SENADO FEDERAL

PROJETO DE LEI
Nº 4752, DE 2025

Institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018.

AUTORIA: Senador Esperidião Amin (PP/SC), Senador Astronauta Marcos Pontes (PL/SP), Senador Chico Rodrigues (PSB/RR), Senador Jorge Seif (PL/SC), Senador Sergio Moro (UNIÃO/PR)

Página da matéria

SENADO FEDERAL
Gabinete do Senador **ESPERIDIÃO AMIN**

PROJETO DE LEI Nº , DE 2025

Institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018.

O CONGRESSO NACIONAL decreta:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Lei institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018.

Art. 2º São objetivos do Marco Legal da Cibersegurança:

I – fortalecer a resiliência cibernética da administração pública direta e indireta, em todos os entes da federação;

II – prevenir, mitigar e responder a incidentes cibernéticos de forma coordenada;

III – promover a integração entre políticas de segurança da informação, proteção de dados e cibersegurança;

IV – estimular a formação e retenção de recursos humanos especializados;

V – fomentar o desenvolvimento de capacidades técnicas e operacionais para defesa cibernética no setor público;

VI – estabelecer mecanismos de financiamento estáveis e sustentáveis para as ações de segurança digital; e

VII – estimular a cooperação e o estabelecimento de parcerias entre o setor público, o setor privado e a sociedade civil organizada.

Art. 3º As políticas públicas de cibersegurança devem observar as seguintes diretrizes, que orientam a atuação dos órgãos e entidades abrangidos por esta Lei:

I – prevenção e mitigação de riscos: promover estratégias e ações preventivas, contínuas e atualizadas, para identificação, análise, redução e controle de vulnerabilidades e ameaças cibernéticas;

II – resposta coordenada a incidentes: estabelecer protocolos claros e mecanismos de comunicação eficazes para detecção, reporte, tratamento e recuperação diante de incidentes cibernéticos, garantindo agilidade, transparência e integração dos esforços públicos e privados;

III – promoção da cultura de cibersegurança: incentivar a educação, a conscientização e a mudança de comportamento de servidores públicos, gestores, cidadãos e parceiros, a fim de criar ambiente institucional e social resiliente às ameaças digitais;

IV – fomento à inovação, à pesquisa e ao desenvolvimento nacional: estimular a criação, o desenvolvimento e a adoção de soluções tecnológicas inovadoras, favorecendo o fomento à produção científica e tecnológica nacional;

V – cooperação entre o setor público, o setor privado e terceiro setor: construir parcerias estratégicas e compartilhar informações, boas práticas e inteligência, com vistas ao fortalecimento da resiliência nacional e à promoção da confiança mútua entre os setores;

VI – proteção das infraestruturas críticas e dos serviços essenciais: identificar, classificar e proteger de forma especial os ativos, sistemas e processos considerados essenciais para a continuidade dos serviços públicos e da ordem econômica e social;

VII – valorização da educação e da formação de recursos humanos especializados: criar e manter programas de atualização profissional, capacitação técnica e formação acadêmica para profissionais de cibersegurança, promovendo a atração e retenção de talentos;

VIII – integração de ações nos diferentes níveis e setores da administração pública: articular e harmonizar as iniciativas de cibersegurança em âmbito federal, estadual, distrital e municipal, respeitando competências e promovendo sinergias intersetoriais;

IX – atualização normativa e tecnológica contínua: revisar e aprimorar periodicamente as normas, procedimentos e tecnologias utilizadas, acompanhando a publicização de vulnerabilidades, a evolução das ameaças e tendências globais em cibersegurança;

X – promoção de parcerias nacionais e internacionais: buscar ativamente colaborações, convênios e projetos conjuntos com países, organismos internacionais, redes de pesquisa e centros de excelência em cibersegurança;

XI – priorização do interesse público e dos direitos fundamentais: garantir que todas as ações e políticas de cibersegurança respeitem e protejam os direitos fundamentais, a privacidade e o interesse público, em conformidade com a Constituição Federal;

