Março de 2026

Internet Impact Brief

PL 4752/2025

Internet Society
Capítulo Brasil

Coordenação

Grupo de Trabalho de Criptografia - ISOC Brasil

IP.Rec

Revisores

Flávio Rech Wagner

Laura Pereira

Raquel Fortes Gatto

João Moreno Falcão

Pedro Amaral

Apoio

ISOC Foundation

Este Internet Impact Brief é fruto do Projeto Encryption and Digital Rights in Brazil: Capacity Building, Dialogue, and Policy Advocacy.

Sumário

Sumário 1
1. Introdução 2
2. Sobre o PL 4752/2025 3
2.1 Principais Dispositivos 3
2.2 Escopo 4
4. Os Impactos transversais da proposta 4
4.1 PC1 –Uma Infraestrutura Acessível com um Protocolo Comum 7
4.2 PC2 – Arquitetura Aberta de Blocos Estruturais Interoperáveis e Reutilizáveis 9
4.3 PC3 – Gerenciamento Descentralizado e um Sistema de Roteamento Distribuído Comum 9
4.4 PC4 – Identificadores Globais Comuns 10
4.5 PC5 – Uma Rede de Propósito Geral e Tecnologicamente Neutra 11
5. Impacto nos Habilitadores de uma Internet Aberta, Globalmente Conectada, Segura e Confiável 12
Objetivo 1: Internet Aberta 12
5.1 H1 – Acesso Fácil e Irrestrito 12
5.2 H2 – Uso irrestrito e fomento ao desenvolvimento de tecnologias para a Internet 13
5.3 H3 – Desenvolvimento, Gerenciamento e Governança Colaborativos 14
Objetivo 2: Internet Globalmente Conectada 14
5.4 H4 – Alcance Irrestrito 14
5.5 H5 – Capacidade da Rede 14
Objetivo 3: Internet Segura 15
5.6 H6 – Confidencialidade de dados, informações, dispositivos e aplicativos 15
5.7 H7 – Integridade de dados, informações, dispositivos e aplicativos 16
Objetivo 4: Internet Confiável 16
5.8 H– Confiabilidade, resiliência e conectividade otimizada 16
5.9 H9 – Prestação de Contas e Responsabilidade 17
5.10 H10 – Privacidade 17
6. Tabela de Impacto 18
6.1 Propriedades Críticas 18
6.2 Habilitadores OGST 19
7. Conclusões e Recomendações 19
7.1 Aspectos Positivos 19
7.2 Áreas de Preocupação 20
7.3 Recomendações Legislativas 21
8. Conclusão 22

Sumário Executivo

O PL 4752/2025 representa avanço significativo na governança de cibersegurança brasileira, com impacto misto na arquitetura da Internet:

Categoria	Descrição	Impacto
Tipo de Mudança	Legislação nacional estabelecendo um arcabouço de governança de cibersegurança	Regulatório
Escopo	Administração pública federal; participação voluntária do setor privado	Nacional
Propriedades Críticas	4 de 5 propriedades potencialmente afetadas	Baixo
Habilitadores	7 de 10 habilitadores impactados (4 positivamente, 3 com efeitos mistos/negativos)	Misto
Preocupação Principal	Preferências tecnológicas nacionais (Art. 14, §1º) e poderes centralizados da autoridade podem fragmentar arquitetura aberta	Atenção Necessária

Dimensão	Avaliação	Principais riscos
Propriedades Críticas da Internet	4 de 5 afetadas	Fragmentação tecnológica, gatekeeping
Habilitadores	7 de 10 impactados	Restrição de acesso, diversidade reduzida
Impacto Econômico	Moderado	Custos de conformidade, concentração
Compatibilidade Internacional	Parcial	Lacunas de harmonização

1. Introdução

Esta Avaliação de Impacto na Internet avalia o Marco Legal da Cibersegurança (PL 4752/2025), proposto pelo Senador Esperidião Amin, usando a Metodologia de Avaliação de Impacto na Internet da Internet Society. A IIAT fornece uma metodologia estruturada para identificar se uma política, tecnologia ou prática empresarial pode prejudicar a arquitetura fundamental da Internet, ameaçando sua natureza global, aberta, segura e confiável.

A Internet deve sua força e sucesso a uma base de propriedades críticas que, quando combinadas, representam o Modo Internet de Interconectividade (MII). Isto inclui: (1) uma infraestrutura acessível com um protocolo comum; (2) uma arquitetura em camadas implementada sobre blocos de construção interoperáveis; (3) um gerenciamento descentralizado com roteamento distribuído; (4) um sistema comum e global de identificadores; e (5) uma rede de uso geral e tecnologicamente neutra. Assim, examinamos os efeitos da proposta sobre os fundamentos do paradigma MII, dos quais a Internet precisa para existir e prosperar como um recurso aberto, globalmente conectado, seguro e confiável.

