INCC
INSTITUTO NACIONAL DE COMBATE AO CRIME CIBERNÉTICO

ALIANÇA MULTISSETORIAL
PELA CIBERSEGURANÇA NACIONAL

AUDIÊNCIA PÚBLICA · SENADO FEDERAL · 30 DE JUNHO DE 2026

Marco Legal da Cibersegurança: integrar para avançar

Marco Legal da Cibersegurança PL nº 4.752/2025

Contribuição da Aliança Multissetorial pela Cibersegurança Nacional

Por que agir agora, e com uma só lei

A urgência é real; as duas iniciativas respondem a ela por ângulos diferentes.

~R$ 2,3 tri

Impacto econômico anual estimado do cibercrime (2024)

Estimativa — FrenCyber/Aliança (verificar fonte primária)

+408%

Crescimento dos estelionatos entre 2018 e 2024 (≈2,16 mi em 2024)

Anuário Brasileiro de Segurança Pública — FBSP, 19ª ed. (2025)

A lacuna

Temos LGPD, Marco Civil, PNCiber e E-Ciber — mas nenhuma lei estruturante que integre tudo.

Duas iniciativas, um mesmo objetivo

PL nº 4.752/2025

Programático e federativo

- Indução e coordenação política
- Financiamento e adesão
- Programa de Segurança e Resiliência Digital

Minuta do CNCiber

Regulatório e operacional

- Governança e gestão de riscos
- Fiscalização e responsabilização
- Resposta a incidentes e reporte

Juntas = força federativa do PL + densidade regulatória da Minuta

Sem sobreposição de obrigações. Sem duplicidade. Um só arcabouço.

A proposta da Aliança: um substitutivo integrador

Sete pilares pragmáticos para um texto único, proporcional e exequível.

1 Sistema Nacional de Cibersegurança

Integra União, estados, municípios, setor privado e ETIRs.

2 Autoridade Nacional com autonomia técnica

Coordenação, competência normativa e fiscalizatória.

3 Harmonização regulatória

Preserva BACEN, ANPD, ANATEL e ANEEL — sem duplicar obrigações.

4 Regulação baseada em risco

Obrigações proporcionais ao porte, criticidade e impacto.

5 Reporte unificado de incidentes

Critérios nacionais e compartilhamento seguro de informações.

6 Proteção de infraestruturas críticas

Gestão de risco, continuidade, testes e exercícios nacionais.

7 Integração com o combate ao crime

Cooperação com PF, polícias civis, MP, Judiciário e inteligência, Sociedade Civil.

Princípio-chave: proporcionalidade. Mais segurança, sem sufocar PMEs e inovação.

ALIANÇA MULTISSETORIAL
PELA CIBERSEGURANÇA NACIONAL

O que sugerimos a esta Casa

Elaborar um substitutivo integrador

que consolide uma Política Nacional de Cibersegurança baseada em coordenação, cooperação, proporcionalidade, inovação, proteção de direitos e fortalecimento da capacidade nacional.

Não deixar de fora

- Cidadãos vulneráveis (idosos, crianças, vítimas)
- PMEs: conformidade simplificada e incentivos
- Educação digital (inclusive na BNCC)
- IA e tecnologias emergentes: security-by-design

Não são propostas concorrentes, são complementares. *Integrá-las é construir a soberania digital do Brasil.*

Como o Brasil chegou até aqui

Cada lei resolveu uma camada. O Marco Legal é o passo que falta na base.

ESTAMOS AQUI

2014
Marco Civil da Internet
Direitos e princípios da rede

2018
LGPD
Proteção de dados pessoais

2020
E-Ciber
Estratégia Nacional (Dec. 10.222)

2023
PNCiber + CNCiber
Política e comitê (Dec. 11.856)

2025
Marco Legal em debate
PL 4.752/2025 + Minuta CNCiber

2026
Lei integrada – Marco Legal

2026-2027
AGÊNCIA & MUDANÇA DE CULTURA & PROTEÇÃO DA SOCIEDADE

- **Estágio 1 — Fundamentos**
  direitos & dados
- **Estágio 2 — Estratégia & governança**
  política & comitê
- **Estágio 3 — Marco Legal: a base estrutural**
  AGORA
- **Estágio 4 — Maturidade: cultura & sociedade**
  PRÓXIMO

