SENADO FEDERAL

COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO E INFORMÁTICA

PAUTA DA 22ª REUNIÃO - SEMIPRESENCIAL

(4ª Sessão Legislativa Ordinária da 57ª Legislatura)

30/06/2026
TERÇA-FEIRA
às 11 horas

PRESIDENTE: Senador Flávio Arns
VICE-PRESIDENTE: Senador Hamilton Mourão

Comissão de Ciência, Tecnologia, Inovação e Informática

22ª REUNIÃO, EXTRAORDINÁRIA - SEMIPRESENCIAL, DA 4ª SESSÃO LEGISLATIVA ORDINÁRIA DA 57ª LEGISLATURA, A REALIZAR-SE EM

22ª REUNIÃO, EXTRAORDINÁRIA - SEMIPRESENCIAL

terça-feira, às 11 horas

SUMÁRIO

1ª PARTE - DELIBERATIVA

2ª PARTE - AUDIÊNCIA PÚBLICA INTERATIVA

COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO E INFORMÁTICA - CCT

PRESIDENTE: Senador Flávio Arns

Vice-Presidente : Antonio Hamilton Martins Mourão

(17 titulares e 17 suplentes)

TITULARES			SUPLENTES		
Bloco Parlamentar Democracia(MDB, PSDB, PODEMOS, UNIÃO)					
Confúcio Moura(MDB)(10)(7)	RO	3303-2470 / 2163	1 Alessandro Vieira(MDB)(10)(7)	SE	3303-9011 / 9014
Efraim Filho(PL)(10)	PB	3303-5934 / 5931	2 Esperidião Amin(PP)(10)(12)	SC	3303-6446 / 6447 / 6454
Ivete da Silveira(MDB)(10)(11)(2)(15)	SC	3303-2200	3 VAGO(10)(2)		
Marcos do Val(AVANTE)(10)(9)	ES	3303-6747 / 6753	4 VAGO(10)		
Oriovisto Guimarães(PSDB)(10)(8)	PR	3303-1635	5 VAGO(10)(8)		
Bloco Parlamentar da Resistência Democrática(PSB, PSD)					
Flávio Arns(PSB)(3)	PR	3303-6301	1 Cid Gomes(PSB)(17)(24)(26)	CE	3303-6460 / 6399
Daniella Ribeiro(PP)(3)	PB	3303-6788 / 6790	2 Sérgio Petecão(PSD)(3)	AC	3303-4086 / 6708 / 6709
Vanderlan Cardoso(PSD)(3)(16)(20)	GO	3303-2092 / 2099	3 Lucas Barreto(PSD)(3)	AP	3303-4851
Chico Rodrigues(PSB)(3)	RR	3303-2281	4 Nelsinho Trad(PSD)(19)	MS	3303-6767 / 6768
Bloco Parlamentar Vanguarda(PL, NOVO, AVANTE)					
Astronauta Marcos Pontes(PL)(1)	SP	3303-1177 / 1797	1 Carlos Portinho(PL)(1)	RJ	3303-6640 / 6613
Dra. Eudócia(PSDB)(1)	AL	3303-6083	2 Wellington Fagundes(PL)(1)	MT	3303-6219 / 3778 / 6209 / 6213 / 3775
Izalci Lucas(PL)(1)	DF	3303-6049 / 6050	3 Hermes Klann(PL)(22)(23)(25)(28)	SC	3303-3784 / 3756
Bloco Parlamentar Pelo Brasil(PDT, PT)					
Teresa Leitão(PT)(5)	PE	3303-2423	1 Randolfe Rodrigues(PT)(5)	AP	3303-6777 / 6568
Beto Faro(PT)(5)	PA	3303-5220	2 Paulo Paim(PT)(5)	RS	3303-5232 / 5231 / 5230 / 5235
Rogério Carvalho(PT)(18)	SE	3303-2201 / 2203	3 Weverton(PDT)(5)	MA	3303-4161 / 1655
Bloco Parlamentar Aliança(PP, REPUBLICANOS)					
Dr. Hiran(PP)(4)	RR	3303-6251	1 Laércio Oliveira(PP)(4)(27)	SE	3303-1763 / 1764
Hamilton Mourão(REPUBLICANOS)(4)(13)	RS	3303-1837	2 Damares Alves(REPUBLICANOS)(21)(4)(13)	DF	3303-3265