Além das propriedades críticas do MII, a avaliação também considera os habilitadores essenciais para que a Internet prospere como um recurso aberto, globalmente conectado, seguro e confiável, conforme definido pela Internet Society (ISOC), quais sejam: (I) Acesso fácil e irrestrito; (II) Uso irrestrito e fomento ao desenvolvimento de tecnologias para a Internet; (III) Desenvolvimento, Gerenciamento e Governança colaborativos; (IV) Alcance irrestrito; (V) Capacidade da rede; (VI) Confidencialidade de dados, informações, dispositivos e aplicativos; (VII) Integridade de dados, informações, dispositivos e aplicativos (VIII) Confiabilidade, resiliência e conectividade otimizada; (IX) Prestação de Contas e Responsabilidade; (X) Privacidade.

Esta avaliação não constitui uma opinião jurídica, nem endossa ou se opõe à legislação. Seu propósito é identificar riscos e oportunidades relacionados à Internet para informar o processo legislativo.

2. Sobre o PL 4752/2025

O PL 4752/2025, conhecido como Marco Legal da Cibersegurança, é um projeto de lei do Senado brasileiro que busca estabelecer um arcabouço jurídico abrangente para a governança nacional de cibersegurança. Ele cria o Programa Nacional de Segurança e Resiliência Digital e designa uma autoridade nacional competente com poderes normativos, de fiscalização e auditoria.

Nesse sentido, o PL emerge em um contexto de intensa reconfiguração geopolítica da infraestrutura digital global. A cibersegurança ocupa posição central nos debates sobre soberania tecnológica, e diferentes países têm respondido a esse desafio por trajetórias radicalmente distintas. O conceito de soberania digital é intrinsecamente ambíguo e pode ser instrumentalizado de duas formas opostas: (i) a

soberania como capacidade, que foca no investimento em educação, infraestrutura própria e autonomia decisória fundada na competência técnica; e (ii) a soberania como controle, que busca autossuficiência por meio de restrições de mercado e preferências geográficas, frequentemente ignorando as interdependências estruturais da cadeia global de suprimentos de tecnologia.

Através da análise a seguir, concluiu-se que o PL 4752/2025 contém elementos de ambas as trajetórias, e é precisamente essa ambiguidade que fundamenta a presente avaliação. Desse modo, pretende-se identificar, com base em evidências técnicas e comparadas, os mecanismos que podem levar à fragmentação tecnológica e sugerir alternativas que fortaleçam a resiliência do Brasil sem comprometer sua participação na Internet global.

2.1 Principais Dispositivos

Os dispositivos mais relevantes do projeto para esta análise incluem:

- Art. 4 – Designa uma Autoridade Nacional de Cibersegurança com amplos poderes normativos, de fiscalização e auditoria sobre entidades públicas participantes no Programa Nacional de Segurança e Resiliência Digital.
- Art. 5 – Estabelece padrões mínimos de cibersegurança para a administração pública federal, alinhados com normas nacionais e internacionais reconhecidas.
- Art. 12 – Cria obrigações de notificação obrigatória de incidentes para entidades federais e participantes do programa.
- Arts. 13–15 – Impõe requisitos de governança de riscos da cadeia de suprimentos, incluindo classificação de risco de fornecedores de tecnologia.
- Art. 14, §1º – Estabelece preferências de aquisição para fornecedores nacionais de tecnologia (produtos e serviços desenvolvidos no Brasil).
- Art. 14, §2º – Concede à autoridade poder de restringir o uso de soluções tecnológicas descontinuadas ou sem suporte.
- Art. 14, §3º – Cria um índice de classificação de risco de fornecedores gerenciado pela autoridade nacional.
- Art. 18 – Estabelece conselhos consultivos multissetoriais e grupos de trabalho.
- Arts. 19–21 – Cria programas de capacitação, educação e P&D para construir capacidade nacional de cibersegurança.
- Art. 25 – Estabelece requisitos de transparência e responsabilização para a autoridade nacional.

- Art. 26 – Aloca 3% do Fundo Nacional de Segurança Pública e 2% das receitas de apostas de quota fixa para cibersegurança.

2.2 Escopo

O escopo principal do projeto é a Administração Pública Federal brasileira. A participação de entidades do setor privado e de governos estaduais/municipais é voluntária via adesão ao Programa Nacional. É importante notar que operadores de infraestruturas críticas podem estar sujeitos a normas setoriais emitidas pela autoridade nacional.

4. Os Impactos transversais da proposta

Antes de analisar cada propriedade crítica e habilitador individualmente (o que será feito nas seções seguintes), esta seção apresenta uma análise transversal do PL 4752/2025, identificando dimensões que perpassam múltiplos aspectos da arquitetura da Internet. O objetivo é fornecer o enquadramento contextual, geopolítico, econômico e normativo, que fundamenta a avaliação específica realizada adiante. Uma constatação de impacto não implica que a legislação seja defeituosa; em vez disso, pode sinalizar áreas em que salvaguardas ou esclarecimentos adicionais podem ser necessários.