INCC
INSTITUTO NACIONAL DE COMBATE AO CRIME CIBERNÉTICO

ALIANÇA MULTISSETORIAL
PELA CIBERSEGURANÇA NACIONAL

NOTA TÉCNICA · 2026

Nota Técnica para Integração Legislativa

Convergência entre o PL nº 4.752/2025 (Marco Legal da Cibersegurança) e a Minuta de Lei Geral de Cibersegurança do CNCiber

Contribuição para a
Audiência Pública — Senado Federal
30 de junho de 2026

Aliança Multissetorial pela Cibersegurança Nacional — Coordenação: INCC · Membros: FECOMERCIO-SP, FEBRABAN, FIESP, ABES, ABRAMED, FIN, ACREFI, ACATE, BRASSCOM, GASA — Global Anti-Scam Alliance (Chapter Brazil), ASSESPRO, FENAINFO, ANVINT — Associação Nacional das Vítimas de Internet, Instituto Peck de Cidadania Digital.

SÃO PAULO · BRASÍLIA | JUNHO DE 2026

DOCUMENTO	Nota Técnica para Integração Legislativa
EMISSOR	Aliança Multissetorial pela Cibersegurança Nacional (coordenação: INCC - Instituto Nacional de Combate ao Cibercrime)
DESTINATÁRIO	Senado Federal - Comissão de Ciência, Tecnologia, Inovação e Informática (CCT) e demais comissões competentes
OCASIÃO	Audiência pública sobre o Marco Legal da Cibersegurança | 30 de junho de 2026
OBJETO	Convergência e complementaridade entre o PL nº 4.752/2025 e a Minuta de Lei Geral de Cibersegurança do CNCiber
RECOMENDAÇÃO	Construção de um substitutivo integrador que consolide uma Política Nacional de Cibersegurança

1 Resumo Executivo

O Brasil atravessa um momento decisivo na construção de sua arquitetura nacional de cibersegurança. O crescimento dos crimes cibernéticos, a ampliação da dependência digital da economia, a expansão das infraestruturas críticas conectadas, o avanço da inteligência artificial e a sofisticação das ameaças exigem a consolidação de um marco legal moderno, coordenado e compatível com as melhores práticas internacionais.

Coexistem hoje duas iniciativas de grande relevância e propósitos complementares:

- **Projeto de Lei nº 4.752/2025**, em tramitação no Senado Federal, que institui o Marco Legal da Cibersegurança e cria o Programa Nacional de Segurança e Resiliência Digital;
- **Minuta de Lei Geral de Cibersegurança** elaborada pelo Comitê Nacional de Cibersegurança (CNCiber), resultado de amplo processo multissetorial envolvendo governo, setor privado, academia e sociedade civil.

Esta Nota Técnica conclui que **as duas iniciativas são amplamente convergentes e devem ser tratadas como complementares**. Enquanto o PL nº 4.752/2025 oferece relevantes mecanismos de indução federativa, coordenação política e financiamento, a Minuta do CNCiber apresenta estrutura regulatória mais robusta - com governança, gestão de riscos, fiscalização, coordenação operacional e responsabilização.

A principal recomendação é a construção de um **texto legislativo convergente**, capaz de incorporar os avanços de ambas as propostas e consolidar uma Política Nacional de Cibersegurança fundada em oito pilares:

- Governança Nacional Integrada.
- Regulação Baseada em Risco.
- Proteção dos Direitos Fundamentais.
- Proteção das Infraestruturas Críticas.
- Cooperação Federativa e Internacional.
- Educação e Cultura de Segurança Digital.
- Desenvolvimento Econômico e Tecnológico Nacional.
- Combate Efetivo aos Crimes Cibernéticos.

2 Contexto e Justificativa

A transformação digital da economia brasileira trouxe benefícios significativos para cidadãos, empresas e governo. Ela ampliou, contudo, a superfície de ataque disponível para organizações criminosas, grupos extremistas, atores patrocinados por Estados estrangeiros e fraudadores digitais.