(1) Em 18.02.2025, os Senadores Astronauta Marcos Pontes, Dra. Eudócia e Izalci Lucas foram designados membros titulares, e os Senadores Carlos Portinho e Wellington Fagundes membros suplentes, pelo Bloco Parlamentar Vanguarda, para compor a Comissão (Of. 008/2025-BLVANG).

(2) Em 18.02.2025, o Senador Marcio Bittar foi designado membro titular, e o Senador Jayme Campos membro suplente, pelo Bloco Parlamentar Democracia, para compor a Comissão (Of. 12/2025-GLUNIAO).

(3) Em 18.02.2025, os Senadores Flávio Arns, Daniella Ribeiro, Vanderlan Cardoso e Chico Rodrigues foram designados membros titulares, e os Senadores Sérgio Petecão e Lucas Barreto membros suplentes, pelo Bloco Parlamentar da Resistência Democrática, para compor a Comissão (Of. 004/2025-GSEGAMA).

(4) Em 18.02.2025, os Senadores Dr. Hiran e Cleitinho foram designados membros titulares, e os Senadores Ciro Nogueira e Hamilton Mourão membros suplentes, pelo Bloco Parlamentar Aliança, para compor a Comissão (Of. 002/2025-GABLID/BLALIAN).

(5) Em 18.02.2025, os Senadores Teresa Leitão e Beto Faro foram designados membros titulares, e os Senadores Randolfe Rodrigues, Paulo Paim e Weverton membros suplentes, pelo Bloco Parlamentar Pelo Brasil, para compor a Comissão (Of. 026/2025-GLPDT).

(6) Em 19.02.2025, a Comissão reunida elegeu o Senador Flávio Arns Presidente deste colegiado (Of. 1/2025-SACCT).

(7) Em 19.02.2025, o Senador Confúcio Moura foi designado membro titular e o Senador Alessandro Vieira, membro suplente, pelo Bloco Parlamentar Democracia, para compor a comissão (Of. 015/2025-GLMDB).

(8) Em 19.02.2025, o Senador Oriovisto Guimarães foi designado membro titular e o Senador Plínio Valério, membro suplente, pelo Bloco Parlamentar Democracia, para compor a comissão (Of. nº 001/2025-GLPSDB).

(9) Em 19.02.2025, o Senador Marcos do Val foi designado membro titular, pelo Bloco Parlamentar Democracia, para compor a comissão (Of. nº 011/2025-GLPODEMOS).

(10) Em 19.02.2025, os Senadores Confúcio Moura, Efraim Filho, Marcio Bittar, Marcos Do Val e Oriovisto Guimarães foram designados membros titulares, e os Senadores Alessandro Vieira e Plínio Valério membros suplentes, pelo Bloco Parlamentar Democracia, para compor a Comissão (Of. 006/2025-BLDEM).

(11) Em 20.02.2025, o Senador Marcio Bittar deixou de compor a Comissão (Of. nº 009/2025-BLDEM).

(12) Em 19.03.2025, o Senador Esperidião Amin foi designado membro suplente, em substituição ao Senador Plínio Valério, que deixa de compor a comissão, pelo Bloco Parlamentar Democracia (Of. nº 024/2025-BLDEM).

(13) Em 11.04.2025, o Senador Hamilton Mourão passa a ocupar a vaga de titular, em substituição ao Senador Cleitinho, que passa a membro suplente, pelo Bloco Parlamentar Aliança, para compor a comissão (Of. n° 17/2025-GABLID/BLALIAN).

(14) Em 29.04.2025, a comissão reunida elegeu o Senador Hamilton Mourão Vice-Presidente deste colegiado.

(15) Em 05.05.2025, a Senadora Ivete da Silveira foi designada membro titular, pelo Bloco Parlamentar Democracia, para compor a comissão (Of. nº 023/2025-BLDEMO).

