Oficio_nº004_2026

Brasília – DF, 08 de julho de 2026.

Aos Excelentíssimos Senhores Senadores
FLÁVIO ARNS
Presidente da Comissão de Ciência, Tecnologia, Inovação e Informática (CCT) do Senado Federal

HERMES KLANN
Relator do PL 4752/2026 na CCT

ESPERIDIÃO AMIN
Autor do PL 4752/2026

Ref.: Contribuições ao PL 4752/2026 – Marco Legal da Cibersegurança.

Excelentíssimos Senadores,

A **Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação – CONFEDERAÇÃO ASSESPRO**, entidade representativa de milhares de empresas do setor de tecnologia da informação em todo o território nacional, vem, respeitosamente, manifestar-se acerca dos debates legislativos em curso relacionados ao **Projeto de Lei nº 4.752, de 2026**, que "*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*".

A Assespro reconhece o elevado mérito da proposta, especialmente por estabelecer diretrizes nacionais para fortalecimento da resiliência cibernética, incentivar a formação de recursos humanos especializados, estruturar mecanismos de governança e promover a integração entre o setor público, a academia e a iniciativa privada.

A entidade tem participado ativamente das discussões sobre o tema junto ao Poder Executivo, possuindo assento de titular e suplente no Comitê Nacional de Cibersegurança (CNCiber), como também em todas as atividades realizadas sobre o tema no âmbito do Senado Federal, incluindo as reuniões e eventos da Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética, bem como da audiência pública promovida no último dia 30 de junho de 2026 pela Comissão de Ciência, Tecnologia, Inovação e Informática (CCT) do Senado Federal. Nessas ocasiões, tem defendido a urgência da aprovação de uma legislação inicial sobre o tema para dotar o país dos instrumentos necessários para proteção de seus cidadãos, empresas e soberania diante dos crescentes ataques cibernéticos domésticos e internacionais.

Entendemos que há convergência entre o texto do PL 4752/2025 e a proposta elaborada pelo Comitê Nacional de Cibersegurança (CNCiber), observando que integração das duas iniciativas é o caminho mais adequado para a construção de uma política nacional efetiva de cibersegurança.

Observando estritamente o PL 4752/2025, entendemos que este possa ser aperfeiçoado em dois aspectos estratégicos para o fortalecimento da capacidade tecnológica nacional.

O **primeiro** consiste na **criação de um programa permanente voltado ao desenvolvimento de capacidades nacionais em cibersegurança e inteligência artificial**, transformando investimentos públicos em inovação,

SRTVS - QUADRA 701 - BLOCO A - SALAS 829/831 - EDIFÍCIO CENTRO EMPRESARIAL BRASÍLIA - | CEP 70340-907 - BRASÍLIA/DF
FONE: + 55 (61) 3201-0932 WWW.ASSESPRO.ORG.BR @CONFEDERAÇAOASSESPRO

propriedade intelectual, fortalecimento da indústria nacional e geração de competências tecnológicas permanentes.

O **segundo** propõe o **aperfeiçoamento do modelo sancionatório** previsto no Projeto, privilegiando uma atuação orientada à conformidade, na qual a autoridade reguladora atue prioritariamente como indutora de boas práticas, reservando as sanções mais gravosas às hipóteses de dolo, fraude, reincidência ou negligência grave.

Essas propostas preservam integralmente os objetivos do Projeto de Lei e reforçam sua capacidade de promover, simultaneamente, segurança nacional, desenvolvimento tecnológico, inovação e crescimento econômico.

1. DESENVOLVIMENTO DE CAPACIDADES NACIONAIS EM CIBERSEGURANÇA E INTELIGÊNCIA ARTIFICIAL

O PL 4752/2025 contempla importantes mecanismos destinados ao fortalecimento da pesquisa, da inovação, da formação de recursos humanos e da cooperação entre os diversos atores do ecossistema de cibersegurança. Contudo, ainda existe oportunidade para incorporar instrumentos capazes de transformar esses investimentos em uma política permanente de desenvolvimento de capacidades nacionais.