Para balizar esta análise e fornecer o enquadramento interpretativo, preocupou-se em analisar três dimensões transversais que se manifestam em múltiplos aspectos do PL 4752/2025: (i) a articulação entre as escolhas regulatórias e os condicionantes geopolíticos da infraestrutura digital; (ii) a economia da alocação pública e privada de recursos para segurança digital; e (iii) lacunas normativas concretas que afetam a pesquisa em segurança, o software de infraestrutura e os mecanismos de governança multissetorial.

Nesse contexto, a efetividade das políticas de Divulgação Coordenada de Vulnerabilidades (CVD) e dos dispositivos de proteção a pesquisadores, um tema central na dimensão (iii), dependem intrinsecamente da clareza normativa, da participação ativa das comunidades técnica e da sociedade civil, e do alinhamento com as realidades sociotécnicas do Sul Global.

Abordagens centradas apenas em obrigações administrativas ou em uma perspectiva focada unicamente em interesses estritamente comerciais tendem a ser insuficientes para garantir resiliência sistêmica, diversidade tecnológica e uma resposta ágil a incidentes.[1]

Além disso, exemplos positivos no Sul Global, como a recente Lei Marco de Cibersegurança no Chile (Lei N°21.663), priorizam mecanismos claros de proteção a pesquisadores, incentivos à participação de pequenas empresas e critérios transparentes para avaliação técnica. Esses elementos fortalecem tanto a segurança quanto a qualidade do gasto público sem recorrer ao protecionismo.

[1] Nesse sentido, ver: https://www.mdpi.com/2227-9709/10/3/71

Por outro lado, a diversidade de arranjos, fornecedores e tecnologias é um componente central de robustez sistêmica, e ambientes excessivamente homogêneos tendem a apresentar maior correlação de falhas e riscos propagados em cascata.[2]

Nesse contexto, cabe observar que o PL 4.752/2025, ao concentrar suas obrigações na notificação de incidentes já consumados (Art. 12), intervém em uma fase tardia do ciclo de ataque, o que a literatura de segurança cibernética identifica como uma limitação conhecida de modelos reativos[3]. Frameworks modernos como o NIST Cybersecurity Framework 2.0 e a arquitetura Zero Trust (NIST SP 800-207) reforçam que a segurança eficaz exige verificação contínua e visibilidade em tempo real, não apenas conformidade estática. Ao não incorporar explicitamente esses paradigmas, o PL perde uma oportunidade de fortalecer a resiliência da infraestrutura digital brasileira nas etapas iniciais da cadeia de ataque.

Nesse sentido, o PL 4.752/2025 perde uma oportunidade ao não incorporar explicitamente esses paradigmas, limitando-se a uma lógica de conformidade estática que pode se tornar rapidamente obsoleta diante da evolução das ameaças. A experiência internacional com incidentes como SolarWinds (2020) e Log4Shell (2021) demonstrou que a cadeia de suprimentos digital é um vetor de ataque crítico que transcende fronteiras nacionais, e que a resposta eficaz depende de cooperação global, transparência na divulgação de vulnerabilidades e adoção de protocolos de segurança na camada de infraestrutura da Internet, como RPKI para segurança de roteamento, DNSSEC para integridade do DNS e TLS 1.3 para confidencialidade em trânsito.

Além disso, a omissão do PL 4.752/2025 quanto à proteção de pesquisadores de segurança e à institucionalização de políticas de divulgação coordenada de vulnerabilidades cria um elo fraco na cadeia de defesa cibernética. A Internet, como rede de propósito geral (propriedade crítica 5) e arquitetura aberta (propriedade crítica 2), depende fundamentalmente de um ecossistema distribuído de pesquisa independente para identificar e corrigir vulnerabilidades antes que sejam exploradas. Sem salvaguardas legais explícitas, incluindo *safe harbors* para pesquisadores de boa-fé e prazos claros para correção por parte dos fabricantes, a descoberta de falhas tende a ser canalizada e concentrada em mercados fechados (mercado de *zero-days*) ou corporações privadas com recursos abundantes , o que reduz a taxa de detecção independente, alonga o tempo até a correção de vulnerabilidades críticas e amplia o custo técnico e econômico dos incidentes.

[2] Nesse sentido, ver: https://www.sciencedirect.com/science/article/pii/S0925527323000221?via%3Dihub e https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf.

[3] A Cyber Kill Chain é um modelo desenvolvido pela Lockheed Martin que descreve as etapas sequenciais de um ataque cibernético, desde o reconhecimento inicial até a exfiltração de dados: (1) reconhecimento, (2) armação, (3) entrega, (4) exploração, (5) instalação, (6) comando e controle, e (7) ações sobre o objetivo. O modelo é amplamente utilizado para estruturar estratégias de defesa em cada fase do ataque.

Essa omissão é particularmente grave no contexto da Internet porque vulnerabilidades em *softwares* amplamente utilizados, como bibliotecas de criptografia, servidores DNS e implementações de protocolos de roteamento, afetam a infraestrutura compartilhada da rede, comprometendo simultaneamente a segurança de múltiplos participantes do ecossistema.

