CÂMARA DOS DEPUTADOS

DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

CPI - CRIMES CIBERNÉTICOS			
EVENTO: Audiência Pública	REUNIÃO Nº: 1843/15	DATA: 24/09/2015	
LOCAL: Plenário 3 das Comissões	INÍCIO: 10h29min	TÉRMINO: 12h38min	PÁGINAS: 46

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

RODRIGO ORTIZ D'ÁVILA ASSUMPÇÃO - PRESIDENTE DA EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA SOCIAL — DATAPREV.
CRISTIANO ROCHA HECKERT - SECRETÁRIO DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO DO PLANEJAMENTO.
ADRIANO CABRAL VOLPINI - DIRETOR SETORIAL DA COMISSÃO EXECUTIVA DE PREVENÇÃO A FRAUDES DA FEDERAÇÃO DOS BANCOS BRASILEIROS — FEBRABAN.
CLAUDIA MARIA DE ANDRADE - COORDENADORA-GERAL DE TECNOLOGIA DA INFORMAÇÃO DA RECEITA FEDERAL.

SUMÁRIO

OBSERVAÇÕES

Houve exibição de imagens.
Houve expressões ininteligíveis.
Houve exibição de imagens.

O SR. PRESIDENTE (Deputado Leo de Brito) - Bom dia!

Declaro aberta a 15ª reunião ordinária de audiência pública da CPI dos Crimes Cibernéticos.

Encontra-se à disposição dos senhores membros a cópia da ata da 14ª reunião, realizada no dia 22 de setembro de 2015.

Não temos membros aqui, então dispensa-se a leitura.

Deputada Conceição Sampaio, faz-se necessária a leitura da ata?

A SRA. DEPUTADA CONCEIÇÃO SAMPAIO - Sr. Presidente, eu peço a dispensa da leitura da ata.

O SR. PRESIDENTE (Deputada Mariana Carvalho) - Certo. Fica dispensada a leitura da ata, a pedido da Deputada Conceição Sampaio.

Em discussão a ata. *(Pausa.)*

Não havendo quem queira discuti-la, em votação. *(Pausa.)*

Aprovada a ata.

Expediente. Comunico o recebimento das seguintes correspondências: declarações assinadas pelos jornalistas Carlos Alberto Sardenberg, Miriam Azevedo de Almeida Leitão e Maria Júlia dos Santos Coutinho Moura e pela atriz Carolina Dieckmann, comunicando-nos a impossibilidade de comparecerem à CPI em razão de compromissos profissionais, elogiando a finalidade da CPI e reafirmando terem sido vítimas de crimes virtuais. As declarações encontram-se à disposição na Secretaria e poderão ser encaminhadas aos membros que solicitarem.

O SR. DEPUTADO SANDRO ALEX - Sr. Presidente, gostaria de solicitar cópias.

O SR. PRESIDENTE (Deputado Leo de Brito) - Pois não. Peço à Secretaria que disponibilize as cópias.

Ordem do Dia. Não haverá apreciação de requerimentos na reunião de hoje.

Antes de iniciar a audiência, reitero convite às Sras. e aos Srs. Deputados para participarem da audiência pública que a CPI vai realizar no próximo dia 5 de outubro, segunda-feira, na cidade de Natal. A CPI vai se deslocar até Natal para verificar o combate à pornografia infantil, atendendo a solicitação do Sub-Relator dos direitos das crianças e adolescentes, Rafael Motta — Requerimento nº 31, de 2015. O Deputado Rafael Motta não se encontra para falar.

Solicito, então, que os membros confirmem a presença e informem à Secretaria da CPI para que sejam adotadas as providências da missão oficial.

Convido também as pessoas que acompanham os trabalhos da CPI, as pessoas aqui presentes e também as que nos acompanham pelas transmissões no portal *camara.leg.br* que visitem, participem e deixem sua opinião na comunidade virtual da CPI. O acesso também é feito pelo *câmara.leg.br*. Entrando no portal do e-Democracia, procure o botão da comunidade virtual da CPI dos Crimes Cibernéticos. Na comunidade há um fórum de discussão de que os internautas poderão participar, interagir, e os Deputados poderão responder aos internautas, postando textos e vídeos. Há um aplicativo para publicação de fotos e também uma ferramenta que possibilita interatividade nas audiências da CPI.

Audiência pública. A audiência pública de hoje trata do enfrentamento dos crimes virtuais nos grandes sistemas do Governo e também no sistema bancário.

Convido para tomarem assento à Mesa o Presidente da Empresa de Tecnologia e Informação da Previdência Social — DATAPREV, o Sr. Rodrigo Ortiz D'Avila Assumpção *(palmas)*; o Sr. Cristiano Rocha Heckert, Secretário de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão — SLTI *(palmas)*; o Sr. Adriano Cabral Volpini, Diretor Setorial da Comissão Executiva de Prevenção a Fraudes da Federação Brasileira de Bancos — FEBRABAN *(palmas)*; e a Coordenadora-Geral de Tecnologia da Informação da Receita Federal, Sra. Cláudia Maria de Andrade *(Palmas.)*

Esta audiência tem por base o Requerimento nº 17, de 2015, dos Deputados João Arruda e Leo de Brito, e o Requerimento nº 26, de 2015, de iniciativa da Deputada Alice Portugal.

Cada participante disporá de 20 minutos para fazer sua exposição. Após as apresentações, será passada a palavra ao Relator, aos Sub-Relatores e aos autores dos requerimentos por 5 minutos. Os convidados respondem a essas primeiras indagações. Em seguida, respeitada a lista de inscrições, os senhores membros poderão interpelar os convidados por até 5 minutos.

Feitos esses esclarecimentos, passo a palavra ao Sr. Rodrigo Assumpção, Presidente da DATAPREV. V.Sa. dispõe de 20 minutos.

O SR. RODRIGO ORTIZ D'ÁVILA ASSUMPÇÃO - Srs. Deputados e demais presentes, muito obrigado. De antemão, declaro que é a primeira vez que eu participo de uma audiência pública como esta. Então, quero antecipar pedidos de desculpas por erros procedimentais, abordagens indevidas ou desobediência aos ritos, mas é pela ignorância.

Vou falar um pouco rapidamente sobre a DATAPREV. Temos uma apresentação que está sendo distribuída. Acreditamos ser extremamente oportuno este debate. Esse é um tema complexo, que vem sofrendo aceleração no que se refere à preocupação de todas as sociedades. Ele é debatido ao redor do mundo de maneira consistente e constante, e é muito promissor que o Parlamento brasileiro se debruce sobre esses temas.

(Segue-se exibição de imagens.)

Para iniciar, só quero dar uma rápida dimensão da DATAPREV. A Empresa de Tecnologia e Informações da Previdência Social hoje tem os números presentes na tela para oferecer ao Estado brasileiro a sua capacidade de processamento, armazenamento e guarda de dados cruciais para a nossa população. Nós temos 3.854 empregados, estamos em todas as capitais do País, nós contamos com cinco unidades de desenvolvimento e a capacidade de processamento e armazenamento é essa declarada. Somos guardiões das maiores bases de dados do Estado.

A próxima tela mostra os principais clientes. Como vocês podem ver, os grandes órgãos de Governo que lidam com políticas sociais são os nossos clientes e são também, junto com várias instituições financeiras públicas e privadas, beneficiários desse sistema de que estamos falando.

Na próxima tela, nós vemos quatro bandeiras do que comumente se reconhecem como os países que de fato têm implantado de forma consciente uma cultura de segurança da informação: a China, os Estados Unidos, a Rússia e Israel. Não é por acaso que todos esses países têm também o desprazer de enfrentar conflitos armados permanentes há pelo menos toda a sua trajetória ao longo do século XX e XXI. Há uma associação muito forte entre a implantação de cultura de segurança da informação e conflitos armados. Obviamente não é por esse caminho que o Brasil gostaria de adquirir experiência e *know-how* nesse processo, mas esse

é o caminho que demonstrou ter o maior resultado na história da humanidade. Essa contradição é algo importante para reflexão.

No próximo eslaide, nós tentamos abordar algo muito significativo. O Estado brasileiro foi um dos adeptos iniciais de uso intensivo de tecnologia da informação desde o final da década de 60 e do início da década de 70. Isso significa que vários dos nossos sistemas ainda hoje em uso, sustentando funções primordiais de Estado, têm filosofias e procedimentos e códigos e linguagens e tecnologias que vêm ainda dessa época e são compostos por grandes sistemas legados que estão em uso há muito tempo.

A filosofia de defesa desses sistemas focava a fraude do dado. Então, a fraude era percebida como a capacidade de alterar um dado como, por exemplo, o nome de uma pessoa; o tempo de contribuição, no caso da previdência; ou até mesmo as relações de emprego. Esse é o histórico de fraude que vem à nossa cabeça, sobretudo ao final do século passado. Isso mudou radicalmente. Cada vez menos a alteração do dado presente no banco de dados é a questão crucial, e sim o acesso indevido.

E não só a cultura de elaboração desses sistemas vem de outra época, com outra preocupação, como existe também um conflito inerente significativo entre a demanda necessária de ofertar acesso e a demanda necessária de proteger esse acesso para que se dê apenas de modo devido. Então, o grande foco da prevenção hoje é garantir o acesso devido e também impedir que ataques a esse acesso, como de negação de acesso, pedido excessivos de oferta de serviços, não afetem essa prestação de serviço.

No próximo eslaide, expressamos essa preocupação e o desafio de, além de proteger o *data center*, além de proteger a empresa e os próprios acessos, além de assegurar que o acesso dos nossos clientes seja adequado, legítimo, seguro e rastreável, nós precisamos também oferecer acesso cada vez mais amplo e efetivo à população, porque são os seus dados que estão sendo guardados por nós. Então, essa contradição entre proteção e acesso, que é o nosso cotidiano, norteia muitas das práticas de que vamos falar a seguir.

Em termos de ações gerais, nós temos parcerias estratégicas com o CTIR Gov; com a APEGR/MPS, uma unidade especial, associada à Polícia Federal, que o

Ministério da Previdência tem para as suas investigações; com o CERT.br, do Comitê Gestor da Internet. Além disso, temos parcerias muito efetivas e constantes com a Polícia Federal e um grupo especializado em análise de segurança e discussão de conformidade com investimentos contínuos na busca desse alinhamento com as melhores práticas.

Nos últimos anos, os órgãos de controle vêm exercendo uma forte fiscalização, não só nas nossas práticas e políticas de segurança, mas na manutenção dos nossos investimentos continuados nessas tecnologias e nesses investimentos.

Para exemplificar, no próximo eslaide, temos o foco da atuação de 2015 nas ações que estão sendo implementadas na DATAPREV. Um foco importante são os planos de continuidade de negócio, tanto para a DATAPREV quanto para todos os nossos clientes. Então, o que fazer no caso de desastres? O que fazer quando há uma interrupção de serviços?

Além disso, há também uma discussão constante de enfrentamento e correção de vulnerabilidades nos sistemas. Estamos tentando aprofundar o desenvolvimento seguro, para matar no nascimento as vulnerabilidades dos novos sistemas que vão sendo colocados em produção. Também estamos atentos ao controle de acesso entre aplicações, porque o acesso hoje em dia não é apenas de indivíduos a sistemas, mas de sistemas a outros sistemas. Isso também exemplifica elementos que precisam ser controlados e segurados.

Outra ação é o desenvolvimento de cofres de senha que emitem senhas temporárias, fazendo as vezes de uma senha única, para que indivíduos não tenham posse de senhas de infraestruturas críticas. Assim, essas senhas são alocadas de maneira temporária para a correção de um problema, e isso é feito de maneira automática por esses cofres de senha, que são estruturas de *softwares* para gerenciar essas senhas.

Há outras preocupações, como a gestão centralizada de registros e eventos, para que possa haver rastreabilidade em todos os processos; o nosso sistema contínuo de gestão de segurança da informação; a gestão de risco em todos os nossos ativos em tecnologia da informação e comunicação; e uma forte conscientização e capacitação em segurança da informação para todos os nossos

funcionários. Faz mais de 4 anos que há um curso de formação em segurança da informação e comunicação obrigatório para todos os funcionários da empresa, incluindo estagiários e todos os indivíduos que circulam nas nossas dependências.

