela agência de inteligência americana em que ele está falando de alguns aspectos que ele considera como críticos quando falamos de defesa cibernética e de guerra cibernética. E ele traz um cenário muito interessante: de todas as preocupações que ele possui, a maior não é exatamente de indisponibilização de um sistema, não é exatamente de um vazamento de uma base de dados, muito pelo contrário. O maior receio que ele tem é que dados sejam manipulados e adulterados, e que isso seja feito de uma forma muito sublime e que não seja percebido, dados de pessoas, dados de Estado. O receio é que isso não seja percebido e que se rompa completamente a cadeia de integridade dessas informações e que seja muito difícil identificar o ponto em que isso ocorreu e como voltar atrás. Então, é um ponto interessante que a gente precisa avaliar também.

Aqui, na linha do tempo, um dos principais casos considerados de guerra cibernética divulgados - há muitos outros que acontecem e que sequer são divulgados. O mais conhecido do público em geral nem é o caso da Estônia, é o caso do Stuxnet, que foi justamente um *malware* que afetou o sensor de temperatura dos geradores de enriquecimento de urânio de uma Indústria nuclear iraniana, e que quase colapsou toda aquela indústria nuclear. E há vários outros casos que vêm acontecendo aí ao longo do tempo.

Então, como eu falei, a gente está falando de perigo real e iminente, que pode estar acontecendo agora ou pode começar acontecer amanhã. Então, essa é uma preocupação muito importante.

Nós vamos nos preocupar com isso? Não, porque preocupar não é uma ação tática. Ação tática é atacar, é defender, é capacitar, é destruir, é evadir, dissuadir. Então, para isso é que nós precisamos, de fato... Existe a Estratégia Nacional de Defesa com os tópicos específicos, e a defesa cibernética é um dos três principais pilares dessa estratégia.

Nós precisamos complementar isso com ações reais, com grupos de trabalho que vão efetivamente implementar essas ações, definir o tempo que vai ser levado para isso e o investimento que vai ser requerido, ou seja, colocar em prática tudo o que tudo que precisa ser feito além das ações já existentes.

Um ponto que destaco nessa questão: termos o Estado como um patrocinador de tudo isso é importantíssimo. Devemos ter também regulamentações robustas em relação a esse assunto. Nós temos hoje um decreto de lei, que é a Política Nacional de Segurança da Informação, que, neste momento, abrange apenas as entidades públicas. Nós precisamos evoluir no sentido de que a Política Nacional de Segurança da Informação também tenha uma abrangência em relação às entidades privadas e de passarmos a ter, pelo menos no início, a regulamentação específica por setor para aqueles setores que pertencem às infraestruturas críticas. Por exemplo, o setor financeiro, o setor de energia, o setor nuclear, o setor de telecomunicações e, gradativamente, ir expandido esse aspecto.

Nós precisamos ter em mente quais são as prioridades, ter um mapeamento claro de quais são os nossos riscos nesse momento e investir naquilo que é mais prioritário, porque o contexto é extremamente amplo, extremamente complexo e, se a gente realmente quiser olhar a partir do todo, vai ser muito difícil materializar alguma ação. Então, há um conceito que a gente chama de "fatiar fininho": vamos olhar aquilo que realmente tem um maior risco e que requer uma prioridade maior, está certo?

Indo já direto aos tópicos principais, que nós devemos considerar dentro da nossa estratégia: um viés de governança, um viés de gestão de riscos. Então, trata-se de ter claramente mapeados quais são os riscos não só para o Governo e Forças Armadas, mas para a iniciativa pública e para a iniciativa privada.

É preciso ter todo o aspecto estruturado de resposta a incidente e resiliência, como foi bem observado aqui. É impossível ter uma segurança cem por cento. Segurança é um objetivo negativo, não é um objetivo positivo. Para um objetivo positivo,

eu consigo definir claramente aquilo que eu vou fazer, para evitar; para um objetivo negativo, eu tenho milhares de possibilidades de que aquilo possa acontecer e é impossível investir para cobrir as milhares de possibilidades. Então a gente tem que assumir o risco em alguns casos, considerar que é possível, sim, que um ataque seja materializado, e a questão é: como identificar rapidamente e responder rapidamente a esse ataque. Por isso, o aspecto colaborativo do ecossistema de segurança é muito importante.