Indicadores como custo por ativo efetivamente protegido e índice de diversidade tecnológica permitem avaliar se o arranjo normativo está ampliando resiliência ou apenas gerando mais obrigações formais.

A demarcação de um caminho regulatório eficaz se torna ainda mais crítica ao considerarmos as dimensões geopolíticas.

É indispensável distinguir os dois principais usos políticos da ideia de "soberania digital": (i) um centrado na construção de capacidades, como o investimento em formação profissional, P&D e a integração com ecossistemas técnicos locais; (ii) outro focado no controle, que se manifesta por meio de restrições de mercado e preferências de origem.

Nesse cenário, o modelo brasileiro deve fazer também uma escolha de natureza política sobre qual tipo de soberania digital irá priorizar. A análise do PL 4752/2025 (especialmente nos dispositivos sobre preferências nacionais de aquisição e classificação de risco) sugere que o projeto contém elementos de ambas as trajetórias. O balanço final entre a soberania como capacidade e a soberania como controle é um ponto de tensão central para a manutenção das propriedades críticas da Internet, como a Infraestrutura Acessível com Protocolo Comum (PC1), tema que será abordado a seguir.

4.1 PC1 –Uma Infraestrutura Acessível com um Protocolo Comum

⚠ Avaliação: Risco baixo com potencial negativo

O PL 4752/2025 não versa diretamente sobre os protocolos da Internet (TCP/IP, DNS etc.) nem substitui nenhum padrão existente. Contudo, ao definir condições mínimas de segurança (Art. 5) baseadas em 'normas nacionais e internacionais reconhecidas', o projeto tem o seu efeito potencialmente aplicado aos protocolos da Internet de forma indireta.

Cabe notar que a referência cumulativa a padrões nacionais e internacionais abre, em tese, a possibilidade de que padrões nacionais sejam priorizados em detrimento da normatização internacional, um caminho que poderia, no limite, levar à segmentação. Todavia, é importante registrar que o Brasil não possui histórico de adoção de padrões incompatíveis com a normatização internacional, e não há indícios concretos de que o PL tenha esse objetivo. O risco, portanto, é de natureza estrutural e prospectiva, não decorrente de uma intenção manifesta do legislador.

Entretanto, o privilégio de soluções e fornecedores nacionais (Art.14 §1º) pode gerar um risco indireto se o desenvolvimento de tecnologias locais de cibersegurança não estiver necessariamente alinhado com os protocolos e padrões internacionais estabelecidos da Internet, potencialmente criando divergência da pilha de protocolos comum que sustenta a alcançabilidade global.

A questão central, porém, não é buscar soberania tecnológica, mas sim como essa soberania é instrumentalizada. Há duas trajetórias possíveis, e o PL, em sua redação atual, não deixa claro qual delas será seguida.

Nesse sentido, soberania como capacidade é a trajetória que fortalece o ecossistema nacional sem ameaçar a infraestrutura global compartilhada. Nessa lógica, o Estado investe em formação de profissionais, incentiva P&D nacional em cibersegurança, fomenta empresas brasileiras capazes de competir tecnicamente no mercado global e cria certificações que elevam o patamar de qualidade dos produtos nacionais. O resultado é que a soberania se expressa como competência acumulada, não como fechamento.

Países que seguiram essa trajetória, como Israel, Estônia e, mais recentemente, o Chile, construíram ecossistemas nacionais de cibersegurança robustos sem fragmentar a infraestrutura comum. O Brasil, inclusive, já tem instrumentos nessa direção nos Arts. 19–21 do próprio PL, que criam programas de capacitação e P&D. Esses dispositivos são exatamente o tipo de soberania como capacidade que não levanta preocupações para PC1.

Soberania como controle é a trajetória que cria preferências, restrições ou exclusões baseadas em origem geográfica ou critérios não-técnicos. Nessa lógica, o Estado não apenas investe no ecossistema nacional, mas também isola o mercado público de fornecedores estrangeiros, seja diretamente (através de preferências de aquisição) ou indiretamente (através de índices de risco sem critérios transparentes).

O risco para PC1 emerge quando produtos implantados em infraestruturas públicas não implementam corretamente protocolos fundamentais da Internet – como IPv6, DNSSEC, TLS 1.3 ou mecanismos de segurança de roteamento como RPKI. A adoção de tecnologias com implementações incompletas ou incompatíveis pode, ao longo do tempo, criar inconsistências operacionais na infraestrutura pública. Além de afetar a interoperabilidade, a ausência desses mecanismos também cria vulnerabilidades estruturais, facilitando ataques como sequestro de rotas BGP, envenenamento de DNS e interceptação de comunicações.

Para evitar esse risco, o projeto deveria exigir que quaisquer soluções nacionais priorizadas sejam plenamente compatíveis com o conjunto de protocolos Internet.