Com relação ao tratamento de incidentes e vulnerabilidades, esses são alguns dos elementos, para que os senhores possam ter uma ideia de como o processo vem se dando e as medições comparativas. É muito interessante, na segunda parte do quadro, ver que o tratamento de riscos e vulnerabilidades é um processo contínuo — como eu mencionei —, que aponta aqui uma curva de aprendizagem. Tanto em 2013 aceitávamos um risco maior, que este ano conseguimos reduzir esse risco aceito a zero, quanto estamos acelerando o tratamento. Cabe notar que ainda estamos tratando dos riscos — alguns mapeados em 2013 — exatamente porque a nossa experiência era menor e tentamos de certa maneira abraçar o mundo com as mãos. Começamos por algumas coisas muito complexas, que agora estamos dando conta de tratar. Esse alinhamento vem produzindo resultados positivos nesses números nos 2 anos subsequentes.

As ameaças que nós monitoramos têm essas categorizações: o vazamento de informações direcionadas a pessoas, processos, tecnologias; as fraudes eletrônicas com *phishing scanner*, envolvendo o ataque, a intencionalidade contra o sistema bancário e serviços da Previdência Social; ataques direcionados, desenvolvidos com foco nos nossos sistemas e serviços de maneira mais específica; ataques com grande volumetria, que o clássico é esse de negação de acesso, em que a demanda excessiva pelos nossos sistemas deve ser interpretada como um ataque que visa a não possibilidade da prestação desse serviço; e, claro, uma preocupação crescente com o sequestro dos dados.

No vazamento de informação, as ações preventivas que são tomadas são de conformidade dos investimentos na busca de alinhamento com as melhores práticas do mercado. O mascaramento de dados, as nossas grandes bases necessitam estar sempre em constante trabalho tanto de testes, homologação, novas tecnologias. Isso não pode ser feito com a base real sem o mascaramento. Isso agrava, de maneira desnecessária, os riscos. Então, um uso muito efetivo de mascaramento de dados para o trabalho que não é de produção efetiva e de entrega dessas informações aos nossos clientes e ao público em geral.

Quanto ao controle de acesso aos sistemas, estamos fazendo uma grande migração para um sistema unificado de controle de acesso, desenvolvido pela própria empresa, que está padronizando o controle de acesso aos nossos sistemas por toda a Esplanada entre os nossos clientes. Além disso, a criptografia na transmissão desses dados, o fortalecimento e a consolidação de um grupo especializado em análise de segurança.

Nas fraudes eletrônicas, temos ações de *antispam*, filtragem de conteúdo, intensificação de ações de conscientização, tratamento de incidentes. Esse é um trabalho intenso, porque geralmente a porta de entrada disso são as agências do INSS, as agências do Ministério do Trabalho e Emprego. Então, há um elemento de conscientização da população que nós ajudamos, mas são os órgãos de comunicação dos nossos clientes que trabalham de maneira mais intensiva. Nós nos concentramos mais na análise dos códigos maliciosos, que muitas vezes vêm junto com esses instrumentos de *phishing* e de *spam*.

Nos ataques direcionados, trabalhamos com proteção em camadas, em que tecnologias de última geração tentam fechar periferias de controle concêntricas, de acordo com naquele desenho inicial, para que possamos garantir, a partir de um espaço menor, seguro, a expansão dessa periferia e assumir o controle da segurança nessa expansão. Nos estudos de tendências e principalmente em uma ação preventiva, o desenvolvimento seguro de *softwares*, com requisitos de segurança bastante definidos no projeto, para que possamos não só padronizar, mas limitar os riscos relacionados.

Nos ataques com grande volumetria, monitoramento proativo de infraestrutura da nossa rede, em parceria com as operadoras, para que vários desses ataques consigam ser lidados no nascimento. Muitas vezes, há um processo importante de recrutamento de computadores, inclusive no exterior, para que esse ataque se efetive, e eliminar esse ataque na origem alivia grande maneira o sobreuso da nossa infraestrutura.

Mencionei a modernização que realizamos nos nossos três *data centers* nos últimos anos — há alguns números de investimento no final da apresentação — e a proteção em camadas. Tudo isso visando à diminuição do tempo de recuperação de incidentes.

É importante nós partilharmos com os senhores e com as senhoras a nossa filosofia, que é como aquela de quem está dentro de uma corrida armamentista. Então, à medida que nós ganhamos proficiência e capacidade com alguma disciplina, com algum elemento nessa luta, sabemos que, nos meses seguintes, o outro lado, por assim dizer, também vai ganhar proficiência no nosso contra-ataque e também vai apresentar novas capacidades de superar o que estamos fazendo. Essa é uma corrida armamentista permanente. E, como toda boa corrida armamentista, leva a evoluções tecnológicas importantes, mas também muito sangue colateral derramado. Para a nossa sorte, é sangue virtual, é sangue de *bits* e *bytes*, e não real.

Em relação ao sequestro de dados, como dissemos, o Programa de Continuidade de Negócio para preservar a integridade desses dados, o processo contínuo de gestão de riscos, de vulnerabilidades técnicas e de avaliação de segurança e a modernização das soluções de proteção de dados.

Para ilustrar o que tudo isso tem significado nos últimos anos da empresa, com alguns números de investimento, contabilizamos que, nos últimos 5 anos, investimos mais de 235 milhões nesses elementos. Em 2011, a solução IPS, uma evolução significativa da nossa rede, a ampliação das nossas soluções de *firewall*, a instalação do nosso NOC na nossa sala de monitoramento. Em 2012, a sala-cofre, a infraestrutura do *data center* do Distrito Federal e o *firewall* de banco de dados. Em 2013, a sala-cofre de São Paulo. Em 2014, a sala-cofre do Rio de Janeiro e uma solução integrada de controle de acesso físico em toda a empresa, em todas as unidades.

E, neste ano, já implantamos *firewall* de rede, solução de criptografia do *backbone*, certificação digital para todos os nossos usuários, certificados digitais para todos os nossos servidores *web*. E estamos implantando o nosso *firewall* de aplicação e uma solução muito efetiva de proteção de dados, que vai nos possibilitar, inclusive, trabalhar muito mais com o *backup* e o *storage* em disco e não mais com aquelas fitas antigas, o que era outra vulnerabilidade.

E estamos em estudo para implantação e aquisição — como eu disse — de cofre de senhas, solução de proteção de intrusão análise estática e dinâmica de código, solução de correlacionamento de eventos, solução de monitoramento de

segurança, solução de análise de segurança e mascaramento de dados. Esses são os investimentos que concentramos nesse foco.

Para encerrar, além desses dados todos, há o testemunho de que, nesta corrida armamentista para dominar o espaço da oferta de serviços de tecnologia da informação, não existem absolutos, não existem garantias totais. Existe um conflito permanente para assegurar que as melhores práticas, as melhores tecnologias e os processos mais adequados estejam em constante utilização para assegurar que o Estado consiga fazer do uso desses dados aquilo que a sociedade espera.

Por outro lado, também é fundamental dizer que essa expectativa da sociedade em relação ao uso dos dados apresenta contradições em si mesma. O acesso total, a comodidade total, o serviço total é contraditório com a proteção total, é contraditório com a segurança total, é contraditório com o controle total.

E esse equilíbrio é dinâmico, é algo que a sociedade costuma expressar, querendo todos os descontos e ofertas por pertencer a um cartão fidelidade, mas não aceitando que os seus dados estejam partilhados pelo comércio em geral. Em relação a esse processo legislativo, inclusive é uma satisfação para nós o fato de esta Casa se debruçar sobre esse debate e nos oferecer orientação.

Muito obrigado. *(Palmas.)*

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada ao nosso querido Rodrigo Assumpção, Presidente da DATAPREV.

Concedo a palavra neste momento, pelo tempo de 20 minutos, ao Sr. Cristiano Rocha Heckert, Secretário de Logística e Tecnologia da Informação do Ministério do Planejamento.

O SR. CRISTIANO ROCHA HECKERT - Bom dia, Deputada Conceição Sampaio, Deputado Sandro Alex e demais Parlamentares integrantes desta Comissão, senhoras e senhores!.

Eu agradeço, em nome da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, a oportunidade de participar desta audiência e compartilhar um pouco das ações que nós temos conduzido em conjunto com outros órgãos de Governo, parceiros.

Eu também preparei alguns eslaides para orientar a nossa fala e que vão ser projetados para os senhores.

(Segue-se exibição de imagens.)

É importante começar esclarecendo a missão da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento. O nosso Ministério orquestra o funcionamento dos órgãos de Governo nas suas diversas e necessárias funções à gestão da administração pública. E, no caso da nossa Secretaria, nós exercemos esse papel em três sistemas da administração. Nós somos o órgão central da área de logística. Portanto, orquestramos o processo de compras governamentais e de gestão dos serviços administrativos necessários ao funcionamento da máquina. Somos também responsáveis por gerir o processo de transferências voluntárias por meio do sistema de convênios e contratos de repasses da União e, também, órgão central do sistema de TI do Governo, o SISP.

No âmbito do SISP, nós coordenamos uma rede hoje composta por 222 órgãos e entidades da administração — estou falando aqui de Ministérios, autarquias e fundações do Poder Executivo Federal —, cada um dos quais tem a sua unidade de TI, que está inserida na estrutura organizacional daquele órgão. E, portanto, segue as diretrizes e prioridades estratégicas do seu órgão como um provedor de soluções tecnológicas para a consecução da política pública. Mas nós fazemos uma coordenação matricial dessas unidades procurando ganhar sinergia, otimização dos esforços e compartilhamento de boas práticas e orquestração das atividades.

Esse trabalho é feito por meio de alguns eixos temáticos, dentre os quais destaco: governança da tecnologia da informação, gestão do pessoal alocado na área de TI, padronização tecnológica, serviços digitais, sistemas de funcionamento da máquina pública, a parte de infraestrutura interna e de rede que conecta os órgãos, contratações de TI, segurança da informação — o tema que nos traz aqui —, interoperabilidade, dados abertos e governo eletrônico.

No campo da segurança cibernética, é importante ressaltar que existe um sistema semelhante ao SISP, aquele que nós coordenamos, que não é coordenado pela nossa Secretaria: é o Comitê Gestor de Segurança da Informação, instituído pelo Decreto nº 3.505, de 2000. Ele traz essa competência de órgão central ao Gabinete de Segurança Institucional da Presidência da República. Nós temos assento nesse Comitê e procuramos desenvolver um trabalho de muita sinergia com

o GSI nas ações de segurança, internalizando, no âmbito dos órgãos que compõem a nossa rede, as orientações e as diretivas trazidas pelo Gabinete de Segurança Institucional.

O Gabinete de Segurança Institucional coordena também o Centro de Tratamento de Incidentes de Rede, o CTIR Gov, mencionado aqui pelo Rodrigo, e incentiva que cada um dos órgãos da administração pública tenha as suas equipes de tratamento de incidentes de rede e que elas reportem, periodicamente, àquele núcleo central, as ocorrências relativas a tentativas de ataque ou a tentativas de burla da segurança da informação governamental.

Então, aqui, nós chegamos a uma figura que tenta representar alguns dos eixos abarcados, quando nós falamos de segurança cibernética. E, como disse o Rodrigo, felizmente nós não estamos num contexto de guerra no Brasil, mas há, sim, ações de proteção à soberania nacional que cada vez mais também têm que ser feitas no mundo digital, no mundo cibernético — e essas ações evidentemente são de responsabilidade do Ministério da Defesa e das Forças Armadas.

Nós temos um segundo conjunto de ações relativo aos crimes digitais, cuja competência para liderar é da polícia, e temos as ações relativas à segurança cibernética, que, como eu falei, são coordenadas no âmbito do Governo pelo GSI, com um apoio forte da nossa Secretaria.

É importante destacar também nessa figura que as ações relativas à segurança não podem se limitar aos aspectos tecnológicos. Nós sabemos que a maior parte das vulnerabilidades encontradas, não só nas organizações públicas, mas também privadas, está, muitas vezes, relacionada não aos aspectos tecnológicos, mas aos aspectos de processo de trabalho e de comportamento das pessoas que integram aquele instituição. Então, é importante que nós tenhamos uma visão holística e procuremos abranger nas nossas ações de prevenção todos esses aspectos.

Dito isso, vou passar a falar um pouco sobre cada uma das nossas iniciativas em andamento nesse âmbito da segurança cibernética.

É importante dizer que existem dois documentos de referência.

Uma estratégia de segurança da informação e comunicações e de segurança cibernética, já publicada pelo GSI, é o documento referencial para as ações de

segurança na administração pública. E nós, lá na SLTI, estamos finalizando o processo de publicação da estratégia de governança digital para a administração pública federal nos próximos 4 anos, que traz também algumas ações no campo da segurança alinhadas com aquelas propugnadas pelo GSI.