Então, o Exercício do Guardião Cibernético trouxe esse viés, esse princípio de criação de um ecossistema e esse princípio de colaboração entre os setores de infraestrutura crítica. O que a gente precisa agora é colocar aquilo no dia a dia, não depender apenas do exercício simulado, mas praticar aquilo no dia a dia, em todo o aspecto de equipar, capacitar e conscientizar não só os profissionais. A gente tem uma escassez de profissionais conhecedores do tema de segurança cibernética não só no Brasil como no mundo. Recentemente, foi criada a Escola Nacional de Defesa Cibernética, e a gente precisa ampliar a parceria entre as Forças Armadas, a Academia e a sociedade civil. Temos que nos calcar nesses três pilares, ampliar a capacitação de profissionais para esse setor e, principalmente, conscientizar a sociedade como um todo. Isso é fundamental, e já foi mencionado aqui.

Há todo o aspecto de legislação e regulamentação, que eu já antecipei. Infelizmente, sem uma legislação e sem uma regulamentação robusta, só na base da boa-fé, é muito difícil que a gente consiga evoluir de forma clara e efetiva em relação a esse assunto. E, como eu já falei, o sistema de colaboração e cooperação.

Não vou passar por todos os pontos, mas eu tenho aqui uma visão de pontos-chave, pontos críticos, para cada um desses tópicos.

Dentro de governança, a gente precisa trazer claramente qual é o nosso plano de implementação. De maneira geral, nós temos uma noção do que precisamos fazer, agora é questão da priorização e da implementação das ações. Vamos começar pela questão do maior investimento em relação à formação? Vamos começar pela questão de um mecanismo, de formas, de ferramentas de compartilhamento de informações em caso de incidentes? Então, a gente precisa ter isso claro.

Quanto à gestão de riscos, como eu já havia comentado: primeiro, estabelecer uma metodologia clara de gestão de riscos. Hoje, cada empresa, cada entidade, cria a sua própria metodologia de risco. Existem *frameworks* de metodologia de risco no mundo inteiro que a gente pode adotar como um padrão nacional, existe o *framework* de cibersegurança do Nist, que não aborda especificamente uma gestão de risco, mas que a gente pode considerar, para o aspecto de mapeamento...

(Soa a campainha.)

O SR. ILTON DUCCINI - ... dos controles e daquilo que precisa ser implementado, e, em resposta a incidentes, um dos pontos que nós já fazemos hoje é justamente o exercício de segurança cibernética, que é fundamental. Precisamos cada vez ampliar mais esse exercício, ter outros setores da economia participando.

Dentro da capacitação, como eu já falei, a tríade entre a Academia, o setor público e privado e as Forças Armadas para fortalecer esse aspecto, haver o currículo da cibersegurança no Brasil.

Legislação: todos os setores carecem de uma legislação específica, de uma regulamentação específica. Alguns já estão trabalhando nisso, o que a gente precisa fazer é acelerar a publicação dessas regulamentações.

E a questão do ecossistema: ter um alinhamento de esforços. E a gente não pode ter a visão só nacional; a gente tem que ter a noção de que, como eu falei inicialmente, o tema de segurança cibernética extrapola fronteiras, extrapola barreiras, e nós temos que também ter uma colaboração muito forte com outros países, com empresas que estão fora do Brasil.

Bom, era isso que eu tinha para falar para os senhores. Fico à disposição para qualquer dúvida.

Muito obrigado pela oportunidade.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Agradeço as palavras do Sr. Ilton Duccini.

Agora eu concedo a palavra ao Sr. Eduardo Bergo.

O SR. EDUARDO BERGO (Para exposição de convidado.) - Bom dia a todos! Bom dia, Senador! Bom dia, presentes aqui, autoridades!

É com grande prazer que eu venho aqui representar a Febraban. Eu sou Diretor na Febraban dessa parte de segurança cibernética e sou Diretor no Banco do Brasil também na parte de segurança.

A Febraban é uma entidade que congrega 119 bancos, instituições, e essas instituições são responsáveis por 28% dos ativos financeiros do País, então quase 100% dos ativos financeiros ali estão nessas instituições que são representadas pela Febraban, a Federação Brasileira de Bancos.

Aqui eu trago um pouco dos números, das transações financeiras que são realizadas nos bancos pelos clientes. A gente vê, como foi dito anteriormente, que grande parte das operações financeiras está sendo realizada hoje através do *mobile*. Quem

daqui, nesta sala, foi a uma agência bancária ultimamente? Qual foi a última vez que você foi a uma agência bancária para fazer uma transação financeira? E a gente vê um crescimento muito grande nas transações no *mobile* e também uma queda nas transações tradicionais na internet, ou seja, o *mobile* sendo o canal principal para a realização de transações. Para se ter uma ideia: a quantidade de contas ativas com movimentação no *mobile* e *internet banking* chegou a 123 milhões em 2018 e, em 2018 também, foram feitos 2,5 bilhões de pagamentos de contas e transferências pelo *mobile banking*.