Recomendação: Exigir explicitamente que todos os padrões mínimos de cibersegurança adotados sob o Art. 5 sejam consistentes com organismos de padrões abertos da Internet internacionalmente reconhecidos (IETF, ICANN, ISO, ITU).

4.2 PC2 – Arquitetura Aberta de Blocos Estruturais Interoperáveis e Reutilizáveis

⚠ Avaliação: Risco baixo com potencial negativo

A arquitetura em camadas da Internet permite construir serviços complexos a partir de blocos modulares. Cada camada (física, enlace, rede, transporte, aplicação) tem protocolos bem definidos e abertos. Por exemplo, blocos estruturais típicos incluem o protocolo de transporte TCP (para entrega confiável) e o IEEE 802.11 (Wi-Fi) na camada de enlace. O PL não rompe essa arquitetura, já que não define nenhum bloco privativo nem impõe novos módulos obrigatórios. Contudo, a arquitetura aberta depende da capacidade de qualquer ator construir soluções ou serviços que se interconectem com os blocos estruturais da Internet sem *gatekeepers*. Várias disposições introduzem dinâmicas de *gatekeeping*:

- Art. 14, §1º (Preferências Nacionais de Aquisição): Priorizar produtos e serviços desenvolvidos nacionalmente cria uma preferência para um subconjunto de tecnologias disponíveis, podendo limitar a gama de componentes interoperáveis, a depender da força dessa priorização. Ainda que não impeça a contratação de soluções estrangeiras, a preferência cria um viés de seleção que pode, na prática, reduzir a gama de componentes interoperáveis considerados nas aquisições públicas, especialmente se os critérios de aplicação da preferência não forem objetivamente definidos.

- Art. 14, §2º (Restrição de Soluções Sem Suporte): O poder de restringir *software* descontinuado pode ser uma medida de segurança sensata, porém, na ausência de critérios claros, dá à autoridade discricionariedade para excluir fornecedores ou famílias de tecnologia.

- Art. 14, §3º (Índice de Classificação de Risco de Fornecedores): Embora a definição material dos critérios de classificação de risco deva ser remetida à regulamentação, a legislação primária deveria estabelecer o procedimento para sua elaboração e revisão, incluindo consulta multissetorial obrigatória (via conselhos do Art. 18), publicação prévia dos critérios, periodicidade de revisão e mecanismos de recurso para fornecedores classificados de modo a garantir que quaisquer restrições se apliquem igualmente a fornecedores nacionais e estrangeiros com base no mérito de segurança, não na origem. .

É importante distinguir que, dentre as soluções de cibersegurança abrangidas pelo PL, aquelas que operam na camada de infraestrutura da Internet, como implementações de protocolos de transporte, roteamento e resolução de nomes, devem manter compatibilidade com os padrões abertos da IETF para preservar a interoperabilidade da rede.

> *Recomendação: Estabelecer critérios claros, publicamente disponíveis e objetivos para decisões de classificação de risco de fornecedores e restrição de tecnologia. Garantir que quaisquer restrições se*

> *apliquem igualmente a fornecedores nacionais e estrangeiros com base no mérito de segurança, não na origem.*

4.3 PC3 – Gerenciamento Descentralizado e um Sistema de Roteamento Distribuído Comum

⚠ Avaliação: Risco baixo com potencial negativo

O PL 4752/2025 não trata diretamente de roteamento, sistemas autônomos ou operações de raiz DNS. Contudo, os poderes de auditoria conferidos à autoridade nacional (Art. 4º) alcançam potencialmente qualquer sistema digital, inclusive sistemas de roteamento. Com base nos resultados dessas auditorias, a autoridade pode limitar a utilização de sistemas considerados inseguros por membros do Programa Nacional de Segurança e Resiliência Digital (Art. 7º). Assim, embora a infraestrutura de roteamento não seja objeto direto da legislação, decisões da autoridade poderiam, indiretamente, afetar as escolhas tecnológicas em matéria de roteamento dentro do setor público.

A resiliência da Internet deriva significativamente de sua governança descentralizada e multissetorial. Uma autoridade nacional com poder de restringir soluções tecnológicas para uma parte significativa da economia digital brasileira poderia, ao longo do tempo, consolidar o controle sobre decisões críticas de infraestrutura da Internet.

Além disso, políticas de soberania que se apoiam em controle estatal ("*command and control*") podem frustrar propriedades críticas como o gerenciamento descentralizado. Além disso, se os poderes da autoridade forem posteriormente estendidos, seja através de legislação subsidiária ou normas setoriais (Art. 4), a operadores privados de infraestrutura crítica e provedores de serviços de Internet, o risco para o gerenciamento descentralizado seria substancialmente maior.

Em contrapartida, há oportunidades: a gestão de riscos na cadeia de suprimentos (Art.13) pode, se bem feita, melhorar a resiliência do roteamento público. Ao exigir, por exemplo, certificações de segurança em dispositivos de rede (firewalls, roteadores) usados pelo governo, o PL fortalece a estabilidade da rede pública.