XII – estabelecimento do princípio da transversalidade no interesse da administração pública: assegurar que a cibersegurança permeie todos os setores, políticas e níveis da administração pública, integrando esforços e responsabilidades de forma compartilhada, em benefício da resiliência institucional e da proteção do interesse público;

XIII – responsabilização dos gestores e agentes públicos: responsabilizar os gestores e agentes públicos pela implementação, supervisão e reporte das políticas e incidentes de cibersegurança, garantindo a observância dos padrões mínimos definidos com base nesta Lei, de acordo com as respectivas atribuições e na forma da legislação funcional a que estiverem submetidos;

XIV – integração da cadeia de fornecimento: promover a adoção de padrões mínimos de cibersegurança por parte de fornecedores e parceiros contratuais, incorporando a avaliação de riscos da cadeia de suprimentos aos programas de resiliência digital; e

XV – garantia da continuidade das comunicações digitais: assegurar a continuidade e a confiabilidade dos meios digitais de comunicação, especialmente em contextos de crise, como componente essencial da resiliência cibernética e da soberania tecnológica da administração pública.

Parágrafo único. As diretrizes estabelecidas neste artigo devem ser observadas na formulação, na execução, no monitoramento e na avaliação das políticas, dos programas e das ações de cibersegurança, integrando-se, sempre que possível, às demais políticas públicas relacionadas.

CAPÍTULO II
DA AUTORIDADE NACIONAL DE CIBERSEGURANÇA

Art. 4º Compete à autoridade nacional de cibersegurança, designada em regulamento, exercer as funções de normatização complementar, fiscalização, auditoria e instrução de processos administrativos, nos termos desta Lei.

Art. 5º A autoridade nacional de cibersegurança estabelecerá e revisará periodicamente padrões mínimos de cibersegurança, abrangendo controles técnicos, organizacionais e processuais, com base em normas nacionais e internacionais reconhecidas.

Parágrafo único. Os padrões mínimos serão objeto de consulta pública prévia, e sua observância será critério para participação no Programa Nacional de Segurança e Resiliência Digital e acesso aos recursos previstos nesta Lei.

CAPÍTULO III
DO PROGRAMA NACIONAL DE SEGURANÇA E RESILIÊNCIA DIGITAL

Seção I
Dos Participantes

Art. 6º Fica instituído o Programa Nacional de Segurança e Resiliência Digital, no âmbito da administração pública federal direta e indireta.

Art. 7º Os estados, o Distrito Federal e os municípios poderão aderir ao Programa Nacional de Segurança e Resiliência Digital mediante assinatura de termo de adesão, nos termos definidos em regulamento, comprometendo-se a implementar as diretrizes, objetivos e instrumentos previstos nesta Lei.

Art. 8º A adesão de organizações do setor privado e do terceiro setor poderá ocorrer por meio de acordos de cooperação, convênios ou parcerias, conforme regulamentação.

Seção II
Dos Objetivos

Art. 9º O Programa Nacional de Segurança e Resiliência Digital tem os seguintes objetivos:

I – implementar os princípios e diretrizes estabelecidos por esta Lei, articulando as políticas e ações de resiliência cibernética em âmbito nacional;

II – estabelecer planos nacionais, estaduais, distritais e municipais de resiliência cibernética, definidos de acordo com critérios técnicos, estratégicos e de risco;

III – definir metas plurianuais e indicadores de desempenho para avaliação da efetividade das ações;

IV – estimular a adesão voluntária de entes federativos e de organizações do setor privado, mediante instrumentos de cooperação, convênios ou parcerias;

V – promover a integração das ações dos diversos setores críticos, garantindo abordagem setorial para saúde, educação, finanças, energia, telecomunicações, transportes, meio ambiente, defesa, segurança pública, entre outros;

VI – garantir atualização periódica dos planos e ações, de acordo com a evolução tecnológica e as novas ameaças identificadas;

VII – fomentar a troca de experiências e boas práticas entre órgãos, entidades e parceiros, nos âmbitos nacional e internacional; e

VIII – qualificar a investigação e o combate ao crime cibernético, a partir da adoção das medidas de segurança previstas nesta Lei, pelos setores público e privado.