(16) Em 03.07.2025, o Senador Pedro Chaves foi designado membro titular, em substituição ao Senador Vanderlan Cardoso, que deixa de compor a comissão, pelo Bloco Parlamentar da Resistência Democrática (Of. nº 46/2025-BLRESDEM).

(17) Em 06.10.2025, o Senador José Lacerda foi designado membro suplente, pelo Bloco Parlamentar da Resistência Democrática, para compor a comissão (Of. nº 100/2025-BLRESDEM).

(18) Em 06.10.2025, o Senador Rogério Carvalho foi designado membro titular, pelo Bloco Parlamentar Pelo Brasil, para compor a comissão (Of. nº 28/2025-BLPBRA).

(19) Em 09.10.2025, o Senador Nelsinho Trad foi designado membro suplente, pelo Bloco Parlamentar da Resistência Democrática, para compor a comissão (Of. nº 102/2025-GSEGAMA).

(20) Em 30.10.2025, o Senador Vanderlan Cardoso foi designado membro titular, em substituição ao Senador Pedro Chaves, que deixa de compor a comissão, pelo Bloco Parlamentar da Resistência Democrática (Of. nº 112/2025/BLRESDEM).

(21) Em 06.11.2025, a Senadora Damares Alves foi designada membro suplente, em substituição ao Senador Cleitinho, que deixa de compor a comissão, pelo Bloco Parlamentar Aliança (Of. nº 62/2025-GABLID/GLREPUBL).

(22) Em 09.12.2025, o Senador Eduardo Girão foi designado membro suplente, pelo Bloco Parlamentar Vanguarda, para compor a comissão (Of. nº 133/2025-BLVANG).

(23) Em 11.12.2025, o Senador Eduardo Girão deixa de compor a comissão, pelo Bloco Parlamentar Vanguarda (Of. nº 135/2025-BLVANG).

(24) Vago em 30.01.2026, em razão da assunção da primeira suplente.

(25) Em 04.02.2026, o Senador Jorge Seif foi designado membro suplente, pelo Bloco Parlamentar Vanguarda, para compor a comissão (Of. 01/2026-BLVANG).

(26) Em 10.02.2026, o Senador Cid Gomes foi designado membro suplente, pelo Bloco Parlamentar da Resistência Democrática, para compor a comissão (Of. nº 008/2026-GSEGAMA).
(27) Em 06.04.2026, o Senador Laércio Oliveira foi designado membro suplente, em substituição ao Senador Ciro Nogueira, que deixa de compor a comissão, pelo Bloco Parlamentar Aliança (Of. nº 014/2026-GABLID/BLALIAN).
(28) Em 06.05.2026, o Senador Hermes Klann foi designado membro suplente, em substituição ao Senador Jorge Seif, que deixa de compor a comissão, pelo Bloco Parlamentar Vanguarda (Of. nº 037/2026-BLVANG).

REUNIÕES ORDINÁRIAS: QUARTAS-FEIRAS 11:00
SECRETÁRIO(A): MATHEUS SOARES TORRES COSTA
TELEFONE-SECRETARIA: 3303-1120
FAX:
TELEFONE - SALA DE REUNIÕES: 3303-1120
E-MAIL: cct@senado.leg.br

SENADO FEDERAL
SECRETARIA-GERAL DA MESA

4ª SESSÃO LEGISLATIVA ORDINÁRIA DA
57ª LEGISLATURA

Em 30 de junho de 2026
(terça-feira)
às 11h

PAUTA

22ª Reunião, Extraordinária - Semipresencial

COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO E INFORMÁTICA - CCT

1ª PARTE	Deliberativa
2ª PARTE	Audiência Pública Interativa
Local	Anexo II, Ala Senador Alexandre Costa, Plenário nº 3

Atualizações:
1. Divisão da reunião em 2 (duas) partes, uma deliberativa e uma audiência pública, atualização sobre confirmação de convidado e alteração para o formato semipresencial da reunião. (26/06/2026 20:03)
2. Atualização de convidados (30/06/2026 11:14)

1ª PARTE

PAUTA

ITEM 1

REQUERIMENTO DA COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO E INFORMÁTICA N° 50, DE 2026

Requer a inclusão de convidados na audiência pública objeto do REQ 18/2026-CCT, destinada a instruir o PL 4752/2025, 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".