Então, vou falar um pouquinho de cada uma dessas dez iniciativas listadas, que serão detalhadas nos eslaides seguintes.

Em primeiro lugar, nós temos, desde o início dos anos 2000, ações na área de interoperabilidade e padronização tecnológica conduzidas por um comitê formado por diversos órgãos, em que se destacam a DATAPREV, o SERPRO, a Receita, aqui representada, a Caixa Econômica Federal e vários dos nossos órgãos de Governo, que procura definir padrões que orientem a interoperabilidade nas comunicações governamentais. E o estabelecimento desses padrões é um elemento importante como prevenção de questões relacionadas à segurança. Dentro da ePING, esse grupo que anualmente edita um documento revisado com esses padrões que devem ser seguidos pelos órgãos governamentais, existe um grupo de trabalho voltado ao tema de segurança que continuamente se dedica a rever as tendências tecnológicas, as padronizações internacionais que, nesse sentido, servem de referência.

Um segundo grupo de ações conduzidas está ligado ao gerenciamento de identidades. Como disse o Rodrigo, muitos dos problemas relacionados à segurança são ligados a acesso indevido aos nossos sistemas de informação e às nossas bases de dados. Então, temos trabalhado, há alguns anos, na busca de soluções mais robustas de controle de acesso pelos servidores públicos e por outros que interagem com sistemas governamentais, para prevenir fraudes, para prevenir acessos indevidos.

Temos alguns projetos em andamento, como o GerID, citado aqui e conduzido pelo consórcio DATAPREV/SERPRO. É uma aposta nossa para, num futuro não distante, criarmos uma federação de identidades que permita o acesso aos grandes sistemas estruturantes de Governo de forma segurança, de forma centralizada, através de uma ferramenta robusta, com os elementos de segurança aqui colocados.

Outra iniciativa é o mapeamento permanente dos ativos de informação do Governo. Nós inventariamos os *hardwares* e *softwares* utilizados pelos órgãos que compõem o nosso sistema, para que tenhamos clareza sobre quais ativos estão sob nossa gestão, para atuarmos também na padronização desses ativos e na prevenção de ataques a essas infraestruturas.

Temos avançado também numa linha de construção de padrões de auditoria de programas e equipamentos adquiridos pelo Governo Federal, conforme o Decreto nº 8.135, publicado em 2013. Agora, em agosto de 2015, nós disponibilizamos um documento de referência em padrões de auditoria que devem ser observados por todos os órgãos da administração na aquisição de programas e equipamentos de tecnologia da informação.

Temos uma parceria em andamento com o INMETRO e com todo o Sistema Nacional de Metrologia para que a auditabilidade e a conformidade dessas soluções de tecnologia possam ser garantidas a longo prazo.

Nessa linha dos padrões de auditoria, formamos um grupo de trabalho que atua no âmbito da ePING, coordenado pela nossa Secretaria, que conta com diversos atores, não só do Governo, mas também da Academia, que nos trazem continuamente à reflexão as referências dos padrões internacionais mais modernos nesse tema.

Estamos, neste momento, em consulta pública, com um documento de referência em gestão de riscos de segurança de informação e comunicações, construído também pela nossa equipe, em conjunto com outros órgãos da nossa rede. Esse documento traz diretrizes importantes a serem seguidas pelos órgãos e está disponível para consulta até o final deste mês de setembro, até para colhermos contribuições e podermos, em breve, oficializá-lo como uma diretriz a ser observada pelos órgãos.

Nós conduzimos também, já há algum tempo, o projeto Data.Gov, um projeto que busca otimizar as infraestruturas de TI dos órgãos. Então, a partir do levantamento da situação dos *data centers* e dos parques tecnológicos de cada órgão, nós procuramos incentivar aqueles órgãos que dispõem de uma infraestrutura mais robusta a ofertarem esse serviço a outros órgãos que não têm condições para investir nessas soluções de segurança. Com destaque, vemos a parceria com

empresas públicas — DATAPREV, SERPRO e TELEBRAS — que, conforme foi explicado pelo Rodrigo, já têm investimentos vultosos nessa área e podem oferecer serviços de qualidade e com alto grau de segurança aos órgãos governamentais.

Atuamos ainda na educação e conscientização permanente dos nossos profissionais nesse tema. E, nesse sentido, nós firmamos uma parceria com a Universidade de Brasília e oferecemos um curso de pós-graduação em gestão de segurança de informação. Temos recebido alunos não só da nossa Secretaria, mas desse conjunto de órgãos que integram o SISP.

Publicamos recentemente uma cartilha com instruções sobre segurança de informação e comunicações e, periodicamente, promovemos palestras, *workshops*, oficinas de trabalho, para discussão com esse conjunto de profissionais.

Gerimos também a INFOVIA, uma rede corporativa do Governo Federal, uma rede extremamente robusta, que hoje conecta praticamente todos os órgãos do Executivo Federal aqui em Brasília, de forma que as comunicações governamentais entre Ministérios e órgãos localizados aqui em Brasília são feitas de forma totalmente segura, trafegando dentro dessa rede governamental, sem sair para as redes das operadoras. E isso vale também para o acesso feito pelos servidores públicos cotidianamente aos sistemas estruturantes de Governo, como o Comprasnet, o SICONV, o SICAF e assim por diante.

Alguns resultados da INFOVIA nos últimos anos.

Nós revisamos o modelo de negócio que trouxe uma queda de 35% no valor dos serviços prestados aos nossos clientes. A rede se expandiu, chegando a 150 quilômetros que hoje cobrem todo o Plano Piloto, como mostrado na figura anterior.

Ampliamos o número de órgãos. Hoje são 91 órgãos federais abarcados por essa rede, com 201 pontos conectados aqui em Brasília. A banda de Internet está sendo continuamente expandida, e nós oferecemos diversos serviços de valor agregado em cima dessa rede, como, por exemplo, telefonia sobre IP e videoconferência.

Estamos com a TELEBRAS num projeto de construção da INFOVIA Brasil, que é a expansão dessa rede segura para conectar todos os órgãos federais em todo o território nacional.

Outro projeto conduzido pela nossa Secretaria é a migração dos ambientes de governo do IPV4 para o IPV6. Essa migração é necessária e está em curso em todo o mundo em função do esgotamento do endereçamento IP na versão 4. Além disso, também traz diversos benefícios relacionados à segurança, uma vez que, com o IPV6, não será mais necessário o compartilhamento de endereço de IP por mais de um usuário, além de todos os requisitos de criptografia que essa versão do protocolo já traz embarcados. Temos um projeto coordenado por nós e conduzido em parceria com SERPRO, TELEBRAS e DATAPREV, em que começamos a migração de fora para dentro, como nós dizemos.

Então, hoje, toda a rede da INFOVIA, por exemplo, já está migrada para o IPV6. E, agora, nós estamos trabalhando junto com cada um dos 222 órgãos para a evolução das suas redes internas e também dos seus portais de Internet e das suas aplicações para esse novo protocolo. Temos um cronograma detalhado, com metas que são acompanhadas semestralmente, que preveem que até 2018 todos os órgãos de governo estejam migrados para a versão 6 do protocolo IP.

Por fim, temos uma série de mecanismos de segurança continuamente implementados e revisados nos chamados sistemas estruturantes de governo. A SLTI mantém três desses sistemas: a plataforma SIASG ComprasNet, em que são feitas todas as licitações e a gestão dos contratos da administração pública federal; o sistema de gestão de convênios, que também operacionaliza todas as transferências voluntárias da União para Estados, Municípios e organizações da sociedade civil; e o Sistema de Concessão de Diárias e Passagens do Governo Federal.

Neste momento, estamos implantando o Processo Eletrônico Nacional, que também visa eliminar a tramitação de documentos em papel nos órgãos e traz diversos requisitos em termos de segurança, além dos outros sistemas que são geridos pelos órgãos parceiros dos Ministérios da Fazenda e do Planejamento e que são acessados pelos nossos clientes.

Então, em todos esses sistemas, nós implementamos mecanismos que evitam o *login* por robôs. Nós trabalhamos com assinatura com certificado digital, temos controle integrado de autenticação e sessão *web*, controle de acessos por meio de sistemas de bloqueio de IP, de *firewall*, e diversas regras de negócio,

notadamente na condução dos pregões eletrônicos, que são constantemente aperfeiçoados para evitar fraudes, para evitar acessos indevidos, para evitar o uso de máquinas na condução dos lances nas licitações. Então, essas são algumas das ações que estão em curso.

Para encerrar, trago aqui uma reflexão quanto aos desafios que todos nós, como Governo e sociedade, enfrentamos num contexto em que é crescente a dependência do Estado por recursos de tecnologia da informação e comunicação. Hoje, nenhuma política pública se faz sem suporte tecnológico — e isso só irá crescer.

Por outro lado, há demanda da sociedade por maior acesso à informação, por compartilhamento, por transparência e por abertura de dados governamentais que possam alavancar o desenvolvimento econômico e social do nosso País sem comprometer os requisitos de privacidade daqueles dados pessoais do cidadão.

Há também demanda dos órgãos públicos por compartilhamento e integração de informação, até para que possamos prestar melhores serviços aos nossos clientes, evitando que solicitemos ao cidadão, reiteradamente, informações de que o Estado já dispõe. Para isso, nós temos que avançar em padronização, temos que avançar na nossa capacidade de armazenamento robusto e seguro de dados, garantindo sigilo e lidando com as restrições que a tecnologia e o ambiente regulatório nos trazem, com essa realidade que está sendo debatida aqui na CPI, que é o crescimento do crime no ambiente virtual.

Então, são essas as minhas reflexões. Agradeço mais uma vez, Deputada, e me coloco à disposição para os questionamentos.

Obrigado. *(Palmas.)*

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada, Sr. Cristiano Heckert, Secretário de Logística e Tecnologia da Informação do Ministério do Planejamento.

Antes de passar ao nosso próximo convidado, eu quero registrar e agradecer a presença do Deputado Daniel Coelho, Sub-Relator desta CPI e representante do PSDB do Estado de Pernambuco. Muito obrigada.

Neste momento, concedo a palavra ao Sr. Adriano Volpini, Diretor da Federação dos Bancos Brasileiros — FEBRABAN, pelo tempo de até 20 minutos.

O SR. ADRIANO CABRAL VOLPINI - Cara Deputada Conceição Sampaio, demais Deputados presentes, colegas da Mesa, demais pessoas presentes, bom dia! Inicialmente, em nome da FEBRABAN, eu gostaria de agradecer a oportunidade desse espaço, nessa relação transparente, para discutirmos temas muito importantes para o desenvolvimento do País: os temas eletrônicos.

Na apresentação, eu vou abordar um pouco mais alguns dados que demonstram que, de fato, temos uma oportunidade muito grande de discutirmos soluções, segurança e implementação num ambiente que cresce. Na medida em que ele cresce, quanto melhor nós implementarmos essas melhorias desde o começo, sem dúvida, todo cidadão terá uma série de benefícios, como veremos aqui adiante.

Eu preparei três itens para a nossa discussão. Primeiro, falarei do contexto de como está a questão dos canais bancários e a utilização dos brasileiros em relação às transações por canais de Internet no Brasil, numa comparação também com o mercado internacional. Depois, vou entrar um pouco mais em detalhes nos crimes cibernéticos, mencionando como eles acontecem, como as fraudes, de fato, acontecem, e demonstrando que mecanismos de prevenção as instituições financeiras implementam e colocam à disposição dos clientes e como nós tratamos a gestão da consequência das tentativas de fraude contra os nossos clientes e contra os cidadãos.

(Segue-se exibição de imagens.)

Sobre o cenário, há alguns números que talvez, de alguma forma, os senhores já tenham tido a oportunidade de acessar. Aqui estão as fontes desses dados. Hoje, mais de 110 milhões de brasileiros têm acesso à Internet. Somos o País em que o cidadão está mais tempo conectado à Internet na América Latina. O nosso acesso ao *mobile*, o nosso telefone, tem um crescimento vertiginoso. Hoje, temos mais de 79 milhões de acessos à rede de Internet através de *mobile* e atingimos a incrível marca de mais de um celular por habitante no Brasil.