Seção III
Dos Instrumentos Operacionais

Art. 10. Para o cumprimento de seus objetivos, o Programa Nacional de Segurança e Resiliência Digital disporá dos seguintes instrumentos operacionais:

I – elaboração e execução de planos setoriais e temáticos de resiliência cibernética;

II – criação de protocolos, manuais e guias de boas práticas para prevenção, detecção, resposta e recuperação de incidentes cibernéticos;

III – implantação de sistemas de monitoramento, alerta e reporte de incidentes de segurança digital;

IV – promoção de campanhas de conscientização e educação em cibersegurança voltadas à sociedade e aos servidores públicos;

V – estabelecimento de mecanismos de adesão voluntária dos entes federativos e de pessoas jurídicas de direito privado, incluindo incentivos e contrapartidas; e

VI – definição de indicadores de desempenho, sistemas de monitoramento, avaliação e revisão periódica das ações do programa.

Seção IV
Dos Compromissos

Art. 11. A participação dos estados, do Distrito Federal e dos municípios no Programa Nacional de Segurança e Resiliência Digital estará associada ao compromisso de desenvolvimento e implementação de iniciativas próprias de cibersegurança que compreendam, entre outros, os seguintes elementos:

I – elaboração e implementação de planos locais ou setoriais de cibersegurança, alinhados às diretrizes nacionais;

II – criação ou fortalecimento de equipes de resposta a incidentes de cibersegurança, próprias ou consorciadas, para atuar na prevenção, detecção e resposta a incidentes em seus âmbitos de competência;

III – promoção de ações de capacitação e formação continuada de servidores e gestores públicos na área de cibersegurança;

IV – adoção de procedimentos padronizados de reporte e comunicação de incidentes, compartilhando informações relevantes com a autoridade nacional de cibersegurança e com demais entes federativos; e

V – integração a fóruns, conselhos e grupos de trabalho regionais e nacionais para intercâmbio de informações, desenvolvimento de projetos conjuntos e harmonização de políticas.

Parágrafo único. Os planos de cibersegurança serão elaborados de acordo com as diretrizes e orientações da autoridade nacional de cibersegurança e compreenderão os seguintes elementos:

I – política de continuidade de serviços;

II – plano de resposta a incidentes;

III – inventário de ativos críticos;

IV – estrutura de governança e responsáveis; e

V – plano de adequação aos padrões mínimos definidos pela autoridade nacional de cibersegurança.

Art. 12. Os órgãos e entidades da administração pública federal e os entes federativos participantes do Programa Nacional de Segurança e Resiliência Digital devem notificar a autoridade nacional de cibersegurança sobre a ocorrência de incidentes de cibersegurança relevantes conforme os prazos, critérios e procedimentos por ela definidos.

§ 1º A autoridade nacional de cibersegurança definirá os critérios de relevância, a forma, o conteúdo mínimo das notificações e os mecanismos de comunicação segura, preservando-se o sigilo das informações sensíveis e estratégicas.

§ 2º A autoridade nacional de cibersegurança estabelecerá os prazos, critérios e procedimentos para a comunicação de incidentes de segurança cibernética pelas entidades do setor privado participantes do Programa Nacional de Segurança e Resiliência Digital.

Seção V
Da Governança de Riscos na Cadeia de Suprimentos

Art. 13. Os órgãos e entidades da administração pública federal e os entes federativos participantes do Programa Nacional de Segurança e Resiliência Digital devem integrar a avaliação, o monitoramento e a mitigação de riscos cibernéticos de seus fornecedores, subcontratados, parceiros e demais entidades da cadeia de suprimentos aos seus programas internos de resiliência cibernética.

§ 1º A avaliação de risco deverá abranger fornecedores, subcontratados, parceiros tecnológicos e prestadores de serviços externos, independentemente do nível de terceirização ou externalização das funções.