Autoria: Senador Esperidião Amin

Resultado: Aprovado o requerimento.

Textos da pauta:
Requerimento **(CCT)**

2ª PARTE

Audiência Pública Interativa

Assunto / Finalidade:

Instruir o PL 4752/2025, 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".

Observações:

A reunião será interativa, transmitida ao vivo e aberta à participação dos interessados por meio do portal e-cidadania, na internet, em senado.leg.br/ecidadania ou pelo telefone da ouvidoria 0800 061 22 11.

Requerimentos de realização de audiência:

- REQ 18/2026 - CCT, Senador Jorge Seif
- REQ 40/2026 - CCT, Senador Hermes Klann
- REQ 42/2026 - CCT, Senador Hermes Klann
- REQ 44/2026 - CCT, Senador Astronauta Marcos Pontes
- REQ 45/2026 - CCT, Senador Rogério Carvalho
- REQ 46/2026 - CCT, Senador Hermes Klann
- REQ 47/2026 - CCT, Senador Esperidião Amin
- REQ 50/2026 - CCT, Senador Esperidião Amin

Reunião destinada a instruir a seguinte matéria:

- PL 4752/2025, Senador Esperidião Amin

Convidados:

Jacy Barbosa Junior
General de Divisão do Comando de Defesa Cibernética do Ministério da Defesa
Presença Confirmada

Marcelo Antonio Osller Malagutti
Secretário-Executivo do Comitê Nacional de Cibersegurança
Presença Confirmada

Demi Getschko
Diretor-Presidente do Núcleo de Informação e Coordenação do Ponto BR
Presença Confirmada

Rodrigo Pereira Pacheco
Diretor Substituto do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações da ABIN
Presença Confirmada

Rony Vainzof
Diretor Titular da Divisão de Cibersegurança da Fiesp e Consultor em Proteção de Dados da FecomercioSP
Videoconferência Confirmada

Rodrigo Jonas Fragola
Vice-Presidente de Articulação Política da Assespro
Presença Confirmada

Luiz Henrique Barbosa
Presidente-Executivo da TelComp
Presença Confirmada

Luca Belli
Professor de Direito, Coordenador do Centro de Tecnologia e Sociedade da FGV
Presença Confirmada

Belisario Contreras
Diretor-Executivo da Digi Americas Alliance
Presença Confirmada

Patricia Peck
Presidente do Instituto Peck de Cidadania Digital e membra titular do Instituto Empoderar
Presença Confirmada

Marta Helena Schuh
Diretora de Seguros Cibernéticos da Howden Brasil
Presença Confirmada

Patrick Aron Rinski
Diretor-Executivo da Unidade 42 da Palo Alto Networks

Presença Confirmada

Rodrigo Marinho
CEO do Instituto Livre Mercado

Presença Confirmada

Luana de Brito Tavares Diniz
Fundadora e CEO do Instituto Nacional de Combate ao Cibercrime

Videoconferência Confirmada

Vinícius Malacco Ferreira
Gerente de subscrição de linhas financeiras na Tokio Marine Seguradora

Videoconferência Confirmada

1ª PARTE - DELIBERATIVA

1

SENADO FEDERAL
Gabinete do Senador Esperidião Amin

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" sejam incluídos os seguintes convidados:

- o Senhor VINÍCIUS MALACCO, especialista em cibersegurança da Tokio Marine;
- a Senhora LUANA TAVARES, representante da Aliança Multissetorial pela Cibersegurança Nacional e Instituto Nacional de Combate ao Cibercrime (INCC).

Sala da Comissão, 26 de junho de 2026.

Senador Esperidião Amin
(PP - SC)

SENADO FEDERAL

PROJETO DE LEI
N° 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

SENADO FEDERAL
Gabinete do Senador **ESPERIDIÃO AMIN**

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

PARECER Nº , DE 2025

Da COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, sobre o Projeto de Lei nº 4752, de 2025, do Senador Esperidião Amin e outros, 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*.