Quando nós olhamos como isso se traduz na penetração de acesso, de fato, ter um dispositivo é uma prerrogativa, é uma premissa. Mas como está o acesso à Internet e como isso se reflete nos canais bancários? Hoje — os dados são de 2014 —, no Brasil, a penetração de *smartphones* está em torno de 41% da população; de

Internet, já em 55%. Quando comparamos à média mundial de países mais desenvolvidos, nós acreditamos que, em 5 anos, teremos reduzido bastante o *gap* do Brasil e dos cidadãos brasileiros em relação à população mundial e, em 10 anos, certamente, estaremos no mesmo nível de acesso e oportunidade do cidadão de se valer da Internet não só para a informação, mas também para resolver os seus problemas do cotidiano.

Como isso se traduz nas transações bancárias? Esse é um dado bastante interessante, cuja fonte é a própria FEBRABAN. São dados que nós também publicamos no CIAB, o nosso congresso de automação bancária. Aqui, eu chamaria a atenção dos senhores para a evolução e para a diferença de como os canais são utilizados no banco ao longo do tempo.

A linha azul abaixo demonstra que a Internet tem um crescimento de 17%, de 2010 a 2014; enquanto o acesso dos nossos clientes às agências e ao *contact center*, que são as chamadas telefônicas, em ambos os casos, apresenta um decréscimo significativo. Chamo a atenção para a última curva, que é o atendimento via *mobile*, que tem um crescimento de 209%.

Eu trouxe esses gráficos só para fazer uma relação muito objetiva. Não são os bancos que desejam de alguma forma que os clientes se autoatendam. Essa é uma ação quase que inexorável na medida em que o cidadão deseja resolver os seus problemas ou acessar diretamente as suas informações. Ele não quer mais ter o intermediário na relação, seja com o banco, seja, muitas vezes, com o Governo. O Governo tem uma série de iniciativas na mesma linha das instituições financeiras, que é prover aos clientes, prover ao cidadão a oportunidade do acesso direto e, com esse acesso direto, ele poderá resolver todos os problemas ou, às vezes, suas eventuais necessidades. E, neste aspecto, tanto a Internet, quanto o telefone, o *mobile*, ambos são muito importantes para, de fato, prover esse serviço aos clientes. E essa é uma tendência não só brasileira, mas é uma tendência quase que global.

Entrando um pouquinho nos crimes cibernéticos em si e em como as instituições financeiras, de alguma forma, enxergam os riscos que estão presentes no seu dia a dia, eu os separei em três blocos bastante genéricos.

O primeiro, que é o foco maior da minha apresentação aqui, são as fraudes financeiras. Essas são as fraudes de terceiros tentando, de alguma forma, ter

acesso ao recurso dos clientes, recurso de nós, cidadãos, e fazendo-se passar por nós para acessar o nosso dinheiro e, de alguma forma, transferi-lo para algum outro local ou efetuar um pagamento.

Aqui eu vou me valer de algumas palavras em inglês, que são as técnicas mais comuns, são técnicas bastante conhecidas. A primeira é a *man-in-the-middle*; a segunda é *man-in-the-browser* e a engenharia social, esta eu vou detalhar um pouco mais adiante. Então, eu só gostaria de repassar, rapidamente, esses critérios e depois nós vamos entrar e eu vou explicar em detalhes como cada uma funciona.

E sobre essas fraudes financeiras, como já foram abordadas pelos meus colegas de Mesa, as instituições financeiras fazem investimentos significativos na proteção da sua infraestrutura e dos seus canais de comunicação. Como os clientes desejam acesso ao banco por esses canais, nós precisamos sempre mantê-lo absolutamente inexpugnável contra fraudes tentadas por terceiros. Entretanto, há um elo nessa corrente que pode ser afetado, e esse elo aqui, normalmente, é a máquina do cidadão, é a máquina do cliente na sua casa, o seu telefone. Depois nós vamos entrar um pouco mais no detalhe, eu vou poder explicar isso com mais clareza. Então, em grande parte dos casos aqui, essas três modalidades acabam respondendo pela fraude.

O segundo é algo que também foi abordado aqui na Mesa, mas que também nos preocupa. Aqui também imagino termos uma grande oportunidade, no Brasil, de tratarmos isso como algo muito ruim para a sociedade brasileira, que são os ataques de indisponibilidade contra todas as estruturas do País, estruturas eletrônicas do País. Isso significa alguém que tenta de alguma forma indisponibilizar o acesso do cidadão tanto ao serviço bancário, quanto ao serviço da Receita, ao serviço da DATAPREV — Empresa de Tecnologia e Informações da Previdência Social. Fazendo uma analogia muito direta, é como se alguém fosse a uma agência bancária, trancasse a porta e dissesse: *"Aqui ninguém entra, ninguém transaciona"*. Isso é algo ruim, corta o acesso dos nossos cidadãos aos serviços necessários, e é algo que os bancos investem bastante.

Hoje nós não vivemos no mesmo cenário vivido por alguns países na Europa e nos Estados Unidos, como, por exemplo, volta e meia nós vemos nos jornais ataques de... Supostos ataques chineses contra infraestruturas americanas, russos

contra chineses e assim sucessivamente. Então isso é algo que nós reputamos uma importância grande de investimento para que o País se proteja e trate isso como algo ruim, algo absolutamente não admissível na sociedade brasileira. Então, punir casos como esses é bastante relevante.

O segundo é a pichação, o que nós chamamos de *defacement*, que nada mais é do que entrar numa página do sistema de qualquer infraestrutura e colocar uma mensagem lá com ativismo político, religioso, social, etc.

E o terceiro bloco é o de roubo ou vazamento de informações, que são tentativas de invasão às nossas infraestruturas a fim de obter dados, obter as informações seja para fraudes, seja para, inclusive, causar situações como as mencionadas aqui, como aconteceu com algumas atrizes recentemente.

Como as fraudes acontecem? E aqui eu me permito fazer um diagrama que vai facilitar entendermos um pouco mais como é o pensamento do fraudador, porque é importante para nos explicar *a posteriori* como nós pensamos em proteger os nossos clientes.

Então, aqui, neste diagrama, nós temos de um lado o golpista, temos o cliente e, aqui, destacada, a máquina do cliente, a comunicação com as instituições financeiras. Os quadrados ali são as instituições financeiras autorizando a transação com os clientes.

Em linhas gerais, como acontece a infecção de um cliente para a realização da fraude? O método absolutamente tradicional é o envio de um *e-mail* para um cliente, para qualquer cidadão. Esse *e-mail* contém lá um arquivo executável, um programa que nós chamamos de programa malicioso. Esse programa malicioso se instala na máquina do cliente, e nós o chamamos de *malware*. E esse *malware* é ativado em diversos momentos. No caso, quando eles tentam uma fraude contra uma instituição financeira, quando alguém digita *www.seubanco.com.br*, esse *malware* começa a funcionar, e a função dele aqui é o passo dois, que é capturar informações, ele quer capturar as informações para transacionar pelo cliente.

Todo o bloco um, dois, três e quatro acontece objetivamente dentro da máquina do cliente. E as instituições financeiras, inclusive, periciam as máquinas muitas vezes para terem certeza de que, de fato, esse é o cenário.

As informações são capturadas seja através de uma página falsa, seja através desse *malware*. Com base nesses dados, o fraudador tem duas alternativas: há uma fraude mais simples, em que ele tenta, de uma máquina terceira, não da máquina do cliente, mas da própria máquina do fraudador, executar transações no *Home Banking*, no *Internet Banking* dos bancos.

E há uma variável mais sofisticada, em que ele tenta fazer a fraude dentro da máquina do próprio cliente. Então, é como se ele colocasse uma camada na relação entre a *Internet Banking* do banco, na própria máquina do cliente. O cliente... No meio dessa transação, o que nós chamamos de *man-in-the-browser*, entra o *malware* do fraudador trocando informações a fim de ludibriar o cliente, obviamente, e mandar essas informações para o banco.

Por que eles se utilizam dessa técnica? Porque os bancos, hoje, possuem dispositivos que permitem identificar se a conexão que aquele cliente está fazendo, no momento da transação, é proveniente de uma máquina, de um equipamento que nós já conhecemos, um equipamento que nós chamamos de equipamento seguro. Algumas instituições financeiras, inclusive, pedem para que os clientes indiquem qual é o equipamento que ele utilizará.

Então, numa variante para tentar transpor essa barreira que os bancos colocaram, ele vai e tenta executar essa fraude diretamente da máquina do cliente, que é como eu expliquei aqui, a parte do *man-in-the-browser*. Então esse *man-in-the-browser* torna mais difícil, torna quase que imperceptível para o cliente que, de fato, algo errado está acontecendo. A transação que eles acabam utilizando bastante aqui são pagamentos de tributos federais, estaduais; e eu vou falar um pouco mais adiante sobre a oportunidades que nós temos para tornar esse crime cada vez menos interessante para o fraudador.

Há uma terceira variante, que essa... E até aqui eu queria fazer um parêntese muito importante: a fraude eletrônica é praticamente um estelionato, como nós o conhecemos há muitos anos. É alguém tentando enganar alguém e usando uma estratégia, nesse momento, de enganar; a estratégia é obter uma ação de alguém.

Então, quando alguém está vendendo um bilhete premiado, há uma pessoa lá enxergando a oportunidade de comprar um bilhete que, na verdade, não existe, pagar muito menos do que ele vale e receber o dinheiro. Aqui, quando o fraudador

manda o *e-mail* para que alguém clique no *malware* e o instale, ele está oferecendo algo, que é um prêmio: *"Você ganhou algo, você foi sorteado, você tem um brinde"*, ou há cenas de catástrofes em geral, mas ele tenta enganar, ele faz um estelionato naquele momento, infecta a máquina do cliente e, a partir dali, ele faz um segundo estelionato, que é fazer o cliente oferecer dados a ele.

Neste caso aqui da engenharia social, muitas vezes as pessoas falam: *"Isso é impossível de acontecer"* e acontece com uma certa frequência, são os fraudadores ligando para a casa das pessoas e pedindo para que elas deem os dados: "*Então, me diga a sua senha, me diga o número do seu token"*. À medida que essas proteções foram transpassadas, é muito difícil você segurar... É como se alguém chegasse na sua casa e dissesse: *"Abra a porta, que eu quero entrar."* E isso acontece com uma certa frequência. Por que nós temos que ter todo esse detalhamento? Isso vai direcionar como nós prevenimos as fraudes.

Neste eslaide, vou procurar mostrar aqui uma sequência de como nós protegemos as transações para garantir que de fato elas são corretas. O primeiro é a autenticação, é saber que nós estamos falando de fato com o cliente. Aqui tem uma série de dispositivos importantes, como a senha eletrônica exclusiva para uso na Internet, a senha do cartão utilizada para assinar as transações dos clientes, teclados virtuais, para impedir que alguém enxergue ou verifique que você está digitando uma senha, o token, que é uma senha específica e única para cada transação, canais cruzados para confirmação de transação, ou seja, você inicia uma transação na Internet e muitas vezes você precisa concretizá-la via ligação ou através de um canal de autoatendimento.

Na parte da máquina do cliente, nós temos uma série de ações para monitorar se de fato há um *malware* instalado nessa máquina. Nós temos os chamados *plug-ins*, que são aplicações que de fato limpam a máquina do cliente com frequência; usamos e temos uma relação muito forte com as empresas fornecedoras de antivírus e fazemos a identificação da máquina.

A proteção das comunicações também é algo muito importante para nós. Toda a nossa comunicação é criptografada, justamente para impedir que alguém capture as informações no caminho. E, ainda assim, como última camada, nós monitoramos o uso das nossas marcas, cada banco faz o monitoramento da sua

marca e, caso identifique páginas falsas, age muito rapidamente para que ela seja retirada do ar. Monitoramos as transações efetuadas pelos clientes. Muitas vezes ligamos para os clientes, pedimos confirmação, se foi ele mesmo que fez. Utilizamos institutos internacionais para certificar os nossos processos e aqui buscando atender às melhores práticas internacionais, e ampliamos bastante os canais aos clientes, tanto de acesso quanto de oportunidade de falar com o banco para confirmar transações.

O último bloco é a conscientização. Como dito aqui, uma boa parte do risco sempre reside em uma questão comportamental. Os bancos investem muito, as instituições financeiras investem bastante em conscientizar os clientes, seja através de guias de segurança, seja através de uma série de ações digitais, como Dia da Internet Segura, *e-mails*, *pop-ups*, etc., para conscientizar o cliente do que fazer e do que não fazer no mundo virtual, e muitas vezes nós vamos além das questões financeiras.