O marco regulatório, aquilo em que os bancos se baseiam. Há vários regulamentos em que os bancos se baseiam, mas os principais são esses aí. Os bancos atinam para a Resolução 4.658 do Conselho Monetário Nacional, que é supervisionada pelo Banco Central, e também a Instrução da CVM 612, além da Lei Geral de Proteção de Dados, que é uma preocupação grande que os bancos têm, e ela passa a vigorar agora em 2020.

Então, os bancos, como foi dito anteriormente, hoje têm um olho muito forte para essa questão da segurança cibernética, mesmo porque hoje o cofre digital é mais importante do que o cofre físico das agências. E as principais ameaças em que os bancos se veem são estas: a engenharia social, ou seja, você tentar obter as credenciais da pessoa por meio de golpes ou outros meios; *malwares*, *ransomwares*, *hacking*, *defacement* e Ataque Distribuído de Negação de Serviço. Essas são as principais ameaças com que os bancos se defrontam hoje.

Isso aqui já foi dito, não vou ser repetitivo, mas a gente traz esse risco, essas ameaças. Então, ali: Equifax. A Equifax é equivalente ao Serasa brasileiro. A Equifax é uma prestadora de serviços também lá nos Estados Unidos: sofreu um ataque *hacker* e dados de 143 milhões de pessoas foram expostos; Facebook: a gente também tem notícias lá relacionadas ao Facebook, ao Yahoo, a hotéis e a outros mais. E também há a questão de algumas nações: bancos no Peru, no Chile, no Equador, aqui, e outros bancos; Netshoes, aqui no Brasil também. Bancos no Brasil tiveram problemas graves relacionados a essa questão de incidentes cibernéticos.

E o que que os bancos têm feito para trabalhar essa questão? Na Febraban, nós temos uma comissão, que é a Comissão de Segurança Cibernética. Ela é composta por diretores de bancos, e lá são discutidas as questões relacionadas a essa proteção, a gente troca informações, porque nesse campo não existem concorrentes. No Brasil, para vocês terem uma ideia - foi dito isso anteriormente também -, o setor bancário, depois do governo, é o setor que mais investe nessa parte de tecnologia. Então, no Brasil, ele equivale ao investimento do governo e, no mundo, ele está em segundo lugar. O setor bancário no Brasil é um dos mais evoluídos do mundo; como nós também temos do outro lado um pessoal bem criativo, procuramos nos proteger.

E, assim, investimentos em solução de segurança: a gente traz aqui uma síntese desses investimentos. Os bancos investem muito na sua infraestrutura de segurança, então nós temos lá: proteções específicas; dados, monitoramento e *feeds*; acesso, identidade e criptografia; redes (proteção de redes), *endpoints*/estação de trabalho e teste de vulnerabilidade. Tudo isso compõe uma disciplina nos bancos que a gente chama Inteligência e Segurança Cibernética.

Basicamente, a estrutura dos bancos, em termos de segurança, respeita esse desenho aí, esse modelo. No entanto, os bancos não podem se preocupar somente com a questão da sua segurança, da segurança do próprio banco: a gente também investe muito na segurança do cliente, das pessoas que se utilizam dos bancos. Então, nós investimos em tecnologias: nós temos tecnologias de utilização de QR Code, de *tokens*, o próprio cartão com *chip*, com o uso de biometria. Os bancos estão fazendo uma pesquisa muito forte no uso de biometria, não só a biometria física, mas também a biometria com o uso para identificação comportamental, de como se utilizam os *devices*. Então, há uma série de investimentos em termos de tecnologia. Isto foi divulgado recentemente: os bancos têm um investimento muito forte em tecnologia e, desse investimento em tecnologia, os bancos investem pesado em segurança.

Os bancos também procuram realizar parcerias. Então, nós temos uma parceria com a Polícia Federal no que diz respeito à investigação dos crimes. Então, a gente trabalha junto com a Polícia Federal num convênio para ajudar na elucidação do crime. Esse projeto se chama Projeto Tentáculos.

A gente também tem alguns desafios novos. Ou seja, a gente está olhando para o futuro e tem alguns desafios. *Open banking*, por exemplo, é o compartilhamento de plataformas entre bancos. A abertura de contas digitais hoje é uma realidade. Para vocês terem uma ideia: uma moça que trabalha lá em casa, até um tempo atrás, não tinha conta corrente; eu mostrei para ela como abrir uma conta digital no Banco do Brasil. Ela abriu a conta digital, o cartão chegou na casa dela e ela não foi numa agência. Então, hoje você tem esse tipo de realidade, o que exige um investimento muito forte dos bancos na identificação de quem está do outro lado transacionando. Então, é um investimento muito pesado.