§ 2º A gestão de riscos na cadeia de suprimentos deverá considerar o ciclo completo de vida do produto ou serviço contratado, incluindo suporte, atualizações de segurança e correções de vulnerabilidades conhecidas.

§ 3º A responsabilidade pelos riscos advindos da cadeia de suprimentos será compartilhada entre os entes contratantes e os respectivos fornecedores, conforme estabelecido em contratos, termos de adesão ou regulamentos específicos.

Art. 14. A adoção de soluções tecnológicas, sistemas, plataformas ou serviços por parte dos órgãos, entidades e entes federativos abrangidos no âmbito do Programa Nacional de Segurança e Resiliência Digital deverá considerar a demonstração de conformidade com os padrões mínimos de cibersegurança definidos pela autoridade nacional de cibersegurança, inclusive no que se refere ao ciclo de vida de desenvolvimento seguro, atualizações regulares e suporte técnico ativo.

§ 1º Sempre que possível, deverão ser priorizados fornecedores e tecnologias nacionais compatíveis com os princípios desta Lei, observados os requisitos de soberania, transparência e rastreabilidade da cadeia e o disposto na Lei nº 14.133, de 1º de abril de 2021.

§ 2º A autoridade nacional de cibersegurança poderá estabelecer restrições à adoção de soluções descontinuadas, sem suporte técnico, sem atualizações regulares ou com histórico de falhas de segurança.

§ 3º A autoridade nacional de cibersegurança poderá instituir mecanismos de classificação de risco por fornecedor, inclusive com base em auditorias, notificações anteriores de incidentes, sanções já aplicadas e grau de aderência às políticas públicas de cibersegurança, com vistas à construção de um índice nacional de maturidade e confiabilidade da cadeia de suprimentos em cibersegurança, disponível em plataforma pública e acessível aos entes federativos participantes do Programa Nacional de Segurança e Resiliência Digital.

§ 4º A autoridade nacional de cibersegurança deverá publicar e atualizar, periodicamente, requisitos mínimos e listas de conformidade, considerando os seguintes critérios, entre outros que se mostrarem relevantes:

I – conformidade com normas, recomendações e boas práticas nacionais e internacionais reconhecidas;

II – existência de plano de resposta a incidentes integrado à cadeia de fornecedores;

III – auditorias periódicas e evidências de conformidade em segurança da informação; e

IV – mecanismos de rastreabilidade e verificação da integridade dos componentes utilizados.

Art. 15. Os incidentes de cibersegurança cuja origem ou exploração envolva falhas ou brechas em fornecedores e parceiros deverão ser reportados nos prazos e formatos definidos pela autoridade nacional de cibersegurança.

Seção VI
Do Acesso a Recursos

Art. 16. A adesão ao Programa Nacional de Segurança e Resiliência Digital conferirá acesso prioritário aos recursos do Fundo Nacional de Segurança Pública destinados à cibersegurança, a programas de capacitação, a sistemas de alerta e resposta, bem como a iniciativas de cooperação técnica nacional e internacional.

Parágrafo único. O acesso aos recursos do Fundo Nacional de Segurança Pública destinados à cibersegurança pode ser concedido a projetos de modernização, inovação, pesquisa e desenvolvimento realizados em regime de cooperação público-privada, desde que observados os critérios técnicos, de interesse público e conformidade com esta Lei.

Art. 17. O acesso aos recursos do Fundo Nacional de Segurança Pública destinados à cibersegurança será prioritário para entes que comprovarem a elaboração e implementação dos planos, a criação de equipes técnicas e a adesão às diretrizes nacionais.

Parágrafo único. A participação ativa em ações colaborativas e projetos intergovernamentais poderá ser considerada como critério de avaliação e priorização no repasse de recursos e na seleção de parcerias.

Seção VII
Da Articulação

Art. 18. Serão instituídos conselhos, fóruns e grupos de trabalho permanentes, em âmbito nacional, regional e local, destinados à integração de políticas, compartilhamento de inteligência, articulação de respostas coordenadas e construção de consensos técnicos.