Seguindo além, um pouco sobre a gestão de consequências, aqui os bancos em geral deixam muito claro que, além de não coadunar, não têm absoluto interesse em receber ou transacionar situações fraudulentas. Nós encerramos contas, sempre que possível, inclusive tiramos o cliente do sistema financeiro, quando ele é um fraudador, temos uma ação muito próxima com a polícia, na parceria com os órgãos públicos, mas aqui nós enxergamos uma oportunidade muito grande que eu gostaria de reforçar com os senhores.

Muitas das fraudes têm como destino final o pagamento de um tributo, seja ele federal, estadual ou municipal. As instituições financeiras têm bastante dificuldade em impedir que essa fraude aconteça e não é apenas a questão de reaver o dinheiro, mas principalmente que nós não permitamos que a pessoa que fez a liquidação permaneça com a dívida quitada. Isso gera uma oportunidade muito grande, um estímulo muito grande para o fraudador para se valer desse mecanismo para obter recursos de fraude. Isso é algo em que precisamos investir bastante.

Segundo, nós temos uma lacuna de reconhecimento dos canais digitais dos bancos. Como eu mostrei nos primeiros eslaides, tem uma oportunidade muito grande de desenvolvimento do País, via canais digitais; temos que evoluir bastante

na regulamentação e na aceitação legal desses canais como meios de relacionamento com o banco.

Por fim, no bloco de apuração de autoria, os bancos estão muito próximos dos órgãos policiais, principalmente da Polícia Federal, via Operação Tentáculos, não só investindo, mas também compartilhando muitas das informações. É nosso total interesse manter os canais digitais absolutamente seguros, porque nós sabemos que, além das estratégias do banco, é algo desejado pelo cidadão brasileiro, e só vão existir bancos saudáveis num sistema financeiro saudável.

Nesse caso aqui, os canais são extremamente importantes para o sistema financeiro.

Mais uma vez, eu gostaria de agradecer a oportunidade, e me coloco à inteira disposição para as eventuais perguntas. *(Palmas.)*

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada ao Sr. Adriano Volpini, Diretor da FEBRABAN.

Antes de passar à nossa última convidada, eu quero registrar e agradecer a presença do Deputado Silas Freire, do PR do Estado do Piauí. Muito obrigada.

Concedo a palavra neste momento à Sra. Claudia Maria de Andrade, da Receita Federal do Brasil, pelo tempo de até 20 minutos.

A SRA. CLAUDIA MARIA DE ANDRADE - Sra. Deputada Conceição Sampaio, senhores colegas de Mesa, Srs. Deputados presentes, senhoras e senhores presentes, é uma oportunidade para a Receita Federal falar de uma vertente um pouco desconhecida de modo geral para o público, que é a questão da nossa política de segurança para armazenamento de dados. Então, muito obrigada pela oportunidade. Certamente vai ser uma oportunidade para mostrar o quanto a Receita Federal é zelosa com os dados do cidadão.

(Segue-se exibição de imagens.)

Antes de mais nada, eu gostaria de apresentar um pouco qual é a abrangência da Receita Federal. Nós temos aí uma abrangência nacional. Isso faz com que nós tenhamos uma linha de ação bastante significativa. Trabalhamos tanto com a fiscalização e a arrecadação de tributos federais como também com o controle do comércio exterior para combate a descaminho e contrabando. Eis o motivo de estarem aqui as lanchas e os helicópteros.

Como nós temos uma abrangência nacional, um dos procedimentos que são adotados administrativamente é a criação de unidades descentralizadas. Na Receita Federal, nós somos divididos em dez Regiões Fiscais: a 1ª Região Fiscal é formada pelos Estados do Centro-Oeste; a 2ª, pelos do Norte; a 3ª , a 4ª e a 5ª, pelos do Nordeste; a 6ª Região é formada por Minas Gerais; a 7ª Região, Rio de Janeiro e Espírito Santo; a 8ª Região, São Paulo; a 9ª Região, Paraná e Santa Catarina; e a 10ª Região, Rio Grande do Sul.

Cada região também é dividida em unidades descentralizadas, que são denominadas de acordo com a sua competência de atuação. Então, nós temos, ali, nos portos e aeroportos e nas unidades de fronteiras, as unidades que nós chamamos de Inspetorias ou Alfândegas. Temos também as Delegacias de Julgamento, que são responsáveis pelo julgamento de primeira instância do contencioso entre a Receita Federal e o contribuinte que contestou algum auto de infração. Por fim, nós temos as Delegacias, que são responsáveis pela fiscalização de tributos fazendários e tributos previdenciárias. Essas delegacias podem ser divididas, dependendo do tamanho e de sua jurisdição, em agências, num total de 566 unidades na Receita Federal.

Sobre a importância da tecnologia, só para dar uma noção do volume de dados com que nós trabalhos: o *site* da Receita — eu peguei aqui algumas informações dos últimos anos — tem em torno de 1,9 bilhão de páginas visitadas em 2013; em 2014, o número é em torno de 1,8 bilhão. Em 2015, até o momento, houve 1 bilhão de acessos ao nosso *site*. É uma média de 1,6 bilhão de acessos. Os serviços mais acessados são a consulta do Imposto de Renda. Isso é normal; cada vez que há a disponibilidade de um novo lote, temos até que fazer um reforço de carga, para suportar o acesso. Todo mundo quer a sua restituição e quer saber se saiu naquele lote ou não. O segundo mais acessado é consulta sobre a situação do seu CPF. A média anual de acesso ao *site* para o serviço de CPF, por ano, é em torno de 227 milhões de acessos.

Na Receita Federal, o uso da Internet tem vários objetivos. O primeiro deles é a simplificação dos processos. Alguns aqui talvez não saibam nem o que eu estou falando. Quando eu era criança, eu era assistente do meu pai na entrega do Imposto de Renda. Ele fazia o rascunho, eu era a assistente que ia lá fazendo o ditado para

ele. Depois, ele passava a limpo, numa máquina de escrever — tem gente que não sabe nem o que é isso —, e hoje nós temos um cenário em que a declaração é entregue por alguns segundos e, nesses segundos, são feitos 56 tipos de batimentos, desde CPF ativo ou não ativo. Isso faz o processo muito mais simples, muito mais seguro, mais cômodo inclusive para o nosso cidadão. Isso também faz geração de redução de custos, de transporte, de sustentabilidade. E eu relacionei aqui alguns programas e alguns sistemas, aplicativos que são conhecidos do público e que eu gostaria de elencar. O Programa do Imposto de Renda, eu acho que esse é o nosso carro-chefe, por assim. Somos mais conhecidos por isso. Mas nós também temos outros, como o SISCOMEX — Sistema de Comércio Exterior. Temos os aplicativos para dispositivos móveis, como disse bem o Dr. Adriano. É uma linha que nós estamos investindo, uma vez que nós sabemos que *smartphones*, *tablets*, dispositivos móveis são uma realidade nacional e mundial. Nós temos aqui processos virtuais. Todos os nossos processos são virtuais. Quando o Dr. Cristiano comenta que vai criar o processo virtual nacional, isso muito nos alegra, uma vez que os ganhos com essa implementação são exorbitantemente positivos, seja em termos de desmaterialização de papel, de mais agilidade. A gente tem a entrega de um processo por outra equipe que pode ser em qualquer lugar do País, em alguns segundos, com um toque apenas, sendo que antes demoravam meses, às vezes, com malote e encaminhamento.

A tecnologia, para a Receita, tem alguns objetivos: agilização dos procedimentos internos, externos, redução de prazos e custos, melhoria da gestão e eficiência. O Dr. Adriano comentou sobre a questão de que as fraudes sempre existiram. Como estou na Receita Federal, no cargo de auditora, há 22 anos — então, eu já sou mais da pedra lascada —, tenho casos muito antigos para contar. Um deles, quando eu trabalhava na área de importação, a gente tinha ainda as declarações entregues em papeis — hoje é tudo pelo sistema —, e uma das grandes fraudes que tinha era a entrega do pagamento dos DARFs. Os DARFs eram entregues em papel, e o sistema que a gente usava, à época, se chamava SINAL. Ele demorava 2 a 3 dias para ter a validade e a confirmação de que havia o depósito. Então, às vezes, a gente liberava a mercadoria e só depois ia descobrir, lá pelas tantas, que o imposto não tinha sido pago. Então, esse tipo de procedimento

— na verdade, a informática, por mais riscos que haja hoje, são outros tipos de riscos —, na verdade, pelo menos sob o ponto de vista da Receita Federal, foi uma grande aliada no combate à fraude. Outras coisas muito importantes também são os cruzamentos de dados que nós fazemos. Isso é trabalhado nas nossas ações de inteligência, investigação, fiscalização. Para vocês terem uma ideia, nós temos duas equipes que trabalham na fiscalização: uma é da área de programação de fiscalização, que faz todo o planejamento — qual contribuinte se pretende fiscalizar; outra equipe separada é a da fiscalização, que vai executar o procedimento. Para vocês terem uma ideia, esse cruzamento de dados faz com que a gente seja tão certeiro que 90% dos procedimentos executados pelos auditores da fiscalização têm efeito positivo. Então, a Receita otimiza e melhora a sua gestão no sentido de que ela vai já sabendo qual é a possibilidade de acerto nessa auditoria.

E a questão da desmaterialização do papel. Bom, eu tinha conhecimento de que nós teríamos aqui à Mesa as duas empresas que dão suporte à Receita Federal no armazenamento de dados, que é o SERPRO e a DATAPREV. Então, nesse caso, em relação ao armazenamento de base de dados, eu vou ser relativamente, diria assim, mais macro, uma vez que aí o Dr. Rodrigo já apresentou os procedimentos que são realizados pela empresa e o SERPRO também, com uma qualidade similar, apresenta uma capacidade muito significativa de segurança de dados. Os dados da Receita Federal — então, os dados dos cidadãos — estão armazenados nesses dois *data centers,* que são empresas de governo, que têm políticas de segurança de dados extremamente estruturadas, têm acesso a controle de ambiente físico, lógico, têm equipes especializadas e uma série de outras ferramentas, que o Dr. Rodrigo apresentou aqui no transcorrer da sua apresentação, inclusive com grupos de resposta a ataques. No caso da Receita Federal, como o nosso *site* está hospedado no SERPRO, essa equipe de resposta a ataques está ali localizada no nosso prestador de serviço, o SERPRO. Além disso, a Receita Federal já tem uma política de segurança que, em seus contratos, sempre coloca a necessidade de implementação pelo prestador, mesmo que ele tenha sempre um lembrete — eu e o Dr. Rodrigo às vezes nos encontramos nas reuniões para lembrar essa importância. Nós sabemos que eles estão trabalhando cada dia de forma mais organizada. A política de rastreabilidade é no sentido de eu saber quem acessou

alguma informação. Tem uma ferramenta — e isso é instalado particularmente no SERPRO, e a DATAPREV também já a está implementando — que se chama Vigia DBA. O que acontece? A gente sempre pensa o seguinte: qual é o elo mais fraco do processo? São as pessoas. Então, essa solução é um gerenciamento de ações dos administradores de dados que trabalham diretamente com os dados. Outra questão que a gente coloca é que os nossos parceiros, SERPRO e DATAPREV, não têm autorização de disponibilização de dados a terceiros nem de informações, tanto é que às vezes tem alguma demanda judicial que cai lá no SERPRO e na DATAPREV e eles devolvem dizendo assim: "*Qualquer informação sobre a aplicação "x", ou o dado "x" deve ser solicitada à Receita Federal*".

Outra questão também, pela qual a gente sempre prima, é a utilização de *captia. Captia* são aquelas letrinhas chatas que você tenta ficar descobrindo o que é para tentar digitar e você nunca acerta na primeira. Ela tem o objetivo de evitar a ação de robôs que pretendem extrair grande lote de informações. Neste caso aqui, por mais que a gente fale que, a princípio, tem que ser uma coisa lógica, nós temos a Lei de Acesso à Informação, uma lei, por sinal, belíssima que faz com que a transparência dos órgãos do Governo junto ao cidadão seja cada dia mais bem apresentada. Mas a gente às vezes recebe alguns pedidos, algumas solicitações, alguns (*ininteligível*) interessantes e um deles é: "*Por favor, tire o captia, o antirrobô*". A gente costuma dizer: "*Mas eu já estou disponibilizando a informação que você está pedindo*." Este mês mesmo o que a gente recebeu — não é, Serginho? — foi pedido para retirar o *captia* do Certidão Negativa... *"Mas se você quer saber, se você está com algum tributo pendente ou não, é só entrar lá e está disponível. A gente está atendendo à lei"*. Aí a gente indeferiu esse pedido, houve um recurso e o colega, o cidadão, falou assim: "*Não, mas eu preciso dessas informações senão vai atrapalhar os meus negócios*." Então, assim, às vezes a gente acha que é uma chateação aquelas letrinhas horrorosas, mas é uma segurança inclusive para nós.