Além daqueles dispositivos que eu coloquei para vocês há pouco, os bancos também investem muito em *analytics* e na inteligência artificial para tentar identificar o comportamento, quem é que está por trás daquelas transações que são realizadas em canais virtuais.

Pagamentos instantâneos: é outro desafio, é um novo meio de pagamento que está surgindo. Na China, isso é bem difundido. Os bancos no Brasil já usam, já têm isso disponibilizado para os correntistas, para os clientes. Então, pagamentos instantâneos. Os bancos também já começaram a trabalhar com tecnologia de *blockchain* para certificar transações entre os bancos, fazer a certificação de transações entre os bancos. E isso tudo compõe um plano estratégico na Febraban.

O Guardião Cibernético também é um exemplo, é uma iniciativa do CDCiber que as instituições financeiras apoiam, porque as instituições financeiras estão cientes da importância do sistema financeiro para a segurança do País. Então, nós também apoiamos o Guardião Cibernético.

De uma forma bem resumida, qual é a posição da Febraban em relação a uma política nacional de segurança cibernética? Nós entendemos que o País deve investir: num documento único nacional e digital, a exemplo do DNI, Documento Nacional de Identificação - esse documento digital é fundamental e, se estiver com um certificado digital embutido, seria muito importante -; na instituição de uma política nacional de segurança cibernética incluindo o setor financeiro, pela importância do setor financeiro, em linha com as regulamentações do Banco Central, CVM e da Lei Geral de Proteção de Dados também; no reforço da importância de estruturas especializadas para investigação de crimes cibernéticos - a gente entende que não basta a gente proteger, mas a gente tem que saber quem é que está do outro lado tentando atacar o sistema como um todo; e, também, num apoio, como foi dito anteriormente aqui, para a criação de academias voltadas para a formação de profissionais especializados -os bancos investem muito em pesquisa, os bancos estão investindo muito em pesquisa; os bancos investem em pesquisa aqui no País, mas também muito em pesquisa no exterior; então, seria muito importante a gente investir aqui no País, numa academia aqui no País para a formação de profissionais especializados -; e na implementação de testes integrados de resiliência cibernética, a exemplo do Guardião Cibernético, que tem tido um sucesso muito grande.

Então, esses são os pontos que eu gostaria de trazer aqui em nome da Febraban.

Quero agradecer mais uma vez o espaço que foi aberto aqui para os bancos para que a gente pudesse expor. Estou à disposição.

Muito obrigado, Senador.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Eu é que agradeço as palavras do Eduardo Bergo.

Vamos, agora, passar para deliberação da ata da reunião anterior.

Proponho a dispensa da leitura e a aprovação da ata da reunião anterior.

As Sras Senadoras e os Srs. Senadores que aprovam permaneçam como se encontram. *(Pausa.)*

Aprovado.

Quero passar algumas notas internacionais.

Referente à França. Faleceu, há poucas horas, Jacques Chirac, ex-Chefe de Estado francês. Tinha 86 anos e sua carreira política é considerada uma das mais excepcionais da França. Chirac foi Primeiro-Ministro, Ministro e Prefeito de Paris e, como Chefe de Estado, governou o país por dois mandatos entre 1995 e 2007.

Sobre o Reino Unido. A decisão do Primeiro-Ministro do Reino Unido, Boris Johnson, de suspender o Parlamento britânico por cinco semanas foi considerada ilegal e nula pela Suprema Corte. O Parlamento foi reaberto e Johnson tem até o dia 31 de outubro para encontrar uma solução para a saída do Reino Unido da União Europeia, com ou sem um acordo entre as partes. Sobre a ONU. O nosso Presidente da CRE, Nelsinho Trad, acompanhou o Presidente Jair Bolsonaro na Assembleia Geral da ONU e destacou pontos importantes do seu discurso, entre eles a adoção de políticas de aproximação com países que se desenvolveram e consolidaram as suas democracias, porque o Brasil é um país aberto ao mundo em busca de parcerias com todos os que tenham interesse de trabalhar pela prosperidade, pela paz e liberdade.

Nosso Presidente mencionou ainda uma agenda internacional que deve seguir até o final do ano para reafirmar a importância do Brasil no cenário mundial e retomar as relações com importantes parceiros, como Suíça, Estados Unidos, Chile, Israel e Argentina.