§ 1º A autoridade nacional de cibersegurança promoverá a realização de encontros, oficinas, treinamentos e exercícios conjuntos, visando fortalecer a cooperação entre os entes federativos.

§ 2º A integração federativa incluirá, sempre que possível, a participação do setor privado, da academia e da sociedade civil, observadas as regras de confidencialidade e segurança da informação.

Seção VIII
Da Formação, da Pesquisa e da Inovação em Cibersegurança

Art. 19. Os participantes do Programa Nacional de Segurança e Resiliência Digital, no âmbito de suas atribuições, devem envidar esforços para:

I – criar e promover programas continuados de capacitação, treinamento e atualização em cibersegurança para servidores públicos, gestores e demais profissionais envolvidos na execução das políticas de cibersegurança;

II – fomentar parcerias com as entidades integrantes do Sistema S, universidades, institutos federais, centros de pesquisa e o setor privado, com o objetivo de ampliar a oferta e o alcance dos cursos, especializações, certificações e eventos de capacitação;

III – incentivar a inclusão de conteúdos de cibersegurança nas grades curriculares de ensino técnico, superior e de pós-graduação, para promover a conscientização desde a formação básica até a especialização profissional; e

IV – priorizar a formação de multiplicadores e de equipes técnicas capacitadas para atuação em resposta a incidentes, gestão de riscos, proteção de dados e governança digital.

Art. 20. As políticas públicas de ciência, tecnologia e inovação dos entes participantes do Programa Nacional de Segurança e Resiliência Digital devem compreender o fomento ao desenvolvimento do conhecimento e de soluções inovadoras na área de cibersegurança, por meio das seguintes ações:

I – apoio a projetos de pesquisa, desenvolvimento e inovação voltados à cibersegurança, em parceria com instituições científicas, tecnológicas e de inovação, empresas e organizações do terceiro setor;

II – estímulo à criação de centros de excelência, laboratórios de testes e ambientes de simulação para experimentação e validação de soluções nacionais em segurança digital;

III – editais de fomento, concessão de bolsas, prêmios e incentivos à pesquisa, ao desenvolvimento e à inovação, priorizando áreas estratégicas para a proteção de infraestruturas críticas e serviços essenciais; e

IV – incentivo à transferência de tecnologia, à incubação de startups, ao empreendedorismo e à difusão de boas práticas em cibersegurança entre diferentes setores produtivos.

Art. 21. Os programas, ações e incentivos previstos nesta seção devem ser articulados com as políticas públicas de educação e de ciência,

tecnologia e inovação, integrando-se a estratégias de desenvolvimento econômico, inclusão digital e proteção de direitos fundamentais.

Seção IX
Do Monitoramento e da Avaliação

Art. 22. O Programa Nacional de Segurança e Resiliência Digital será objeto de monitoramento contínuo, com publicação periódica de indicadores, metas, resultados alcançados e ajustes necessários, visando à melhoria da resiliência cibernética nacional.

Parágrafo único. Caberá à autoridade nacional de cibersegurança revisar, a cada ciclo plurianual, os planos e metas, propondo ajustes com base em relatórios de avaliação e na evolução do cenário de ameaças.

Art. 23. A avaliação da efetividade do Programa Nacional de Segurança e Resiliência Digital deve considerar, entre outros, os seguintes critérios:

I – grau de adesão dos entes federativos: mensurar o número e o percentual de entes da federação participantes e em conformidade com os requisitos do programa;

II – evolução da maturidade cibernética institucional: avaliar o progresso dos órgãos e entidades em modelos reconhecidos de maturidade em cibersegurança;

III – tempo médio de resposta e recuperação a incidentes: medir a eficiência na detecção, resposta e restabelecimento das operações após incidentes cibernéticos;

IV – redução do número e do impacto de incidentes reportados: comparar dados históricos de incidentes para verificar a efetividade das ações preventivas e corretivas implementadas;