A cibersegurança deixou de ser apenas uma atividade destinada à proteção de sistemas computacionais para assumir papel estratégico na segurança nacional, na proteção das infraestruturas críticas, na competitividade econômica e na autonomia tecnológica dos Estados. Da mesma forma, a inteligência artificial tornou-se elemento central das modernas plataformas de segurança digital, ampliando significativamente a capacidade de prevenção, detecção e resposta a incidentes.

Observa-se, simultaneamente, crescente concentração mundial da capacidade computacional, dos modelos de inteligência artificial, da propriedade intelectual e das plataformas de cibersegurança em um número reduzido de fornecedores internacionais. Essa concentração amplia dependências tecnológicas, aumenta riscos relacionados à cadeia global de suprimentos e reduz a autonomia dos países na proteção de seus ativos estratégicos.

O Brasil possui um ecossistema consolidado de empresas de tecnologia, composto majoritariamente por micro, pequenas e médias empresas altamente inovadoras. Essas organizações desenvolvem soluções competitivas, geram propriedade intelectual, formam profissionais especializados e desempenham papel relevante na segurança digital do País. Entretanto, parcela significativa dos investimentos públicos continua destinada à aquisição de tecnologias desenvolvidas no exterior, limitando o efeito multiplicador desses recursos sobre a economia brasileira.

Um dos principais desafios da inovação nacional consiste na superação do chamado "vale da morte" da inovação. Embora o Brasil disponha de importantes instrumentos de apoio à pesquisa e ao desenvolvimento tecnológico, muitas soluções nacionais não conseguem atingir escala comercial por inexistência de demanda estruturante.

Nesse contexto, o poder de compra do Estado representa um dos mais relevantes instrumentos de política pública para o desenvolvimento tecnológico. Quando utilizado de forma estratégica, permite transformar investimentos em pesquisa em inovação aplicada, geração de empregos qualificados, fortalecimento da indústria nacional, ampliação da propriedade intelectual brasileira e redução de dependências tecnológicas consideradas estratégicas.

SRTVS - QUADRA 701 - BLOCO A - SALAS 829/831 - EDIFÍCIO CENTRO EMPRESARIAL BRASÍLIA - | CEP 70340-907 - BRASÍLIA/DF
FONE: + 55 (61) 3201-0932 WWW.ASSESPRO.ORG.BR @CONFEDERAÇAOASSESPRO

A presente proposta não busca estabelecer mecanismos de reserva de mercado nem restringir a competição internacional. Seu objetivo é criar condições para o desenvolvimento de capacidades nacionais, permitindo que empresas brasileiras possam competir em igualdade de condições e que os investimentos públicos contribuam para ampliar a capacidade tecnológica instalada no País.

Propõe-se, assim, a criação do Programa Nacional de Desenvolvimento de Capacidades Nacionais em Cibersegurança e Inteligência Artificial (ProCiber-IA), destinado a promover a integração entre governo, universidades, Instituições Científicas, Tecnológicas e de Inovação (ICTs), centros de pesquisa e empresas brasileiras, fortalecendo continuamente as competências nacionais necessárias à proteção das infraestruturas críticas e dos sistemas estratégicos.

Proposta de Redação

Art. 21-A Fica instituído o Programa Nacional de Desenvolvimento de Capacidades Nacionais em Cibersegurança e Inteligência Artificial (ProCiber-IA), com a finalidade de fomentar o desenvolvimento tecnológico nacional, fortalecer a autonomia tecnológica do País e estimular a pesquisa, o desenvolvimento, a certificação, a produção e a adoção de soluções brasileiras de cibersegurança e inteligência artificial, prioritariamente destinadas à proteção das infraestruturas críticas e dos sistemas estratégicos da administração pública.

Art. 21-B O ProCiber-IA priorizará projetos destinados a:

I – ampliar as capacidades nacionais de pesquisa, desenvolvimento e inovação em cibersegurança e inteligência artificial;

II – desenvolver soluções de hardware e software por empresas brasileiras que detenham propriedade intelectual ou capacidade de desenvolvimento, suporte e evolução tecnológica no País;

III – fomentar modelos de inteligência artificial treinados em infraestrutura localizada no território nacional quando destinados ao tratamento de informações estratégicas ou sensíveis;

IV – incentivar soluções abertas, interoperáveis, auditáveis e aderentes às melhores práticas internacionais;

V – fortalecer laboratórios nacionais de pesquisa, testes, certificação e validação tecnológica;

VI – promover programas de transferência de tecnologia e formação de recursos humanos especializados.