Relator: Senador **HAMILTON MOURÃO**

I – RELATÓRIO

Vem para análise do Senado Federal o Projeto de Lei nº 4752, de 2025, do Senador Esperidião Amin e outros, 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 matéria foi distribuída à Comissão de Constituição, Justiça e Cidadania - CCJ, onde me coube a relatoria, e posteriormente seguirá para análise da Comissão de Ciência, Tecnologia, Inovação e Informática - CCT, cabendo à última comissão a decisão terminativa.

Entre os objetivos principais da proposição, ínsitos no Capítulo I, estão o fortalecimento da resiliência cibernética da administração pública, a prevenção e mitigação de incidentes cibernéticos, a promoção da integração entre políticas de segurança da informação, o estímulo à formação de recursos humanos especializados, e o fomento da cooperação entre setores público, privado e sociedade civil.

O Capítulo II do projeto define as competências da Autoridade Nacional de Cibersegurança, que incluem normatização, fiscalização, auditoria e instrução de processos administrativos. A autoridade também estabelecerá padrões mínimos de cibersegurança, que serão revisados periodicamente e submetidos a consulta pública.

O Programa Nacional de Segurança e Resiliência Digital, previsto no Capítulo III, é instituído no âmbito da administração pública federal, com possibilidade de adesão por estados, municípios e organizações do setor privado. Os seus objetivos incluem implementar princípios e diretrizes de resiliência cibernética, estabelecer planos de resiliência, definir metas e indicadores de desempenho, e promover a integração das ações entre diversos setores críticos. Para cumprir seus objetivos, o programa contará com instrumentos como planos setoriais de resiliência, protocolos de resposta a incidentes, sistemas de monitoramento, campanhas de conscientização e mecanismos de adesão voluntária.

A participação dos entes federativos no programa está associada ao compromisso de desenvolver e implementar iniciativas próprias de cibersegurança, incluindo planos locais de cibersegurança, criação de equipes de resposta a incidentes e promoção de ações de capacitação. Além disso, os entes participantes devem integrar a avaliação e mitigação de riscos cibernéticos de seus fornecedores aos seus programas internos de resiliência cibernética, bem como devem promover programas de capacitação, parcerias com universidades e centros de pesquisa, e incentivar a inclusão de conteúdos de cibersegurança nas grades curriculares. Em contrapartida, a adesão ao programa confere acesso prioritário aos recursos do Fundo Nacional de Segurança Pública destinados à cibersegurança, incluindo programas de capacitação e sistemas de alerta.

Ademais, o programa será monitorado continuamente, com publicação periódica de indicadores, metas e resultados alcançados, visando à melhoria da resiliência cibernética nacional. De acordo com o art. 25 da proposição, os órgãos responsáveis pela aplicação dos recursos devem publicar relatórios detalhados das receitas, despesas e resultados alcançados, submeter suas contas à auditoria e garantir a participação e controle social.

Nas disposições finais (Capítulo IV), altera-se a Lei nº 13.756, de 12 de dezembro de 2018, para destinar um percentual dos recursos do Fundo Nacional de Segurança Pública a ações de cibersegurança, incluindo financiamento de projetos de modernização tecnológica, formação de recursos humanos e apoio à pesquisa e inovação.

A exposição de motivos destaca, entre outros aspectos, que:

> 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.

Não foram recebidas emendas no prazo regimental.

II – ANÁLISE

O projeto de lei em análise não apresenta vício de constitucionalidade, juridicidade e regimentalidade e está redigido de acordo com os padrões de redação preconizados pela Lei Complementar nº 95, de 26 de fevereiro de 1998.

Os requisitos formais e materiais de constitucionalidade são cumpridos. A iniciativa parlamentar é legítima; os termos da proposição não importam em violação de cláusula pétrea; e não há reserva temática de iniciativa que importe em vício.