Eu vou falar um pouco mais sobre a questão interna da Receita Federal, como eu disse aos senhores, em decorrência já dos esclarecimentos do Dr. Rodrigo em relação ao armazenamento de dados. Por que a Receita Federal, o pessoal interno da Receita Federal — os nossos usuários chegam a dizer até que a gente da área de segurança é chato —, por que a gente é tão criterioso em relação à política

robusta e estruturada de segurança? Por causa do sigilo fiscal. Esse é um mantra que você, quando entra na Receita Federal, já aprende. "*Olha, reserva porque tem o sigilo fiscal."* E esse reflexo às vezes... No mês passado, por exemplo, estávamos com um consultor alemão e perguntamos sobre novas formas de autenticação para aplicativos móveis — *tablets* e *smartphones.* Dissemos: *"Olha, queremos um mecanismo seguro"*. Ele disse: *"Não. Se houver algum problema, depois se resolve".* Dissemos: *"Mas o problema é dano à imagem, a imagem da instituição e a imagem do cidadão"*.

Até, Dr. Adriano, permita-me contar um caso aqui. A primeira vez que tive meu cartão de crédito clonado, eu acordei de manhã e vi que algumas pessoas tinham feito uns procedimentos de compra de passagem aérea. Liguei para o cartão de crédito e imediatamente foi estornado. Eu me senti a pessoa mais importante do mundo. Eu perguntei: *"Eu não preciso provar nada?" "Não."* Já estornaram, fiquei feliz. Então, apesar de o meu cartão ter sido clonado, ter sido utilizado indevidamente, eu fiquei extremamente feliz com as ações do sistema bancário. Primeiro, porque me foi avisado da ocorrência pelo celular, e, segundo, estornaram, acreditando na minha palavra. Fiquei felicíssima. Só que, infelizmente, para uma instituição pública, às vezes, esse acontecimento tem um dano mais difícil de ser superado.

Portanto, para nós, essa questão de dano e imagem, não que o sistema bancário não passe por isso, a margem de erro é baixíssima.

Alguns princípios e premissas da nossa política de segurança. Primeiro, a política de segurança é para todos. Algumas empresas falam assim: *"Nossa, mas área de TI sofre muito, porque afinal de contas chega o diretor-presidente e fala que quer que instale aqui alguma coisa".*

Na Receita Federal, graças a Deus, na área de TI, temos uma política tão estruturada, a instituição é bastante organizada nesse ponto, que para todos, sem exceção, seja o Secretário da Receita, seja o estagiário, seja qualquer um, a política é a mesma. Se o Secretário pede para eu instalar alguma coisa, um Skype, que não é, no caso, homologado por nós, falo assim: *"Sinto muito, mas não está homologado"*.

Há outras questões. A segurança da informação não é meramente técnica, é uma questão estratégica, até para criticidade em relação aos dados que nós temos armazenados. Seguimos políticas do gabinete de segurança institucional, regulamentações dos órgãos de controle, normas em relação à questão. Nós temos um alto envolvimento da administração, por meio da criação de um comitê de tecnologia e segurança da informação, instituído já há alguns anos na Receita Federal e é formado pelo Secretário, por Subsecretários e pela Coordenação de Tecnologia.

Nós entendemos que, por mais que devamos acreditar nas pessoas, a tecnologia e a segurança, em particular, têm que depender o menos possível de pessoas. Os procedimentos a serem adotados pela instituição têm que buscar uma segurança maior.

Um exemplo: quando a Receita Federal começou a utilizar isso, nos idos de mil novecentos e nada, eu me lembro de que usávamos apenas uma senha para acessar a abertura do computador. A engenharia social, como disse o Dr. Adriano, é muito interessante.

Eu sou de São Paulo e havia um colega carioca. O menino disse assim: *"Eu vou descobrir a tua senha".* Dito e feito. O menino carioca, em São Paulo, adorava futebol. Qual era a senha dele? *(Pausa.)* Flamengo.

Aí foi avançando em relação a essas questões, para que hoje, eu, além de ter uma senha que tem aquelas letras maiúsculas e minúsculas, uso também uma forma de autenticação, que é o certificado digital, citado aqui. Portanto, não só a senha forte, com complexidade, mas também é necessário um equipamento complementar para abrir um computador e as suas aplicações.

As pessoas têm papéis, responsabilidades e o acesso tem que ser motivado. Não adianta o colega dizer: *"Ah, eu não sabia".* Quando ele recebe a senha, recebe também um termo de responsabilidade.

Outra coisa que implementamos na Receita Federal — o Dr. Adriano comentou sobre a eventual fragilidade do equipamento do seu cliente — é uma política em que só pode ser utilizado pelos funcionários o equipamento corporativo. Há uma ideia futura — em algumas empresas, já estão utilizando — de se trazer seu equipamento para dentro da empresa. Na Receita Federal, nós não permitimos esse

tipo de procedimento, porque a nossa política de segurança é bastante robusta e ainda não identificamos um modelo para que esse uso de equipamento pessoal possa ser implementado com segurança.

Alguns pilares da área de segurança são os processos, as tecnologias e as pessoas. Temos alguns modelos de questões relacionadas a processos. A primeira questão é a política de acesso.

Eu, por exemplo, sou coordenadora da área de tecnologia, já há alguns anos, e auditora fiscal. Então eu tenho acesso a todos os sistemas da Receita Federal? Não; eu, particularmente, tenho acesso para saber quem acessou alguma declaração, mas não há por que eu ter acesso a alguma coisa de cobrança, a alguma baixa de algum pagamento ou débito, porque não é da minha atribuição esse tipo de atividade. Então, a Receita Federal trabalha com procedimentos bastante formais, por meio da criação de portarias, que segregam o acesso: dependendo do cargo, da atribuição, da função, recebe-se um perfil compatível com as suas atividades. Então, eu não tenho acesso a tudo.

São 20 minutos? Estou terminando.

E há ainda algumas situações em que se faz a identificação do nome, do CPF, da pessoa que acessou, da hora em que acessou. Além disso, trabalhamos com processos de auditoria. Nesses processos de auditoria, no primeiro momento, fazemos a inspeção de códigos, mesmo que seja de algum prestador de serviço. Há uma equipe especializada em auditoria interna de procedimentos e uma corregedoria que trabalha com o objetivo de combater desvios de conduta de alguma pessoa.

Em termos de infraestrutura interna, há ferramentas, como os colegas comentaram: antivírus, *firewall*. Há monitoramento da rede e restrição de acesso a *sites*. Por exemplo, às vezes, se for algum *site* de rede social, bloqueamos. Há dados criptografados e políticas de descarte de mídias. Só pode ser instalado na máquina *software* devidamente homologado, analisado e aprovado pela área de tecnologia. Além disso, o usuário não é um administrador de máquina: se eu quiser instalar agora um *software* aqui, eu, Cláudia, Coordenadora-Geral de Tecnologia da Informação da Receita Federal, não consigo, porque não sou a administradora da máquina.

Há alguns procedimentos em relação à utilização, como eu tinha comentado com os senhores, de certificação digital. Nós usamos também algumas ferramentas para que haja gerenciamento e otimização e para que identifiquemos quem são as pessoas que têm acesso. Há uma aplicação responsável por esse assunto que faz um batimento com os empregados ativos sobre regras — se eu me aposentar hoje, sou automaticamente desabilitada nos sistemas — e faz relatórios gerenciais.

Outra linha de trabalho em relação a isso é a questão do usuário, que, como dissemos, é o elo mais fraco do processo tecnológico.

Eu até trouxe aqui um exemplo, Deputada Conceição, que mostra que às vezes a área de tecnologia leva a culpa por questões que não são decorrentes de tecnologia, mas de fatores humanos.

Em 1978, a maior fraude de computador, segundo o *Guinness Book*, foi atribuída a problemas de computação, mas a única coisa que a pessoa que fraudou conseguiu foi ver a senha a pessoa colocava no computador. Ele viu como funcionava, pegou a senha e se passou pela pessoa.

Essa é uma questão na qual trabalhamos bastante. Nós, internamente, temos uma equipe especializada em segurança da informação e temos gestores de segurança que fazem auditorias nos procedimentos.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Sra. Cláudia, a senhora só tem mais 1 minuto.

A SRA. CLÁUDIA MARIA DE ANDRADE - Perfeito.

Temos procedimentos de convênio com outros órgãos, com alguns procedimentos formais. A mesma coisa ocorre em relação ao Judiciário. Há um sistema que faz a relação com o Judiciário, para que não haja trâmite de ofícios nem documentos, através de uma aplicação.

E, para falar um pouco sobre a Receita Federal, em termos de governança, como disse o Dr. Cristiano, somos controlados por alguns órgãos, como o TCU, que mostram que a Receita Federal tem uma situação bastante positiva em governança de tecnologia, em termos da administração direta. Temos recebido elogios de órgãos de controle. A Receita Federal tem recebido vários prêmios por aí.

Estamos à disposição.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada, Sra. Cláudia Maria de Andrade, da Receita Federal do Brasil.

A SRA. CLÁUDIA MARIA DE ANDRADE - Obrigada a V.Exa.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Quero registrar e agradecer a presença do Deputado Nelson Marchezan Junior, do PSDB do Rio Grande do Sul.

Após a apresentação dos nossos convidados, nós abrimos a palavra para os questionamentos dos colegas Parlamentares. Já há dois Parlamentares inscritos, o Deputado Daniel Coelho e o Deputado Silas.

Passo a palavra ao Deputado Daniel Coelho, que é também Sub-Relator desta CPI.

O SR. DEPUTADO DANIEL COELHO - Obrigado, Sra. Presidente.

Eu quero cumprimentar a Deputada Conceição Sampaio, que preside esta audiência, e a todos os presentes.

Creio que o que eu tenho a dizer pode ser respondido pelos quatro debatedores. Eu acho importante fazermos uma análise da legislação atual no Brasil. Os crimes cibernéticos são variados e, a cada dia, aparece uma novidade. A grande verdade é essa. Então, tem que se considerar o grande dinamismo de tudo o que acontece na Internet. E a velocidade nem sempre é acompanhada pela legislação, pela própria ação das empresas envolvidas e do Governo, de uma forma geral. Isso é natural. Temos que compreender, como disse, a velocidade de tudo o que acontece no mundo virtual.

Eu queria que os senhores fizessem uma análise da legislação que existe atualmente para coibir e tentar punir os crimes cibernéticos. Há sugestão, por parte dos senhores, para aperfeiçoarmos a nossa legislação?

Ao longo da CPI — nós temos tido diversas audiências —, temos ouvido especialistas. Já sentimos que há dificuldades, por parte do Ministério Público, da Polícia Federal e daqueles que, por dever, têm que investigar os crimes cibernéticos, em rastrear, ir atrás dos culpados, buscar quem cometeu o possível crime, seja ele um crime contra a Receita Federal, contra o sistema bancário, contra a honra, de pedofilia, seja ele de qualquer outra natureza, exatamente pela lentidão, pela própria

burocracia. Quando se chega ao fundo da investigação, às vezes a pessoa não está mais lá, aquele IP já não existe mais. Quer dizer, o tempo passou.

Enfim, peço um comentário nesse sentido, para saber se a legislação atual brasileira está adequada, se nós precisamos aperfeiçoá-la e se os senhores têm alguma sugestão que a CPI possa avaliar ao final dos trabalhos.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada, Deputado Daniel Coelho.

Concedo a palavra ao Deputado Silas Freire.

O SR. DEPUTADO SILAS FREIRE - Quero, cumprimentando a Deputada Conceição Sampaio, cumprimentar a todos, tanto aos debatedores como aos colegas Parlamentares presentes.

Tenho algumas considerações a fazer. Quero dizer que o crime cibernético hoje, principalmente a invasão de dados privados do cidadão, às vezes conta com o consentimento de determinadas empresas: elas passam a consentir no momento em que não cuidam de sua segurança cibernética. Elas analisam os ataques cibernéticos apenas como inevitáveis. A empresa que faz isso automaticamente faz também um *mea-culpa*, quando seus clientes ou quando seus acervos são atacados.

Dito isso, eu tenho algumas indagações. Dirijo-me, primeiro, à Dra. Cláudia.