Art. 21-C O Poder Executivo promoverá a destinação de recursos específicos ao ProCiber-IA, observadas as disponibilidades orçamentárias e financeiras, priorizando projetos desenvolvidos em parceria entre Instituições Científicas, Tecnológicas e de Inovação (ICTs), universidades, centros de pesquisa e empresas brasileiras de base tecnológica.

§ 1º Nas contratações públicas de soluções de cibersegurança e inteligência artificial realizadas pelos órgãos participantes do Programa Nacional de Segurança e Resiliência Digital, poderão ser considerados, como critérios técnicos de julgamento, fatores relacionados:

I – ao desenvolvimento de capacidades nacionais;

II – à geração de propriedade intelectual brasileira;

III – à capacidade de evolução tecnológica no País;

IV – à rastreabilidade da cadeia de suprimentos;

V – à auditabilidade e transparência das soluções;

SRTVS - QUADRA 701 - BLOCO A - SALAS 829/831 - EDIFÍCIO CENTRO EMPRESARIAL BRASÍLIA - | CEP 70340-907 - BRASÍLIA/DF
FONE: + 55 (61) 3201-0932 WWW.ASSESPRO.ORG.BR @CONFEDERAÇAOASSESPRO

VI – à redução de dependências tecnológicas consideradas estratégicas;

VII – à formação de competências técnicas e científicas no território nacional, observado o disposto na Lei nº 14.133, de 1º de abril de 2021.

Art. 21-D Fica vedada a aplicação dos recursos do programa em ferramentas que utilizem APIs, bibliotecas proprietárias ou serviços de computação em nuvem cuja propriedade intelectual ou controle acionário pertença a pessoas jurídicas sediadas em países que submetam o Brasil a legislação de controle ou sanção unilateral e outras medidas extrajurisdicionais, conforme definido em regulamento, ressalvados casos de licenciamento perpétuo com código-fonte depositado em repositório nacional.

2. MODELO SANCIONATÓRIO ORIENTADO À CONFORMIDADE

O texto atualmente apresentado do PL 4752/2025 não contempla, até o presente momento, um capítulo específico disciplinando infrações e sanções administrativas. Entretanto, considerando que a definição de mecanismos de responsabilização vem sendo objeto de discussões ao longo da tramitação da matéria e tende a integrar futuras versões do projeto, a Confederação Assespro entende oportuno apresentar contribuição voltada ao aperfeiçoamento desse tema, caso venha a ser incorporado ao texto final.

A efetividade do Marco Legal da Cibersegurança dependerá não apenas da definição de obrigações e da existência de mecanismos sancionatórios, mas principalmente da construção de um ambiente regulatório capaz de induzir a adoção contínua de boas práticas de segurança pelo setor público e privado.

A experiência nacional e internacional demonstra que modelos regulatórios baseados predominantemente em sanções tendem a produzir menor cooperação entre reguladores e regulados, desestimulando a comunicação voluntária de incidentes, a implementação tempestiva de medidas corretivas e o compartilhamento de informações relevantes para o fortalecimento da resiliência cibernética nacional.

Por outro lado, modelos regulatórios orientados à conformidade priorizam a prevenção, a orientação técnica e a melhoria contínua da maturidade em cibersegurança, reservando as medidas sancionatórias mais gravosas para situações em que haja dolo, fraude, reincidência, descumprimento reiterado das determinações da autoridade competente ou condutas caracterizadas por negligência grave.

Esse modelo torna-se particularmente relevante no setor de tecnologia da informação, composto majoritariamente por micro, pequenas e médias empresas inovadoras. Essas organizações desempenham papel essencial no desenvolvimento tecnológico nacional, na geração de propriedade intelectual, na formação de profissionais especializados e no fortalecimento do ecossistema brasileiro de cibersegurança. Devem, portanto, ser reconhecidas como parceiras estratégicas do Estado na construção da resiliência cibernética nacional.

A presente proposta não busca limitar a atuação fiscalizatória da futura autoridade nacional de cibersegurança, nem reduzir sua capacidade sancionatória. Seu objetivo é assegurar que eventual regime de responsabilização administrativa observe os princípios da proporcionalidade, razoabilidade, boa-fé, cooperação e incentivo à conformidade regulatória, distinguindo organizações que atuam de forma diligente e colaborativa daquelas que deliberadamente descumprem seus deveres legais.