Sobre o mérito, o PL nº 4752, de 2025, de autoria do Senador Esperidião Amin e outros, institui o Marco Legal da Cibersegurança com um foco pragmático: fortalecer a resiliência cibernética da administração pública em todos os entes da federação (União, estados, Distrito Federal e municípios).

As diretrizes do PL são focadas na gestão pública, incluindo a resposta coordenada a incidentes, a promoção de uma cultura de cibersegurança entre

servidores, a proteção de infraestruturas críticas e a responsabilização de gestores e agentes públicos. O projeto prevê a designação de uma "autoridade nacional de cibersegurança", que será responsável por normatizar, fiscalizar e auditar, além de estabelecer padrões mínimos de segurança, cabendo ao Poder Executivo sua determinação.

O núcleo do projeto é o Programa Nacional de Segurança e Resiliência Digital, voltado para a administração pública federal, com possível adesão de estados e municípios, comprometendo-se a desenvolver seus próprios planos locais de cibersegurança e a criar ou fortalecer equipes de resposta a incidentes.

A proposição enfatiza a governança de riscos das cadeias de suprimentos, em que cabe aos órgãos públicos participantes a avaliação dos riscos cibernéticos de seus fornecedores e parceiros. A autoridade nacional poderá, inclusive, criar um índice de maturidade e confiabilidade de fornecedores e restringir a adoção de soluções descontinuadas ou sem suporte.

Além disso, a criação de um mecanismo de financiamento estável é inovadora, mediante alteração da Lei nº 13.756, de 2018, pelo art. 26 da proposição, para determinar que, no mínimo, 3% dos recursos do Fundo Nacional de Segurança Pública (FNSP) sejam aplicados em ações de cibersegurança. Em acréscimo, destina 2% da arrecadação das apostas de quota fixa (apostas esportivas) para o FNSP, especificamente para ações de cibersegurança.

Portanto, a proposição demonstra alto grau de maturidade institucional e pragmatismo, sendo seu foco na resiliência da administração pública um recorte estratégico e factível, diante de ameaças cibernéticas que podem causar enormes danos às nossas infraestruturas críticas e soberania.

Merece, assim, total apoio deste relator.

III – VOTO

Por ser conveniente e oportuno aos interesses nacionais, constitucional, jurídico e regimental, somos pela **aprovação** do Projeto de Lei nº 4752, de 2025.

Sala da Comissão,

, Presidente

, Relator

SENADO FEDERAL
Gabinete do Senador Jorge Seif

REQUERIMENTO Nº DE - CTFC

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, a realização de audiência pública, com o objetivo de instruir o PL 4752/2025, 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".

Proponho para a audiência a presença dos seguintes convidados:

- representante Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações (Cpesc) da Agência Brasileira de Inteligência - ABIN;
- representante Gabinete de Segurança Institucional - Presidência da República;
- representante Ministério da Defesa.

JUSTIFICAÇÃO

O Projeto de Lei nº 4.752/2025 propõe a criação de um marco normativo estruturante para a cibersegurança no Brasil, com reflexos diretos sobre a transparência pública, a governança digital, a fiscalização estatal e a proteção dos consumidores.

A crescente incidência de ataques cibernéticos contra órgãos públicos, empresas e serviços essenciais evidencia a necessidade de uma política nacional

coordenada, capaz de prevenir riscos, mitigar danos e assegurar a continuidade de serviços críticos à população.

Nesse contexto, a proposta apresenta medidas relevantes, como a criação de um Programa Nacional de Segurança e Resiliência Digital, o estímulo à cooperação entre setor público e privado, a priorização de investimentos na área e a possível instituição de uma autoridade nacional de cibersegurança.

A matéria dialoga diretamente com as competências desta Comissão, especialmente no que se refere à transparência na gestão pública, à governança de dados, ao controle de riscos institucionais e à proteção dos consumidores diante de vazamentos e incidentes digitais.

Diante da complexidade técnica e dos impactos regulatórios, econômicos e sociais da proposta, faz-se necessária a realização de audiência pública para:

- aprofundar o debate sobre o modelo institucional proposto;
- avaliar a integração com estruturas já existentes, como a Autoridade Nacional de Proteção de Dados;
- examinar os impactos sobre a proteção de dados pessoais e os direitos dos consumidores;
- colher contribuições de especialistas e dos setores diretamente afetados.