Portanto, recomenda-se que o texto da lei ou dos regulamentos seja complementado, estabelecendo que nenhuma modificação obrigatória de roteamento será implementada sem ampla consulta técnica.

> *Recomendação: Limitar claramente os poderes normativos e o escopo da autoridade na legislação primária. Garantir que qualquer extensão a entidades do setor privado exija aprovação parlamentar adicional. Exigir que decisões que afetem roteamento e endereçamento da Internet sejam feitas em coordenação com o NIC.br e o CGI.br, bem como observem as práticas já estabelecidas em nível internacional através da ICANN, do IETF e de outras entidades relevantes.*

4.4 PC4 – Identificadores Globais Comuns

✔ Avaliação: Não Impactado

O PL 4752/2025 não contém disposições que afetariam DNS, endereçamento IP, identificadores de roteamento ou outros recursos globalmente únicos de nomeação e numeração da Internet porque não contempla a criação de sistemas de nomeação paralelos, raízes DNS nacionais ou fragmentação do espaço de endereços global.

4.5 PC5 – Uma Rede de Propósito Geral e Tecnologicamente Neutra

⚠ Avaliação: Risco baixo com potencial negativo

A Internet foi concebida para múltiplos usos, sem otimização apenas para um tipo de tráfego. Ela foi concebida como uma rede de propósito geral desde o início, sendo que a neutralidade tecnológica permite que ela sirva propósitos que não foram previstos no momento do *design*.

O PL 4752 não impõe a utilização de uma arquitetura de rede ou protocolo específico, logo, a neutralidade de uso permanece preservada. Contudo, a combinação de preferências nacionais de aquisição (Art. 14, §1º) com o poder da autoridade de restringir soluções tecnológicas (Art. 14, §2º) introduz um viés de seleção que pode, na prática, favorecer determinadas famílias tecnológicas ou aplicações em detrimento de outras.

Essa preferência cria um ambiente regulatório no qual a escolha de tecnologia deixa de ser orientada exclusivamente por critérios funcionais e de interoperabilidade, passando a incorporar variáveis de origem geográfica e conformidade administrativa.

O risco indireto para a PC5 reside no fato de que, ao longo do tempo, a restrição do universo de soluções disponíveis para a administração pública pode limitar a capacidade do setor público de adotar tecnologias emergentes que ainda não possuem versão nacional, criando uma defasagem tecnológica que compromete a premissa de propósito geral. Além disso, se o índice de classificação de risco (Art. 14, §3º) operar com critérios opacos, fornecedores de tecnologias inovadoras podem ser dissuadidos de participar do mercado público brasileiro, reduzindo a diversidade de soluções disponíveis e, por consequência, a capacidade da rede de servir a fins não antecipados.

Conforme discutido na análise transversal, a trajetória de soberania como capacidade (Arts. 19–21) é a que melhor preserva PC5, criando condições para que soluções brasileiras sejam competitivas..

Por outro lado, a trajetória de soberania como controle, apoiada em preferências de origem e critérios opacos de classificação de risco (Art. 14, §3º), pode produzir o efeito inverso criando defasagem tecnológica que compromete a premissa de propósito geral da rede.

Além disso, o PL 4752/2025 deve ser interpretado em harmonia com a Lei nº 12.965/2014 (Marco Civil), especialmente com relação aos art. 9º (neutralidade de rede), art. 10º (discriminação ou degradação de tráfego), e art. 11º (priorização de aplicações).

A Autoridade Nacional de Cibersegurança não deve ter poderes para determinar priorização de tráfego ou bloqueio de protocolos específicos sob justificativa de segurança, exceto em casos de incidentes ativos comprovados, com supervisão judicial. Ademais, quanto ao risco de Fragmentação de Camada, se o índice de classificação de risco (Art. 14, §3º) resultar em restrições baseadas em protocolos específicos (ex: bloqueio de VPNs, Tor, ou protocolos P2P), isso configura violação da neutralidade tecnológica e poderia fragmentar a arquitetura em camadas da Internet.

> *Recomendação: Assegurar que os critérios de seleção tecnológica priorizem interoperabilidade, conformidade com padrões abertos e mérito técnico, garantindo que a neutralidade tecnológica da Internet seja preservada como princípio orientador das aquisições públicas em cibersegurança e que a soberania seja alcançada como construção de capacidade, condicionando eventuais preferências nacionais à demonstração de conformidade com padrões abertos e interoperáveis da Internet. assegurando que o fortalecimento do ecossistema brasileiro se dê pela via da excelência e não pela restrição do acesso a tecnologias. Além disso, deve-se incluir dispositivo que: i) garanta que nenhuma restrição tecnológica viole o princípio de neutralidade de rede; ii) exija que decisões de bloqueio ou filtragem sejam temporárias, proporcionais e supervisionadas judicialmente; iii) proíba discriminação baseada em tipo de aplicação ou protocolo.*

5. Impacto nos Habilitadores de uma Internet Aberta, Globalmente Conectada, Segura e Confiável

Objetivo 1: Internet Aberta

5.1 H1 – Acesso Fácil e Irrestrito

⚠ Avaliação: Risco baixo com potencial misto

O projeto não impõe restrições diretas de acesso a usuários finais ou provedores de serviços de Internet. No entanto, as preferências nacionais de aquisição de tecnologia (Art. 14, §1º) e o índice de classificação de risco de fornecedores (Art. 14, §3º) poderiam limitar indiretamente o acesso a tecnologias e serviços específicos para entidades dentro do escopo do projeto.