V – capacitação e certificação de recursos humanos: monitorar o número de servidores, gestores e profissionais treinados ou certificados em cibersegurança a cada ciclo de avaliação;

VI – implementação de planos setoriais e temáticos de resiliência cibernética: aferir a elaboração, atualização e operacionalização dos planos específicos por setor ou tema;

VII – conformidade com boas práticas e normas técnicas de segurança: verificar a adoção de políticas, normas e padrões reconhecidos, tais como autenticação forte, cópias de segurança e gestão de vulnerabilidades;

VIII – eficiência e impacto da utilização de recursos públicos: analisar o volume, o destino, a eficiência e os resultados gerados pelos recursos aplicados no âmbito do programa;

IX – participação em exercícios, treinamentos e simulações de incidentes: avaliar a frequência, a abrangência e os resultados das atividades práticas promovidas pelo programa;

X – grau de integração e cooperação com redes nacionais e internacionais: mensurar a participação ativa em fóruns, iniciativas conjuntas e compartilhamento de inteligência com entidades externas; e

XI – promoção da cultura de cibersegurança: aferir o nível de conscientização e mudança de comportamento de servidores, gestores e sociedade por meio de pesquisas, auditorias ou métricas de treinamento.

Art. 24. A autoridade nacional de cibersegurança definirá e publicará indicadores de desempenho, eficiência, economicidade, eficácia e impacto das políticas e ações de cibersegurança, com atualização periódica.

§ 1º Os resultados dos indicadores serão apresentados em linguagem acessível, com comparativos históricos e metas futuras.

§ 2º Será assegurada a participação da sociedade civil e de especialistas na avaliação dos resultados, por meio de consultas, audiências ou grupos de trabalho específicos.

Seção X
Da Transparência, do Controle e da Prestação de Contas

Art. 25. Os órgãos e entidades responsáveis pela aplicação dos recursos previstos no âmbito do Programa Nacional de Segurança e Resiliência Digital devem:

I – publicar, anualmente, relatório detalhado das receitas, despesas e resultados alcançados pelos recursos destinados à cibersegurança;

II – submeter suas contas à auditoria interna e externa, de acordo com as normas vigentes e os procedimentos estabelecidos pelos respectivos sistemas de controle;

III – disponibilizar informações atualizadas em portais eletrônicos de acesso público, respeitadas as normas de sigilo e proteção de dados sensíveis; e

IV – garantir a participação e o controle social por meio de conselhos, audiências públicas e outros instrumentos de diálogo e fiscalização.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 26. A Lei nº 13.756, de 12 de dezembro de 2018, passa a vigorar com as seguintes alterações:

"**Art. 5º**

.....

.....

..

§ 5º No mínimo, 3% (três por cento) dos recursos empenhados do Fundo Nacional de Segurança Pública deverão ser aplicados em ações de cibersegurança, observadas as seguintes prioridades:

I – financiamento de projetos e programas de modernização tecnológica da administração pública;

II – formação, capacitação e certificação de recursos humanos em cibersegurança;

III – apoio à pesquisa, desenvolvimento e inovação em tecnologias de cibersegurança;

IV – fortalecimento de estruturas e operações dos centros de resposta e equipes de tratamento de incidentes cibernéticos;

V – apoio a estados, Distrito Federal e municípios para a execução de suas políticas e planos locais de cibersegurança; e

VI – realização de campanhas de educação e conscientização para a sociedade.” (NR)

“**Art. 30.** .....

.....

§ 1º-A. Do produto da arrecadação após a dedução das importâncias de que tratam os incisos III e V do *caput* deste artigo, 86% (oitenta e seis por cento) serão destinados à cobertura de despesas de custeio e manutenção do agente operador da loteria de apostas de quota fixa e demais jogos de apostas, excetuadas as modalidades lotéricas previstas nesta Lei, 2% (dois por cento) serão destinados ao FNSP para ações na área de cibersegurança e sem prejuízo da destinação prevista na alínea *a* do inciso II, e 12% (doze por cento) terão as seguintes destinações:

.....” (NR)

Art. 27. Esta Lei entra em vigor na data de sua publicação.