Segundo dados reunidos pela Aliança Multissetorial pela Cibersegurança Nacional, o Brasil figura entre os países mais atacados do mundo e pode registrar impactos econômicos anuais da ordem de **R$ 2,3 trilhões** decorrentes de violações de dados e incidentes cibernéticos. Paralelamente, entre 2018 e 2024, os crimes de estelionato cresceram **mais de 400%**, alcançando cerca de 2,16 milhões de registros em 2024 - movimento fortemente impulsionado pela fraude digital. (Ver Notas e Fontes ao final.)

Apesar de importantes instrumentos normativos - o Marco Civil da Internet, a LGPD, a Lei do Governo Digital, a PNCiber e a E-Ciber - o país ainda **não dispõe de legislação estruturante** capaz de integrar governança, regulação, proteção de infraestruturas críticas, prevenção, resposta a incidentes e cooperação institucional.

A aprovação de um marco legal integrado representa oportunidade histórica para preencher essa lacuna. O PL nº 4.752/2025, de autoria do Senador Esperidião Amin, já foi aprovado na Comissão de Constituição e Justiça (CCJ) e segue para análise na CCT, o que torna a presente audiência pública um momento oportuno para harmonizar as duas iniciativas em curso.

3 Principais Convergências entre as Propostas

As duas iniciativas apresentam forte alinhamento estratégico. Os principais pontos convergentes são:

3.1 Governança Nacional

Ambas reconhecem a necessidade de coordenação nacional da cibersegurança, com definição clara de competências, diretrizes e mecanismos de articulação institucional.

3.2 Autoridade Nacional de Cibersegurança

As duas propostas preveem autoridade nacional responsável pela coordenação, normatização e supervisão das políticas de cibersegurança.

3.3 Proteção de Infraestruturas Críticas

Há convergência sobre a proteção prioritária dos setores essenciais da economia e do Estado.

3.4 Gestão de Riscos, Notificação e Capacitação

Ambas adotam abordagem baseada em gestão de riscos e maturidade institucional, reconhecem a importância da comunicação de incidentes relevantes e do compartilhamento estruturado de informações, e defendem a ampliação da formação de profissionais e da cultura nacional de cibersegurança, bem como mecanismos de incentivo à indústria nacional, à pesquisa aplicada e ao desenvolvimento tecnológico.

4 Principais Diferenças entre as Propostas

As diferenças observadas são predominantemente de escopo e profundidade regulatória. O **PL nº 4.752/2025** possui caráter mais programático e federativo; a **Minuta do CNCiber** apresenta caráter mais regulatório, operacional e institucional. Tais diferenças não representam incompatibilidades, mas **oportunidades de complementaridade**.

Dimensão	PL nº 4.752/2025	Minuta do CNCiber
Natureza	Programática e federativa	Regulatória e operacional
Grau de obrigatoriedade	Adesão e indução	Obrigações vinculantes
Fiscalização	Mecanismos gerais	Estrutura detalhada

Dimensão	PL nº 4.752/2025	Minuta do CNCiber
Regime sancionatório	Pouco detalhado	Regime estruturado
Resposta a incidentes	Diretrizes	Mecanismos operacionais
Cadeia de suprimentos	Tratamento incipiente	Tratamento específico
Reporte de incidentes	Princípios gerais	Regime estruturado de reporte

A leitura combinada das duas propostas permite reunir a força indutora e federativa do PL com a densidade regulatória e operacional da Minuta, sem sobreposição de obrigações.

5 Recomendações Estratégicas para Integração

RECOMENDAÇÃO 1

Consolidar um Sistema Nacional de Cibersegurança (SNCiber)

Instituir formalmente o SNCiber, integrando União, Estados, Distrito Federal, Municípios, Autoridades Setoriais, Autoridade Nacional, Centros de Resposta, Infraestruturas Críticas e setor privado.