Se o índice de classificação de risco resultar na exclusão efetiva de grandes fornecedores internacionais de tecnologia das aquisições do setor público brasileiro, isso restringiria o acesso das entidades do setor público a um ecossistema tecnológico globalmente diversificado.

Por outro lado, a lei promove investimentos em cibersegurança (3% do Fundo Nacional de Segurança Pública), que podem financiar melhor infraestrutura de rede em órgãos públicos menos atendidos. Isso melhora o acesso desses órgãos à Internet (mais banda, menor latência). Para equilibrar o impacto, recomenda-se que a futura Agência implemente o índice de risco com critérios estritamente técnicos (por exemplo, vulnerabilidades conhecidas, histórico de falhas) e que permita concorrência de soluções de código aberto ou internacionais que comprovem conformidade.

Deve-se lembrar que a Internet "não obedece fronteiras" : esforços de soberania digital devem expandir capacidades internas sem criar portões de acesso.

> *Recomendação: O índice de risco de fornecedores deve ser baseado em critérios estritamente técnicos (vulnerabilidades, histórico de falhas), não em origem nacional, permitindo competição de soluções abertas e internacionais que comprovem conformidade.*

5.2 H2 – Uso irrestrito e fomento ao desenvolvimento de tecnologias para a Internet

⚠ Avaliação: Risco médio com potencial negativo

Este é o habilitador mais diretamente em risco pelo PL 4752/2025. A combinação de preferências nacionais de aquisição (Art. 14, §1º), o poder da autoridade de restringir soluções (Art. 14, §2º) e o índice de classificação de risco de fornecedores (Art. 14, §3º) cria um arcabouço em que a implementação de tecnologia dentro do setor público está sujeita a *gatekeeping* centralizado.

Historicamente, políticas desse tipo foram usadas não apenas para cibersegurança, mas também para favorecer políticas industriais. No caso brasileiro, não há indicação explícita de imposição de padrões técnicos diferentes, mas o recurso de restringir soluções desatualizadas dá poder à autoridade de decidir caso a caso. Isso pode gerar receio nos fornecedores de tecnologia de que atualizações possam ser barradas por critérios de risco. Internacionalmente, políticas de "soberania tecnológica" tendem a seguir dois caminhos: (i) fortalecem o mercado interno (causando danos mínimos à Internet) ou (ii) aumentam controles estatais (podendo fragmentar a rede).

A arquitetura da Internet prosperou justamente porque qualquer participante pode implementar e inovar sobre seus protocolos abertos sem gatekeepers; a introdução de mecanismos de aprovação centralizados, mesmo com boas intenções, pode erodir gradualmente esse princípio fundamental.

> *Recomendação: Definir fundamentos precisos e exaustivos para restrição de tecnologia na legislação primária. Exigir a abertura de consultas públicas multissetoriais para restrições que afetem múltiplas entidades ou classes de tecnologia. Alinhar metodologia de classificação com estruturas internacionais para prevenir exclusões arbitrárias.*

5.3 H3 – Desenvolvimento, Gerenciamento e Governança Colaborativos

✔ Avaliação: Impacto Positivo

A disposição do Art. 18 para conselhos consultivos multissetoriais e grupos de trabalho é um aspecto que se alinha com os princípios de governança colaborativa da Internet. A inclusão da sociedade civil, academia, setor privado e governo nos processos de definição de padrões de cibersegurança espelha o modelo multissetorial que sustenta a governança da Internet no nível global.

O Art. 3, V nomeia explicitamente a colaboração intersetorial como princípio orientador do Programa Nacional. Os Arts. 19–21 com foco em educação, treinamento e P&D fomentam um ecossistema nacional mais amplo de expertise em cibersegurança. Os requisitos de transparência do Art. 25 apoiam ainda mais a governança colaborativa responsável.

> *Recomendação: para maximizar o impacto positivo deste habilitador, os conselhos consultivos devem ter papéis significativo sem decisões sobre definição de padrões e restrição de tecnologia.*

Objetivo 2: Internet Globalmente Conectada

5.4 H4 – Alcance Irrestrito

✔ Avaliação: Não Impactado

O PL 4752/2025 não contém disposições que restringiriam a alcançabilidade da rede, imporiam mandatos de bloqueio ou criariam restrições de roteamento.

Tecnologicamente, a Internet considera que um pacote IP do servidor A deve chegar ao usuário B independente das políticas locais. Assim, a conectividade cresce à medida que mais participantes se conectam. Reforçando esse ponto, o Art.2 do PL destaca a continuidade das comunicações digitais como vital para a soberania tecnológica, o que implica justamente manter enlaces internacionais.