Qual é o impacto de uma tecnologia da informação sobre a percepção dos usuários, nos processos de trabalho no âmbito da Secretaria da Receita Federal? Quais são os efeitos provocados pela implantação de uma nova tecnologia na Receita Federal? Qual a validação do instrumento que foi criado e quais os efeitos gerados pela tecnologia da informação? Essas são as indagações que faço a V.Sa.

Dirijo-me agora aos representantes ligados à área da proteção bancária.

Para que tenhamos mais segurança nas transações bancárias, que eventuais medidas necessárias poderíamos estar tomando para que as chances de golpes ou ataques via Internet fossem contidas? Os aplicativos de Internet *Banking*, via telefonia móvel, são seguros? Acho que todo mundo tem a curiosidade de saber isso.

Quanto às indagações sobre os golpes, eu faculto à Mesa decidir quem responde. Relativamente aos golpes na Internet, a crimes como fraudes eletrônicas

feitas através de aplicativos, aplicativos falsos, qual a forma mais eficaz de combate? Há uma forma de identificar, de punir quem os aplica? Seria bom que algum dos convidados pudesse nos dar um esclarecimento sobre isso.

Mais uma pergunta: quais os impactos da utilização da grafoscopia e da documentoscopia na redução das fraudes contra as instituições bancárias, relativamente a empréstimos consignados?

Seriam basicamente essas as colocações. Ao longo, eu posso tentar interferir novamente.

Muito obrigado, Sra. Presidente.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Obrigada, Deputado Silas.

Deputado Marchezan, V.Exa. gostaria de fazer uso da palavra? *(Pausa.)*

Passo a palavra à Mesa. Os convidados podem se sentir à vontade para responder aos Parlamentares.

Antes, contudo, gostaria de também deixar aqui, aberto a todos os convidados, um questionamento a respeito, principalmente, do que foi colocado pelo representante da DATAPREV, que falou muito sobre as ameaças externas, mas ressaltou que nenhum sistema, por mais seguro que possa parecer, resiste a um acesso interno com interesse de fraudar.

Eu gostaria muito de ouvir V.Sas. a respeito de fraudes que podem acontecer internamente.

Com a palavra os nossos convidados.

O SR. DEPUTADO RAFAEL MOTTA - Deputada Conceição, permita-me dar uma informação.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Pois não.

O SR. DEPUTADO RAFAEL MOTTA - Eu queria aproveitar este momento para fazer um convite a todos os Deputados desta Comissão.

No dia 5 de outubro, nós teremos uma reunião da Comissão na cidade de Natal, no Estado do Rio Grande do Norte, que represento. Por estar à frente da Sub-Relatoria que trata dos crimes contra crianças e adolescentes, eu convido todos os Deputados a participar, o Deputado Marchezan, o Deputado Daniel Coelho, o

Deputado Silas. A Deputada Mariana Carvalho, Presidente desta Comissão, estará presente.

Já de antemão digo que nós ouviremos diversas entidades — o Ministério Público, representantes do Governo do Estado, a Secretaria de Segurança Pública —, para debater os problemas que acontecem principalmente nos Estados do Nordeste e do Norte brasileiro, que é onde se concentra grande parte dos crimes cometidos contra as nossas crianças e adolescentes, a exemplo das Operações Araceli, Darknet, e Gênesis, recentemente deflagrada.

Então, deixo aqui o convite aos que quiserem participar para o dia 5 de outubro, em Natal. Reforço o convite ao Deputado Daniel Coelho. Também o Deputado Marchezan já esteve conversando conosco.

Por fim, Sra. Presidente, parabenizo V.Exa. pela condução dos trabalhos.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada, Deputado. Está feito o registro do convite. Certamente será um grande momento para debatermos o problema também no Rio Grande do Norte. Parabéns pela iniciativa!

A palavra está aberta à Mesa.

A SRA. CLÁUDIA MARIA DE ANDRADE - Deputado Silas, muito obrigada pelas perguntas.

Com relação à questão apresentada pelo Deputado Daniel sobre se a legislação atual atende ou não à necessidade que há hoje de combate ao crime cibernético, concordo com S.Exa. quanto a que hoje em dia está tudo muito mais rápido: a informação está toda mais rápida, os crimes são mais inovadores a cada dia. Além de achar que a legislação tem que avançar, como aconteceu no caso da Lei Carolina Dieckmann, acho que é importante haver investimentos na área. Se nós não tivermos agilidade para fazer a detecção da fraude de forma tempestiva e dar a ela tratamento, a coisa acaba sendo inócua no primeiro momento, porque a indisponibilidade de serviço ou da imagem já terá acontecido. Então, eu acredito que precisamos trabalhar em investimento em equipes e em ferramentas. Além disso, precisamos trabalhar na legislação, como os senhores já estão fazendo, para atualizá-la para a nossa realidade atual.

Com relação à questão levantada pelo Deputado Silas sobre qual o impacto da TI na percepção dos usuários e quais são os efeitos da tecnologia na Receita Federal, o que posso dizer é que a Receita é completamente dependente da tecnologia.

Quando temos problema de indisponibilidade por algum motivo interno, como manutenção, simplesmente um dos telefones que mais toca é o meu. Todos os nossos processos são virtuais. É difícil identificar na Receita Federal um processo interno que não seja dependente da tecnologia. Tanto nos procedimentos de comunicação com o cidadão — leilão eletrônico de mercadoria apreendida, relação de obrigações acessórias — quanto nos processos internos, a dependência é igualmente grande. Todos os nossos processos são virtuais.

Esses dias eu estava conversando com uma guria que entrou no ano passado na Receita Federal. Ela não é da área especializada em tecnologia. Ela me disse: *"Eu estou estranhando e não sei como que vou fazer".* Eu lhe disse: *"Em qualquer lugar que você estiver na Receita, ou você entende de tecnologia, e, mais do que isso, entende os procedimentos de segurança, ou então você vai estar completamente fora do padrão. Você está no lugar errado"*.

Quanto à percepção dos usuários — estou acompanhada aqui do Sérgio Fuchs, gestor da área de segurança da informação na Receita —, nós temos um cenário em que, mesmo identificando que a segurança pode ser um fator complicador — nossos usuários ficam muito raivosos quando não podem instalar um *software* na máquina —, nós estamos num modelo de maturidade já bastante consolidado que diz o seguinte: nós temos que ter a segurança da informação. E, para tanto, não podemos depender de pessoas, simplesmente. Lógico que as pessoas têm que ser conscientes, têm que passar por um processo, palestras, mas não podemos mais depender disso.

Com relação ao nosso usuário externo, a Receita Federal busca sempre avançar em serviços virtuais, com o objetivo de prestar um serviço melhor para a sociedade. Às vezes dizemos que a minha área é a área boazinha da instituição, porque ela tenta buscar soluções em serviços virtuais que facilitem a vida do cidadão.

Por fim, alguém comentou sobre a preocupação que há com fraudes por vias externas e indagou sobre como fazemos em relação ao acesso interno. Na verdade, este é um processo bastante necessário: se a instituição não tiver zelo com os seus procedimentos internos, haverá uma linha muito grande de fraudes. Tanto é assim que a minha apresentação visou basicamente mostrar procedimentos internos na Receita para que nós tenhamos a mitigação, da forma a mais próxima, da totalidade dos ataques internos.

Muitos procedimentos são feitos internamente, não só de tecnologia implementada, mas processos e questões relacionadas a isso.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada.

Com a palavra o Sr. Cristiano.

O SR. CRISTIANO ROCHA HECKERT - Eu queria comentar a sua fala, Deputada, sobre a questão da fraude interna. Eu acho que três pontos precisam ser atacados.

O primeiro ponto é capacitação e conscientização, sobretudo de um conjunto de profissionais que às vezes não têm má-fé, mas que, por desconhecimento ou ingenuidade, não seguem os procedimentos adequados de segurança.

O segundo ponto, tão ou mais importante, é o que a Cláudia enfatizou muito em sua apresentação: procedimentos robustos aplicáveis a todos. Com eles, eliminamos muito a possibilidade de ataque por parte daqueles que têm má-fé em suas ações.

O terceiro ponto é um bom sistema de controle de acesso, de garantia de autenticidade e identificação inequívoca de quem é a pessoa que está acessando o sistema.

O SR. ADRIANO CABRAL VOLPINI - Vou abordar alguns dos itens. Acho que o primeiro item faz menção à legislação. Sem dúvida, temos uma oportunidade muito grande. Os gráficos que eu apresentei há pouco mostram a evolução do Brasil no uso dos canais eletrônicos. Como a evolução é muito rápida, não necessariamente a nossa maturidade acompanha essa evolução, tampouco a legislação.

E eu diria que nós temos algumas oportunidades bastante grandes. A primeira é em relação à produção de provas vinculadas aos *logs*, vinculadas à

possibilidade de manutenção das informações que permitam às autoridades policiais responsabilizarem o respectivo autor. É uma grande oportunidade, sobretudo, que nós também consigamos de fato utilizar todos esses *logs*, essas informações como conteúdo probatório. Caso contrário, produziremos *logs* que não poderiam ser utilizados como insumos para incriminar ninguém.

Falando aqui em nome da FEBRABAN, e de forma bastante clara, para nós, no sistema eletrônico brasileiro, as duas vertentes vinculadas a proteger, no nosso caso, não só clientes e cidadãos, mas também a infraestrutura das empresas brasileiras, sejam elas públicas ou privadas, é algo que deveria estar bastante explícito na legislação brasileira, bem como uma definição bastante clara das consequências de se cometer um crime assim. Crime que se comete com consequências muito pequenas estimula sua manutenção e execução. Então, para mim, esses dois itens são fundamentais.

Em relação às medidas contra golpes aos clientes em geral, às transações bancárias, e à segurança dos aplicativos — vou entrar um pouco mais em detalhes —, eu diria que é inexorável o caminho de a relação entre cliente e sistema financeiro se dar através de canais eletrônicos. Os bancos investem significativamente na proteção da sua infraestrutura interna para quando o cliente se conecta com eles. O principal papel dos bancos é, de fato, proteger os recursos e as informações dos clientes, que inclusive pagam por isso. Os bancos investem significativamente para cumprir esse papel de forma impecável.

O nosso grande desafio é ajudar, ensinar e apoiar o desenvolvimento, não só no que diz respeito aos nossos clientes, mas também ao ambiente como um todo, de como se relacionar num ambiente eletrônico.

Fazendo uma relação bastante direta, quando as pessoas saem à rua à noite, normalmente elas já sabem por onde podem andar e por onde não podem andar, se têm que andar acompanhadas ou não, se podem deixar a carteira na calçada ou se não podem deixar a carteira na calçada.

Os conceitos de fragilidade e de risco a que se está exposto precisam estar muito claros para todo cidadão brasileiro, não só para o cliente bancário. Muitas vezes o crime eletrônico não está em busca só do dinheiro de um correntista

bancário, mas atrás de informações para serem utilizadas contra aquela pessoa, como aconteceu recentemente contra artistas famosos.

Então, no que diz respeito ao direito à privacidade, os latinos têm uma diferença muito grande em relação aos anglo-saxões. Quando se verifica como um americano, por exemplo, cuida dos seus dados pessoais, constata-se que é de forma absolutamente diferente de como o brasileiro o faz. Eu vou usar aqui um exemplo simples: o nosso lixo conta muito sobre nós. Não raro, as pessoas pegam correspondências, documentos bancários, declarações de Imposto de Renda e documentos fiscais e os jogam no lixo sem destruí-los. Assim, pessoas com engenharia reversa acabam nos conhecendo muito e usando essas informações para diversos crimes contra nós. Esse cuidado é algo que não está no nosso DNA, não está no DNA do latino, mas nós precisamos de alguma forma mudar isso, porque é importantíssimo para que os canais eletrônicos se movimentem e evoluam com segurança.

Os aplicativos bancários são, sim, seguros. Eu posso dizer de forma muito objetiva — sou responsável pela segurança da informação também no sistema — que muitos conceitos dos aplicativos dos celulares estão sendo transportados para os aplicativos feitos para nossos PCs, *notebooks*, etc., porque nesses aplicativos, seja por *mobile*, seja por *tablets*, o controle dos códigos é muito importante, de modo que nós temos uma proteção de código bastante robusta nesses terminais.

Quanto à grafoscopia e à documentoscopia em relação a empréstimos consignados — vou aproveitar e responder a todas as perguntas —, sem dúvida elas são ciências excepcionais que agregam muito ao processo investigativo pós-fato, quando precisamos investigar se a assinatura no documento de fato foi feita com a correta pressão da caneta, por exemplo. Os grafoscopistas têm bastante propriedade em nos fornecer os laudos nesse sentido.