RECOMENDAÇÃO 2

Criar uma Autoridade Nacional de Cibersegurança com autonomia técnica

Dotada de autonomia técnica, coordenação nacional, competência normativa e fiscalizatória, e articulação com as autoridades setoriais — em modelo semelhante ao adotado por Chile, União Europeia, Singapura e Reino Unido.

RECOMENDAÇÃO 3

Estabelecer expressamente o princípio da harmonização regulatória

Preservar as competências do Banco Central, ANPD, ANATEL, ANEEL e demais reguladores setoriais, evitando sobreposição regulatória e duplicidade de obrigações.

RECOMENDAÇÃO 4

Adotar abordagem regulatória baseada em risco

Calibrar as obrigações conforme porte da organização, criticidade da atividade, exposição ao risco e impacto potencial para a sociedade.

RECOMENDAÇÃO 5

Criar um regime nacional unificado de reporte de incidentes

Estabelecer critérios nacionais, classificação de incidentes, interoperabilidade entre órgãos e compartilhamento seguro de informações.

RECOMENDAÇÃO 6

Fortalecer a proteção das infraestruturas críticas

Exigir gestão de riscos, planos de continuidade, testes periódicos, exercícios nacionais e Equipes de Tratamento e Resposta a Incidentes (ETIRs) estruturadas.

RECOMENDAÇÃO 7

Integrar segurança cibernética e combate ao crime cibernético

Prever cooperação permanente entre a Autoridade Nacional, a Polícia Federal, as Polícias Civis, o Ministério Público, o Poder Judiciário e os órgãos de inteligência.

6 Recomendações Adicionais (para integração ou nova proposição legislativa)

Os pontos a seguir não estão suficientemente contemplados nas propostas atuais e merecem incorporação expressa no texto integrador.

6.1 Proteção dos cidadãos e grupos vulneráveis

Incorporar instrumentos voltados a idosos, crianças e adolescentes, pessoas com baixa alfabetização digital e vítimas de golpes digitais.

6.2 Educação e cultura de segurança digital

Inclusão da segurança digital na BNCC, formação continuada de professores, capacitação de servidores públicos e campanhas nacionais permanentes.

6.3 Apoio às PMEs

As pequenas e médias empresas representam parcela significativa da economia e figuram entre os grupos mais vulneráveis. Recomendam-se linhas de crédito específicas, incentivos fiscais, programas de capacitação e modelos simplificados de conformidade.

6.4 Desenvolvimento da indústria nacional

Criar mecanismos de compras públicas seguras, incentivos à inovação, programas de certificação e estímulos à exportação.

6.5 Inteligência artificial e tecnologias emergentes

Prever sandboxes regulatórios, **security-by-design**, avaliações contínuas de risco e governança de IA aplicada à segurança.

7 Alinhamento com Experiências Internacionais

A análise comparada demonstra forte alinhamento com experiências internacionais bem-sucedidas. Os países mais resilientes combinam governança forte, coordenação nacional, cooperação com o setor privado, educação, inovação e proteção de infraestruturas críticas.

País / Bloco	Contribuição de referência para o modelo brasileiro
Chile	Autoridade Nacional + proteção de infraestruturas críticas
União Europeia (NIS2)	Regulação baseada em risco + reporte obrigatório de incidentes
Reino Unido	Coordenação nacional + cultura de segurança
Estados Unidos	Framework NIST + cooperação público-privada
Israel	Integração entre segurança, inovação e desenvolvimento econômico
Singapura	Governança centralizada + metas nacionais

Ressalva: os modelos acima são apresentados em caráter ilustrativo e de alto nível. A transposição de qualquer arranjo estrangeiro deve considerar as especificidades constitucionais, federativas e setoriais brasileiras.

