ASSESPRO
PODER LEGISLATIVO
SENADO FEDERAL
Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética (FPCIBERSEG)

Reunião: Início das atividades da FPCIBERSEG

A Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética do Senado Federal realizou no dia 28 de maio, a 2ª reunião do grupo visando a **abertura oficial dos trabalhos**, deliberar sobre alterações no estatuto, eleger cargos para comissão da FPCIBERSEG **e debater sobre o custo econômico-social da segurança cibernética no Brasil**. O evento foi conduzido pelo presidente da Frente, senador **Esperidião Amin** (PP/SC) e contou com a participação de outros membros do colegiado, a saber: senador **Sergio Moro** (União/PR); senador **Marcos do Val** (PODE/ES); e a deputada **Tabata Amaral** (PSB/SP).

Estiveram presentes:

- **Fábio Diniz**, presidente do Instituto Nacional de Combate ao Cibercrime (INCC);
- **Luana Tavares**, CEO do INCC;
- **Marcelo Malagutti**, assessor especial do Gabinete de Segurança Institucional da Presidência da República (GSI);
- **Andrei Gutierrez**, presidente da Associação Brasileira das Empresas de Software (ABES);
- **Rodrigo Fragola**, diretor de Cibersegurança e Defesa da Confederação Assespro;
- **Keli Carvalho**, assessora econômica da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomércioSP); e
- **Leandro Volochko**, promotor de justiça do Ministério Público do Mato Grosso.

O senador **Esperidião Amin** destacou três prioridades da Frente: (i) a criação de uma agência nacional de cibersegurança, (ii) a formação de um centro de cooperação técnica entre governo e setor privado — *inspirado no modelo da National Cyber-Forensics and Training Alliance (NCFTA)* —, e (iii) o fortalecimento da formação profissional. Em seguida, admitiu um quarto eixo, voltado à contribuição legislativa. Ressaltou a importância de experiências como o Guardião Cibernético promovido pelo Exército Brasileiro e anunciou que será marcada nova reunião até o recesso de julho, possivelmente online, para consolidar propostas objetivas.

O senador **Sergio Moro** enfatizou que a segurança cibernética é pauta suprapartidária e uma prioridade nacional. Destacou a necessidade de criar uma agência com foco técnico e autônomo, e defendeu o engajamento do setor privado para desenvolver centros colaborativos como o NCFTA. Propôs que a Frente receba sugestões normativas para aprimorar o arcabouço legal vigente e sugeriu um *fusion center – ambiente criado para o compartilhamento de informações e inteligência entre diferentes agências de segurança* – que também atue como centro de treinamento. Reiterou a urgência de avançar institucionalmente antes de o país ser surpreendido por um ataque de grandes proporções.

O senador **Marcos do Val** mencionou o PL 2051/2025, de sua autoria, que trata da inclusão de cibersegurança e inteligência artificial no ensino médio público que pode contribuir para a citada necessidade de capacitação. Destacou a importância de representação parlamentar permanente das entidades do setor, inclusive para acompanhar e influenciar a tramitação de projetos que possam impactar negativamente a área.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Fábio Diniz do INCC, apresentou os quatro pilares de atuação da entidade: articulação público-privada; estudos técnicos; cooperação com forças de segurança; e ações de letramento digital. Destacou o papel da Aliança Multissetorial pela Cibersegurança Nacional para colaborar com a estratégia nacional de cibersegurança. **Luana Tavares** também do INCC, propôs formalizar um acordo de cooperação técnica da Aliança com a Frente, reforçando que há forte convergência entre o diagnóstico do grupo empresarial e as diretrizes da Frente, defendendo que o momento agora exige execução coordenada.

Marcelo Malagutti do GSI, relatou a criação de quatro grupos de trabalho no âmbito do CNCiber: um para elaborar o Plano Nacional de Cibersegurança com ações até 2031, outro para organizar os Centros de Compartilhamento e Análise de Informações (ISACs, na sigla em inglês), um terceiro para regulamentar a interação entre esses centros e a rede federal de gestão de incidentes, e um quarto para definir exigências mínimas de segurança para serviços essenciais e infraestrutura crítica. Mencionou ainda a nova estratégia nacional, a ser publicada via decreto presidencial, que, segundo ele, posicionará o Brasil em uma política de terceira geração, superando defasagens históricas.

Andriei Gutierrez da ABES, também representando o Conselho de Economia Digital e Inovação da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (Fecomercio-SP), afirmou que o sentimento no setor empresarial é de urgência. Destacou o aumento de ataques de ransomware e a ausência de estatísticas confiáveis. Disse que a coalizão multissetorial se reúne quinzenalmente e propôs que a governança da política de cibersegurança seja construída com segurança jurídica, proporcionalidade regulatória e cooperação entre reguladores já existentes.