Ao privilegiar medidas preventivas, orientadoras e corretivas sempre que compatíveis com a natureza da infração, o modelo proposto fortalece a cultura de segurança, estimula investimentos contínuos em cibersegurança, amplia a cooperação entre regulador e regulados e contribui para elevar o nível geral de proteção das infraestruturas digitais brasileiras.

SRTVS - QUADRA 701 - BLOCO A - SALAS 829/831 - EDIFÍCIO CENTRO EMPRESARIAL BRASÍLIA - | CEP 70340-907 - BRASÍLIA/DF
FONE: + 55 (61) 3201-0932 WWW.ASSESPRO.ORG.BR @CONFEDERAÇAOASSESPRO

Proposta de Redação

Art. XX A atuação sancionatória da autoridade nacional de cibersegurança observará os princípios da proporcionalidade, razoabilidade, boa-fé, cooperação e estímulo à conformidade regulatória, privilegiando, sempre que possível, medidas preventivas, orientadoras e corretivas em relação às sanções de natureza restritiva ou pecuniária.

§ 1º Na aplicação das sanções administrativas serão considerados, entre outros:

I – a gravidade da infração;

II – a boa-fé do agente;

III – a adoção prévia de medidas de segurança compatíveis com o porte da organização;

IV – a cooperação durante o processo de fiscalização;

V – as ações voluntárias de remediação;

VI – a capacidade econômica do infrator;

VII – o grau de maturidade em cibersegurança da organização.

§ 2º As sanções previstas nos incisos II, III, V, VI e VII do artigo correspondente serão aplicadas prioritariamente nas hipóteses de dolo, fraude, reincidência específica, descumprimento reiterado das determinações da autoridade competente ou quando a conduta revelar negligência grave capaz de comprometer a continuidade de serviços essenciais, infraestruturas críticas ou expor terceiros a riscos relevantes.

Certos de que podemos contar com atenção de Vossas Excelências para acatamento das sugestões apresentadas, colocamo-nos à disposição para continuar contribuindo com os debates legislativos e com a construção de políticas públicas modernas, equilibradas e promotoras da inovação, da soberania tecnológica e da segurança digital no Brasil.

Respeitosamente,

DEYBSON DE S. CIPRIANO
Presidente

RODRIGO JONAS FRAGOLA
Vice-Presidente de Articulação Política

A CONFEDERAÇÃO ASSESPRO

Fundada em **1976**, a ASSESPRO é uma entidade sem fins lucrativos, sediada em Brasília/DF, regida por seus Estatutos Sociais, criada com o intuito de representar de forma distinta e empreendedora, empresas privadas nacionais produtoras e desenvolvedoras de software, produtos e serviços de tecnologia da informação, telecomunicações e internet. Ao longo dessas quase quatro décadas, a entidade vem defendendo os interesses das empresas nacionais e a indústria nacional da tecnologia da informação.

Hoje com mais de **3.500 empresas** associadas em **todos os estados** do Brasil e com **14 entidades regionais**, a ASSESPRO assume cada vez mais esta posição de representante do setor junto aos governos municipais, estaduais e federal, junto a sociedade, e também perante as instituições de ensino, com o objetivo de integrar a comunidade acadêmica com a empresarial e contribuir para formação de pessoal capacitado para as demandas do mercado.

Nos últimos anos, a ASSESPRO tem se destacado no **debate dos principais temas de interesse do setor** de tecnologia da informação e inovação junto ao Congresso Nacional, Poder Judiciário e órgãos do Governo Federal, participando de inúmeras audiências públicas, seminários, reuniões de trabalho e outras atividades visando **contribuir para o aprimoramento das políticas públicas** desse importante segmento produtivo brasileiro.

SRTVS - QUADRA 701 - BLOCO A - SALAS 829/831 - EDIFÍCIO CENTRO EMPRESARIAL BRASÍLIA - | CEP 70340-907 - BRASÍLIA/DF
FONE: + 55 (61) 3201-0932 WWW.ASSESPRO.ORG.BR @CONFEDERAÇAOASSESPRO