Parágrafo único. O art. 26 desta Lei produzirá efeitos a partir do primeiro dia do quarto mês subsequente ao de sua publicação.

JUSTIFICAÇÃO

O Brasil tem enfrentado uma escalada de incidentes cibernéticos que afetam a prestação de serviços públicos, expõem dados

sensíveis de milhões de cidadãos e colocam em risco a estabilidade institucional de diversos órgãos e entidades da federação. Esses episódios evidenciam a fragilidade das estruturas nacionais diante de ameaças cada vez mais sofisticadas, persistentes e com forte impacto geopolítico. Globalmente, os crescentes prejuízos decorrentes de ciberataques têm levado governos a estruturarem marcos legais, investir em recursos humanos e criar órgãos permanentes para coordenar a segurança cibernética.

Nesse contexto, cumpre chamar a atenção para a posição isolada do Brasil. Sendo a décima maior economia do planeta, o país é praticamente a única entre as vinte maiores do mundo que ainda não consolidou um arcabouço normativo com força de lei para sustentar uma política de Estado nessa área. Embora existam avanços importantes, como a Política e a Estratégia Nacionais de Cibersegurança, essas iniciativas carecem de suporte legal e financeiro, não vinculam os entes federativos e não possuem mecanismos de indução estruturante para sua efetiva implementação.

É com o propósito de sanar essa lacuna que a presente proposição legislativa busca instituir o Marco Legal da Cibersegurança. A proposta nasce com a ambição de estabelecer um arcabouço normativo estruturante, com foco em objetivos claros e diretrizes estratégicas. Adicionalmente, propõe-se a criação do Programa Nacional de Resiliência Digital, de cunho executivo e operacional, com a ambição de engajar não apenas os órgãos e entidades da administração pública federal, mas também os estados, o Distrito Federal, os municípios e entidades do setor privado que atuam em serviços públicos essenciais e infraestruturas críticas.

A proposição também enfrenta o tema da autoridade nacional de cibersegurança. Trata-se de lacuna fundamental na área de cibersegurança no Brasil, apontada em relatórios de avaliação tanto do Tribunal de Contas da União como da própria Comissão de Relações Exteriores e Defesa Nacional do Senado Federal. Nesse contexto, a construção de um modelo institucional apto a lidar com um cenário de riscos e ameaças crescentes é discussão que não pode mais ser adiada.

Propõe-se ainda a vinculação de recursos oriundos das receitas dos operadores de apostas de quota fixa, por intermédio do Fundo Nacional de Segurança Pública, ao fomento de ações de cibersegurança, com o

objetivo de assegurar recursos para modernização tecnológica, capacitação de pessoal e fortalecimento da resposta a incidentes.

Trata-se de um passo estratégico e necessário para mitigar riscos cibernéticos estruturais, garantir a integridade das funções públicas essenciais e proteger a sociedade brasileira de danos imensuráveis. Visando contribuir para o fortalecimento da segurança cibernética em âmbito nacional, a proposta constitui instrumento adequado e urgente para reposicionar o Brasil na vanguarda da governança digital global.

Submetemos, portanto, a proposta ao exame de nossos pares, certos de sua aprovação e possível aperfeiçoamento.

Sala das Sessões,

Senador ESPERIDIÃO AMIN

LEGISLAÇÃO CITADA

- Constituição de 1988 - CON-1988-10-05 - 1988/88
  https://normas.leg.br/?urn=urn:lex:br:federal:constituicao:1988;1988
- Lei nº 13.756, de 12 de Dezembro de 2018 - LEI-13756-2018-12-12 - 13756/18
  https://normas.leg.br/?urn=urn:lex:br:federal:lei:2018;13756
- Lei nº 14.133, de 1º de Abril de 2021 - Lei de Licitações e Contratos Administrativos (2021) - 14133/21
  https://normas.leg.br/?urn=urn:lex:br:federal:lei:2021;14133