A deputada **Tabata Amaral** reforçou que o trabalho da Frente deve também mirar na proteção da população mais vulnerável, como idosos e crianças, que estão cada vez mais expostos a golpes e aliciamentos no ambiente digital. Disse que a responsabilidade pelo combate a esses crimes não pode recair apenas sobre pais ou educadores, e sim sobre o Estado, o arcabouço regulatório e os provedores de serviços. Citou que a população percebe essa migração do crime físico para o digital e cobrou medidas para enfrentar o problema com rastreabilidade, fiscalização e conscientização.

Rodrigo Fragola da ASSESPRO, relatou que a Confederação estruturou uma diretoria específica para cibersegurança e defesa, reconhecendo o caráter estratégico do tema. Informou que mais de 100 empresas participam atualmente de um grupo técnico que já iniciou discussões sobre proposições legislativas e ideias ligadas à cibersegurança. Mencionou conversas com integrantes da Frente Parlamentar para desenvolver ações mais concretas no segundo semestre de 2025 e declarou apoio da Confederação às iniciativas da Frente e da Aliança Multissetorial.

Kelly Carvalho da Fecomercio-SP, apresentou dados sobre o impacto dos crimes cibernéticos nas PMEs, destacando que 60% das pequenas empresas encerram suas atividades em até seis meses após sofrerem um ataque, o que evidencia a vulnerabilidade desse segmento diante das ameaças digitais, que enfrentam, limitações técnicas e falta de acesso a linhas de crédito específicas. Informou que o Conselho de Economia Digital e Inovação da entidade elaborou o documento Decálogo da Regulação e Governança da Cibersegurança no Brasil, que reúne diretrizes para formulação de uma política pública harmônica. Manifestou disposição para colaborar com a Frente na elaboração de propostas voltadas à melhoria do ambiente de negócios.

Marcelo Almeida da ABES, chamou atenção para a Lei nº 14.533/2023, que institui a Política Nacional de Educação Digital, e destacou que ela pode servir como base legal para a

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

inclusão da cibersegurança nos currículos escolares. Apontou que o uso dos recursos do FUST é autorizado para a execução dessa política e sugeriu articular sua implementação por meio de conselhos municipais, estaduais e nacionais de educação.

O promotor de Justiça **Leandro Volochko** apresentou dados da pesquisa conduzida pela Global Anti-Scam Alliance (GASA), com participação do MP-MT, segundo os quais **94% dos entrevistados no Brasil relataram ter sido alvo de tentativas de golpe ao menos uma vez por mês**, o que evidencia que os crimes cibernéticos deixaram de ser eventos esporádicos para se tornarem um **fenômeno cotidiano e massivo**.

Chamou atenção para o fato de que **66% das vítimas não confiam nas autoridades para denunciar os crimes**, sobretudo por três razões: percepção de que a denúncia "não dará em nada", dificuldade operacional para registrar a ocorrência e desconhecimento sobre o canal apropriado de denúncia. Além disso, **61% dos golpes se concretizam em menos de 24 horas após o primeiro contato com a vítima**, indicando a agilidade e sofisticação das fraudes.

O impacto econômico estimado, segundo Volochko, é da ordem de **R$ 297,7 bilhões por ano**, com **apenas 4% de recuperação efetiva dos valores perdidos pelas vítimas**. Destacou também que **57% das vítimas têm mais de 54 anos**, o que reforça a preocupação com o grupo de idosos — *frequentemente exposto a perdas financeiras e fragilizado pela vergonha de admitir que caiu em um golpe, o que alimenta um ciclo de subnotificação e impunidade*.

Diante desses dados, propôs a implementação de sete medidas: (i) campanhas permanentes de conscientização pública; (ii) simplificação e padronização nacional dos boletins de ocorrência; (iii) ampliação da colaboração público-privada; (iv) criação de um suporte estruturado para acolhimento e orientação de vítimas; (v) melhoria dos mecanismos de recuperação financeira; (vi) uso de inteligência artificial e big data em sistemas de detecção e prevenção de fraudes; e (vii) criação de um banco nacional de golpes acessível ao público para consulta e prevenção em tempo real.

Além disso, sugeriu alterações legislativas, como a atualização dos tipos penais para abranger as condutas descritas na Convenção de Budapeste sobre o Crime Cibernético, da qual o Brasil é signatário; a revisão da competência territorial para crimes cometidos em ambiente digital – *atualmente atrelada à residência da vítima, nos termos do Código de Processo Penal* – ; e a transformação da ação penal condicionada à representação em ação penal pública incondicionada para os crimes digitais de maior impacto coletivo.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br