A iniciativa permitirá o aprimoramento do texto legislativo, assegurando maior segurança jurídica, eficiência regulatória e alinhamento com as melhores práticas internacionais em matéria de cibersegurança.

Diante do exposto, conto com o apoio dos nobres pares para a aprovação do presente requerimento.

Sala da Comissão, 30 de abril de 2026.

Senador Jorge Seif
(PL - SC)

SENADO FEDERAL

Esta página foi gerada para informar os signatários do documento e não integra o documento original, que pode ser acessado por meio do QRCode

Assinam eletronicamente o documento SF266146307239, em ordem cronológica:

1. Sen. Jorge Seif
2. Sen. Esperidião Amin

SENADO FEDERAL
Gabinete do Senador Hermes Klann

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" sejam incluídos os seguintes convidados:

- o Senhor Belisario Contreras, Diretor-Executivo da Digi Americas Alliance;
- o Senhor Rony Vainzof, Diretor e Coordenador (Cibersegurança) da Fiesp e Consultor em Proteção de Dados da Fecomercio/SP;
- o Doutor Luca Belli, Professor da FGV e membro do Conselho Consultivo do Comitê Interministerial para a Transformação Digital;
- representante Confederação Asserpro - Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação;;
- representante CGI.BR - Comitê Gestor da Internet no Brasil.

Sala da Comissão, 19 de maio de 2026.

Senador Hermes Klann
(PL - SC)

SENADO FEDERAL
Gabinete do Senador Hermes Klann

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" seja incluído o seguinte convidado:

- representante Instituto Livre Mercado.

Sala da Comissão, 1º de junho de 2026.

Senador Hermes Klann
(PL - SC)

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" seja incluído o seguinte convidado:

- o Senhor Luiz Henrique Barbosa, Presidente Executivo da TelComp (Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competitivas).

Sala da Comissão, 22 de junho de 2026.

Senador Astronauta Marcos Pontes
(PL - SP)

SENADO FEDERAL
Gabinete do Senador Rogério Carvalho

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" seja incluído o seguinte convidado:.

- Senhor Luiz Henrique Barbosa, Presidente Executivo da TelComp (Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competitivas).

Sala da Comissão, 22 de junho de 2026.

Senador Rogério Carvalho
(PT - SE)

SENADO FEDERAL
Gabinete do Senador Hermes Klann

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 58, § 2º, II, da Constituição Federal e do art. 93, II, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT sejam incluídos os seguintes convidados:

- a Senhora Marta Helena Schuh, Diretora de Seguros Cibernéticos da Howden Brasil;
- o Senhor Patrick Aron Rinski, Managing Director e Líder da Unit42 para América Latina e Caribe.

Sala da Comissão, 23 de junho de 2026.

Senador Hermes Klann
(PL - SC)

SENADO FEDERAL
Gabinete do Senador Esperidião Amin

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" seja incluída a seguinte convidada:

- a Senhora PATRICIA PECK do Instituto Peck de Cidadania e do Instituto Empoderar.

Sala da Comissão, 23 de junho de 2026.

Senador Esperidião Amin
(PP - SC)

SENADO FEDERAL
Gabinete do Senador Esperidião Amin

REQUERIMENTO Nº DE - CCT

Senhor Presidente,

Requeiro, nos termos do art. 93, I, do Regimento Interno do Senado Federal, que na Audiência Pública objeto do REQ 18/2026 - CCT, com o objetivo de instruir o PL 4752/2025, 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" sejam incluídos os seguintes convidados:

- o Senhor VINÍCIUS MALACCO, especialista em cibersegurança da Tokio Marine;
- a Senhora LUANA TAVARES, representante da Aliança Multissetorial pela Cibersegurança Nacional e Instituto Nacional de Combate ao Cibercrime (INCC).

Sala da Comissão, 26 de junho de 2026.

Senador Esperidião Amin
(PP - SC)