8 Proposta de Estrutura Legislativa Integrada

Sugere-se que o substitutivo integrador adote a seguinte arquitetura de capítulos, capaz de reunir os avanços das duas propostas em um único corpo normativo coerente:

Capítulo I — Disposições Gerais
Capítulo II — Princípios, Direitos e Garantias
Capítulo III — Sistema Nacional de Cibersegurança
Capítulo IV — Autoridade Nacional e Autoridades Setoriais
Capítulo V — Infraestruturas Críticas e Serviços Essenciais
Capítulo VI — Gestão de Riscos e Notificação de Incidentes
Capítulo VII — Educação, Cultura e Capacitação

9 Conclusão

O Brasil tem hoje a oportunidade histórica de consolidar um modelo moderno, equilibrado e efetivo de governança da cibersegurança. A análise técnica demonstra que o PL nº 4.752/2025 e a Minuta de Lei Geral de Cibersegurança do CNCiber **não são propostas concorrentes, mas complementares**.

A integração de seus dispositivos permitirá construir um arcabouço jurídico compatível com as melhores práticas internacionais, preservando as competências setoriais existentes, fortalecendo a proteção das infraestruturas críticas, ampliando a segurança dos cidadãos e criando as bases institucionais para uma política nacional permanente de segurança e resiliência digital.

A recomendação final desta Nota Técnica é a elaboração de um **substitutivo integrador** que reúna os avanços das duas iniciativas e consolide uma Política Nacional de Cibersegurança baseada em coordenação, cooperação, proporcionalidade, inovação, proteção de direitos e fortalecimento da capacidade nacional, marco estruturante para a soberania digital, a competitividade econômica e a proteção da sociedade brasileira nas próximas décadas.

Aliança Multissetorial pela Cibersegurança Nacional
Coordenação: INCC — Instituto Nacional de Combate ao Cibercrime · São Paulo / Brasília, junho de 2026

Notas, Fontes e Ressalvas Metodológicas

[1] PL nº 4.752/2025 — fonte primária. Senado Federal, Projeto de Lei nº 4.752, de 2025 (autoria do Senador Esperidião Amin), que institui o Marco Legal da Cibersegurança e cria o Programa Nacional de Segurança e Resiliência Digital. Aprovado na CCJ em dezembro de 2025; remetido à CCT. Tramitação: www25.senado.leg.br/web/atividade/materias/-/materia/170613. Status sujeito a alteração — recomenda-se confirmar o andamento atualizado no portal do Senado antes da audiência.

[2] Estelionato (2018–2024) — fonte primária/secundária. Fórum Brasileiro de Segurança Pública (FBSP), Anuário Brasileiro de Segurança Pública, 19ª edição (julho de 2025): cerca de 2,16 milhões de casos de estelionato em 2024, com crescimento aproximado de 408% em relação a 2018, fortemente associado à fraude digital. Ressalva: o dado refere-se ao estelionato em sentido amplo; o recorte de "estelionato por meio eletrônico" possui série própria e magnitudes distintas. Verificar a edição oficial do Anuário (forumseguranca.org.br).

[3] Impacto econômico (~R$ 2,3 trilhões) — estimativa, verificar. Cifra divulgada em 2024 e reproduzida em materiais associados à Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética (FrenCyber) e à Aliança Multissetorial, por vezes apresentada como equivalente a cerca de 18% do PIB potencial. Ressalva metodológica: trata-se de estimativa de impacto agregado, com metodologia e período de referência que variam conforme a fonte; recomenda-se citar a fonte primária e o ano-base ao utilizá-la em manifestação oficial. Não tratar como dado contábil consolidado.

Marco normativo citado. Marco Civil da Internet (Lei nº 12.965/2014); LGPD (Lei nº 13.709/2018); Lei do Governo Digital (Lei nº 14.129/2021); Política Nacional de Cibersegurança — PNCiber (Decreto nº 10.222/2020 e Decreto nº 11.856/2023, que cria o CNCiber); E-Ciber. Verificar a vigência e a numeração junto ao Planalto (planalto.gov.br) antes da citação formal.

Ressalva geral: esta Nota Técnica foi elaborada a partir de documento de contribuição da Aliança Multissetorial e de verificação complementar em fontes públicas (Senado Federal e FBSP). Os números estatísticos são indicativos e devem ser confirmados em suas fontes primárias antes de uso em peça oficial. A Minuta de Lei Geral de Cibersegurança do CNCiber é referida conforme apresentada no processo multissetorial; recomenda-se anexar a versão de referência utilizada.