Também a dinâmica do empréstimo consignado está indo muito mais do papel para o mundo eletrônico, também ela segue essa tendência. Então, eu diria que a proteção dessas transações deve passar por um maior emprego de tecnologia na vinculação da relação entre o consumidor e a instituição financeira, ou órgão federal, ou estadual, envolvida nessa relação.

Sobre proteção interna, toda empresa que se preze, como foi muito bem colocado aqui, precisa considerar dois itens importantes. O primeiro é que o risco pode acontecer de fora para dentro: alguém pode tentar entrar na nossa casa, mas também nós podemos eventualmente colocar alguém dentro da nossa casa que cause problemas e leve para fora informações nossas.

Nosso grande lema no sistema financeiro é: nossos processos, nossos sistemas precisam ser a prova da ingenuidade, porque muitas vezes não há má-fé, mas há ingenuidade, que pode levar ao risco. E, para provar a ingenuidade, uma série de investimentos são feitos, considerando que essa hipótese sempre existe. Tal qual disse a Dra. Cláudia, os bancos têm o papel fundamental, similar ao da Receita, de manter o sigilo bancário dos clientes, de acordo com a Lei Complementar nº 105. Nós tratamos as instituições financeiras com tratamos a Receita Federal, ou seja, o cuidado com as informações internas é muito rigoroso.

O SR. DEPUTADO SILAS FREIRE - Só uma observação: nessa questão da segurança interna, há algumas promoções, alguns aplicativos feitos até com os servidores mesmos. Eles são usados na Internet, são atraídos através da grande rede, e isso é um risco grande. Por isso eu disse que as empresas precisam tomar cuidado não só com os ataques a elas. E não podem pensar que *"isso é inevitável"*, ou que *"isso está acontecendo com todo mundo"*. Se as empresas raciocinarem dessa forma, nós vamos estar cada vez mais distantes do caminho de proteção total.

O SR. ADRIANO CABRAL VOLPINI - O Deputado Silas me deu um gancho importante: eu havia me esquecido de mencionar a legislação.

Na maioria das situações em que nós temos uma tentativa de ataque contra uma empresa brasileira, estão envolvidos os servidores mantidos em outros países. Isso representa um desafio enorme para a conclusão das investigações das tentativas de ataques cibernéticos no Brasil. Nesses casos, a morosidade nos atrapalha. Então, a possibilidade de convênios internacionais, convênios legais que permitam a agilidade da investigação, traria um patamar de proteção para o ambiente brasileiro muito grande.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Com a palavra o Sr. Rodrigo.

O SR. RODRIGO ORTIZ D'ÁVILA ASSUMPÇÃO - Muito obrigado.

Para contribuir um pouco com este debate, destaco dois pontos.

O primeiro é que a literatura deixa muito claro que as ameaças internas, em número e em profundidade, superam sobremaneira as ameaças externas, não só porque há uma certa facilidade inerente à proteção de ameaça interna, como porque a discussão cultural nos prepara para isso: a ideia de que o inimigo é sempre o outro tem impacto sobre nossa ética e tem impacto sobre nossa política de segurança. O fato é que, muitas vezes, o inimigo está muito mais próximo da gente, o que o torna inimigo numa hora e colega de trabalho na outra.

E a anuência, como já foi aqui colocado, passa por ingenuidade, passa por desconhecimento, passa por simples desleixo, passa por não se levar a sério certas situações. Uma das coisas que eu faço frequentemente quando visito instituições é tentar esticar um pouquinho o acesso à segurança.

Ontem eu vim a esta Casa para outro compromisso. Passei direto, da mesma maneira que estou aqui, sem crachá, sem nada. A pessoa que inicialmente me barrou foi convencida de que eu tinha um compromisso muito importante, com uma pessoa muito importante, e que eu podia passar sem me identificar. Hoje, isso não foi possível. Tentei a mesma coisa, mas o segurança me barrou e depois me identificou, Disse que a Deputada me esperaria tranquilamente para o início da reunião e que eu não estava atrasado. Essa experiência de passar direto já ocorreu no Palácio, já ocorreu no exterior.

A cultura da segurança é um processo em que precisamos assumir, nesta cidade especialmente. Eu sou de São Paulo, e uma das coisas que se aprende aqui muito rápido é que, se estiver de terno e gravata e fizer cara de autoridade, a pessoa tem acesso a quase todos os lugares.

É esse o início da discussão sobre segurança interna, muito mais do que a discussão sobre procedimentos, processos, *tokens.*

Quanto à legislação — não sou nenhum especialista, mas, há muitos anos, eu me formei em História, sempre com certa predileção por tecnologia —, a humanidade nunca abandonou nenhuma tecnologia por motivos éticos; ela só abandona uma tecnologia quando essa tecnologia é superada. A humanidade nunca abandonou nenhuma tecnologia por legislação; ela só abandona a tecnologia

quando outra dinâmica social estrutura uma outra forma. É aquela história: a idade da pedra lascada não acabou porque faltavam pedras. O processo é de evolução e mudança da cultura organizacional.

Então, eu não sei se o problema está especificamente na legislação. Nós estamos falando de crimes que são tipificados de maneira bastante clara. Nós estamos falando de veículos e canais diferentes para crimes habituais. Foi citado aqui, de maneira até explícita, que fraude é fraude. Engano e sequestro de identidade são engano e sequestro de identidade.

O que talvez nós precisemos discutir é a responsabilização institucional de entes públicos e privados que não adotarem práticas adequadas de proteção e rastreamento dos seus dados. Vou usar fazer uma analogia. Quando discutíamos a Lei de Acesso à Informação, tive algumas conversas com jornalistas que tinham a seguinte tese: o Governo está se opondo à LAI, porque o Governo não quer dar acesso à informação. Eu, desesperadamente, tentava explicar a eles que o Governo tinha alguma relutância quanto à LAI, porque nós não estávamos organizados e as informações não estavam classificadas para darmos acesso a elas. Não havia nenhuma expectativa de ocultar nada, só o que ocorria é que as informações não estavam organizadas para o acesso — coisa que, com o andamento do processo, vai acontecendo.

Talvez essa analogia funcione da seguinte maneira: o problema não é bloquear uma rastreabilidade, o problema não é dizer ao delegado: *"Não, você não pode investigar".* O problema é que, muitas vezes, o *log* não existe. A estruturação do sistema não foi feita para isso. E, aí, se não se implantou um *log*, não há o que rastrear. Se você não controlou os seus processos, não existe rastreabilidade.

Talvez uma discussão interessante seja a da responsabilização e de processos adequados. Obviamente estamos falando de investimentos muito vultosos e, portanto, o conceito de processos adequados, que também será dinâmico e também evoluirá com o tempo, precisa ser estabelecido de maneira muito prudente, para não se criminalizar a atuação profissional, a atuação empresarial e a atuação governamental. Mas talvez aí esteja um aspecto importante, o de que há um compartilhamento de culpas, se se deixa a porta aberta ou se não

se é capaz de rastrear aquilo que aconteceu. Esse é um elemento que mereceria, pelo menos, uma discussão.

Ao mesmo tempo, gostaria também de agregar um grande apoio à última ideia colocada pelo Adriano, relativa a acordos internacionais. Não reconhecer o caráter descentralizado e supranacional da Internet é uma miopia terrível. Esse não será um problema resolvido por nenhum único país do mundo. Ou será resolvido enquanto sociedade da informação global, ou não será resolvido.

Sobre o último assunto, a evolução da capacidade de compreensão da sociedade, como já foi estruturado, digo que evolui tanto a tecnologia quanto as necessidades de intervenção e de reflexão legislativa. Portanto, uma legislação mais flexível, mais genérica, que se preocupe com o processo evolutivo, que tem uma dinâmica muito acelerada, talvez tenha mais longevidade do que uma que aponte apenas para o problema específico de hoje, que certamente não será o problema específico de amanhã.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Gostaria de agradecer aos convidados, que certamente trouxeram informações importantes para os trabalhos desta CPI.

Agradeço ao Sr. Rodrigo Assumpção, ao Sr. Cristiano Heckert, ao Sr. Adriano Volpini e à Sra. Cláudia Maria de Andrade.

Vou conceder 1 minuto a cada um de V.Sas. para as considerações finais.

Tem a palavra a Sra. Cláudia.

A SRA. CLÁUDIA MARIA DE ANDRADE - Novamente, muito obrigada pela oportunidade de apresentar todos os processos da Receita Federal relacionados à tecnologia, bem como de falar sobre a importância da tecnologia e de todo o zelo que a Receita Federal tem em relação aos dados dos cidadãos. Nós sabemos que somos fiéis depositários das informações, não somos os donos das informações, e isso traz uma obrigação muito grande quanto aos nossos procedimentos internos e quanto ao respeito ao cidadão. Então, muito obrigada pela oportunidade.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada.

Tem a palavra o Sr. Cristiano.

O SR. CRISTIANO ROCHA HECKERT - Também agradeço a oportunidade, Deputada Conceição, e aproveito esta última fala para apoiar os dois últimos

comentários feitos aqui. Refiro-me à importância dos acordos internacionais e ao último comentário do Rodrigo, no sentido de haver uma legislação que não tente cobrir casos específicos. Nós que sempre trabalhamos produzindo normas sabemos que estamos sempre atrás, estamos sempre correndo atrás de uma dinâmica social que, nesse caso, é muito intensa. Se nós ficarmos tentando cercar todas as possibilidades com uma legislação muito restritiva, estaremos sempre em defasagem em relação aos avanços da sociedade, especialmente daqueles mal-intencionados.

Talvez o caminho seja realmente dar segurança quanto aos crimes já tipificados, para que possam ser de fato combatidos no ambiente virtual.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada.

Tem a palavra o Sr. Adriano.

O SR. ADRIANO CABRAL VOLPINI - Inicialmente, eu gostaria de reforçar os conceitos da Federação Brasileira de Bancos, o nosso compromisso sério e unilateral com a manutenção de ambiente eletrônico para transações bancárias absolutamente seguras. Essa é uma premissa muito importante para o sistema financeiro e da qual não abrimos mão.

Enalteço o debate. Saio daqui absolutamente satisfeito, saio mais informado e feliz por saber que esta discussão deve produzir, sem dúvida, um avanço grande para o País.

Por fim, agradeço a oportunidade de a Federação Brasileira de Bancos estar presente numa discussão tão importante quanto esta e parabenizo a Deputada Conceição Sampaio pela presidência da Mesa.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada.

Tem a palavra o Sr. Rodrigo.

O SR. RODRIGO ORTIZ D'ÁVILA ASSUMPÇÃO - Muito obrigado.

Faço meus agradecimentos por esta oportunidade, por este tipo de troca, de interação. Além de isso contribuir para o meu crescimento pessoal, sinto-me muito feliz, como servidor público, por ver este debate na Câmara dos Deputados.

Quero parabenizar a CPI, a todos os participantes, porque isto também é parte da trajetória de evolução da compreensão não só desses fenômenos, mas das

demandas, desejos e reações da sociedade. A dinâmica entre a sociedade e a tecnologia é profundamente interativa. A tecnologia é gerada, criada, contestada, destruída a partir das demandas da sociedade, e essa tecnologia, por sua vez, molda e estrutura e, muitas vezes, destrói demandas da mesma sociedade. Na hora em que essa interação é sistematizada e consolidada por um debate parlamentar de alto nível, ela promete bons resultados para a nossa sociedade.

Muito obrigado.

A SRA. PRESIDENTA (Deputada Conceição Sampaio) - Muito obrigada, Sr. Rodrigo.

Eu quero só reforçar o informe trazido pelo Deputado Rafael Motta, do PROS do Rio Grande do Norte. No dia 5, esta CPI estará no Estado do Rio Grande do Norte para a realização de audiência para ouvir e debater, principalmente, a questão dos crimes de pedofilia através da Internet contra as crianças e adolescentes daquele Estado.

Nada mais havendo a tratar, vou encerrar a presente reunião, antes convocando reunião ordinária da Comissão para a próxima terça-feira, dia 29 de setembro, a partir das 14h30min, conforme pauta que será disponibilizada por meio eletrônico.

Agradeço aos servidores da Casa pelo belíssimo trabalho de sempre e às pessoas que nos honraram com suas presenças neste plenário.

Agradecendo a Deus pela paz neste ofício, declaro encerrada esta reunião.