Esse foi um momento histórico para todos os brasileiros. Foi possível mostrar ao mundo que o Brasil é soberano em seu território e nas decisões governamentais sobre suas riquezas e sobre suas riquezas naturais. Nosso País tem um potencial infinito e o nosso horizonte é a prosperidade. *(Pausa.)*

Desculpe, Senador Amin, eu não tinha observado que o senhor já estava sentado aí. O senhor gostaria de fazer algumas considerações?

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Gostaria só de fazer um agradecimento.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Claro.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Em primeiro lugar, a V. Exa., que supriu... Hoje foi um dia muito tumultuado aqui. Tivemos duas sessões no Plenário, além da sessão prevista. Tivemos uma sessão extraordinária de manhã para deliberar e agora estamos tendo a sessão de promulgação da emenda à Constituição relativa à cessão onerosa e, nesse ínterim, tivemos uma sessão solene em homenagem à amizade Brasil-Palestina, que foi proposta por mim e eu tive que presidir. Além disso, estamos tendo uma sessão igualmente muito delicada na Comissão de Serviços e Infraestrutura sobre uma fusão reversa CGTEE-Eletrosul.

Então, eu peço desculpas por não ter podido acompanhar pessoalmente tudo. Agradeço muito a V. Exa. por ter coberto tanto a minha ausência quando a do nosso Senador Nelsinho Trad, que esteve, inclusive, na posse do Procurador-Geral da República. Portanto, a manhã foi muito tumultuada.

Eu gostaria só de agradecer muito especialmente aos integrantes dessa segunda mesa, da qual eu apenas pude ter notícia. Acho que cumpriu-se o objetivo desta fase do nosso plano de trabalho de avaliação da política pública. Esse assunto não vai terminar hoje. Teremos uma nova reunião, que V. Exa. certamente vai convocar, muito especial para a próxima semana, dia 3 de outubro. Mas eu não posso deixar de agradecer principalmente a sua presença aqui, que preservou a integridade do objetivo desta reunião, que foi cumprido graças à participação de todos os oito convidados.

Muito obrigado.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Eu é que agradeço as palavras do nosso mestre aqui no Senado, Esperidião Amin, uma pessoa fantástica, com conhecimento fora do normal. Sinto-me honrado pelas palavras. Sempre que precisar, estarei à disposição, porque são trabalhos importantíssimos para a Nação, e a gente tem que se virar para poder atender.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Desta vez, eu fiz o pedido como seu eleitor. *(Risos.)*

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Agradeço, mais uma vez, a participação das Sras. e Srs. Senadores, das autoridades aqui presentes, especialmente a dos nossos convidados: Sr. Marcelo Buz, Diretor-Presidente do Instituto Nacional de Tecnologia da Informação; Sr. Fabio Reis Cortes, Gerente de Arquitetura e Segurança de Tecnologia da Informação do Operador Nacional do Sistema Elétrico; Sr. Marcos Allemand Lopes, Gerente de Departamento de Gestão da Segurança da Informação e da Continuidade de Negócios do Serviço Federal de Processamento de Dados; Sr. Ricardo Felipe Custódio, Professor Supervisor do Laboratório em Segurança da Computação da Universidade Federal de Santa Catarina; Sra. Cristine Hoepers...

A SRA. CRISTINE HOEPERS (*Fora do microfone*.) - Estou até sem voz para falar.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC. *Fora do microfone*.) - Temos uma grande família Hoepers em Forquilhinha, Santa Catarina.

A SRA. CRISTINE HOEPERS (*Fora do microfone*.) - É de lá.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - É de lá.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - É a origem? *(Fora do microfone.)*

O primeiro Prefeito foi Paulo Hoepers.

A SRA. CRISTINE HOEPERS (*Fora do microfone*.) - É primo do meu pai.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - E a minha querida amiga Mirian Berkenbrock Hoepers.

O SR. PRESIDENTE (Marcos do Val. PODEMOS - ES) - Cristine Hoepers é Gerente-Geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil; Sr. Márcio da Silva Nunes, Vice-Presidente da Associação Nacional de Certificação Digital; o Sr. Ilton Duccini, Diretor de Segurança Digital na Empresa Telefônica Brasil e Professor da Universidade Estadual de Campinas (Unicamp); e Sr. Eduardo Bergo, Diretor Setorial da Comissão Executiva de Segurança Cibernética da Febraban junto ao Banco do Brasil.

Agradecendo a todos pela presença, declaro encerrada a presente reunião.

(Iniciada às 9 horas e 28 minutos, a reunião é encerrada às 11 horas e 59 minutos.)