A legislação não visa a filtragem de conteúdo, obrigações de ISP para gerenciamento de tráfego ou restrições de fluxo de dados transfronteiriços. A alcançabilidade irrestrita na camada de rede não é ameaçada por este projeto.

5.5 H5 – Capacidade da Rede

✔ Avaliação: Impacto Positivo

As significativas disposições de financiamento do projeto (Art. 26 alocando 3% do Fundo Nacional de Segurança Pública e 2% das receitas de apostas de quota fixa para cibersegurança) apoiarão investimentos em infraestrutura que contribuem para a capacidade e resiliência da rede.

Ao fortalecer a postura de cibersegurança de sistemas governamentais, a legislação reduz a probabilidade de incidentes cibernéticos em larga escala que podem degradar a capacidade de rede para todos os usuários.

A disposição do Art. 20 para programas nacionais de P&D em cibersegurança também pode gerar inovações que melhoram o desempenho da rede e o gerenciamento de capacidade.

Objetivo 3: Internet Segura

5.6 H6 – Confidencialidade de dados, informações, dispositivos e aplicativos

✔ Avaliação: Impacto Positivo

A orientação geral de cibersegurança do projeto, incluindo padrões mínimos (Art. 5), cultura de cibersegurança (Art. 3, III) e programas de treinamento (Art. 19), deve promover a adoção de práticas de criptografia e comunicações seguras em todo o setor público. Posturas mais fortes de cibersegurança governamental reduzem riscos sistêmicos que poderiam comprometer a confidencialidade de dados para cidadãos que interagem com serviços públicos.

Outro ponto positivo é que o projeto não contém disposições que exijam *backdoors*, criptografia enfraquecida ou custódia de chaves, medidas que prejudicaram a confidencialidade de dados em outras estruturas legislativas de cibersegurança.

Não obstante, seria mais contundente explicitar no PL que mecanismos fortes de criptografia devem ser permitidos e mesmo incentivados. Caso a autoridade nacional estabeleça padrões de segurança cibernética (Art. 5), faz sentido que esses incluam criptografia de dados em trânsito (TLS 1.3, como mínimo) e em repouso, além da adoção de protocolos de segurança na camada de infraestrutura, como DNSSEC, RPKI e DMARC/SPF/DKIM para segurança de e-mail.

A ausência de restrições à criptografia no texto sugere que a confidencialidade pode ser mantida conforme boas práticas internacionais, mas a explicitação desses requisitos em posterior regulamento da Autoridade fortaleceria a postura de segurança do arcabouço normativo e sinalizaria compromisso com a segurança da camada de infraestrutura da Internet.

Considerando a soberania digital no sentido de proteção dos cidadãos, recomenda-se afirmar explicitamente que nenhuma norma obrigará a quebra de criptografia ou coleta excessiva de dados

pessoais. Tecnologias como VPNs, Tor e criptografia ponta-a-ponta devem permanecer disponíveis para uso público e governamental onde necessário, desde que compatíveis com a lei.

> *Recomendação: O PL deve afirmar explicitamente que os padrões de cibersegurança (Art. 5) incluem criptografia forte em trânsito e em repouso, e que nenhuma norma poderá obrigar a quebra de criptografia ou coleta excessiva de dados pessoais.*

5.7 H7 – Integridade de dados, informações, dispositivos e aplicativos

✔ Avaliação: Impacto Positivo

Integridade significa garantir que dados e sistemas não sejam alterados indevidamente. O PL 4752 enfatiza controles de segurança que reforçam a integridade. O Art. 13 obriga avaliação de riscos de fornecedores e a mitigação de falhas em toda a cadeia , o que implica auditorias e testes regulares – práticas que melhoram a integridade geral.

Além disso, o Art. 14 §2º permite proibir soluções desatualizadas ou inseguras , incentivando o uso de versões de software corrigidas. Por exemplo, se um sistema crítico possui vulnerabilidade de injeção SQL, ele teria de ser substituído ou atualizado para não figurar na lista proibida. Esse tipo de medida, quando transparente, aumenta a confiança de que os serviços públicos serão executados sem adulteração.

Contudo, há *trade-offs*. Se o índice de risco for aplicado por questões não-técnicas, pode haver menos alternativas de alta integridade. Por isso é essencial que a futura Agência adote *frameworks* internacionais de verificação de integridade (ex.: modelos de maturidade em segurança cibernética) e permissão de certificações de terceiros para que um fornecedor atenda os critérios sem discriminação.

A interoperabilidade de logs e registros de eventos também deve ser incentivada para que, por exemplo, se use formatos abertos de log (JSON, syslog padrão), permitindo auditoria independente. Ao permitir que quaisquer partes interessadas revisem a integridade dos sistemas públicos (como previsto pela transparência do PL), reforça-se que os dados e serviços públicos não serão corrompidos, mantendo-se a integridade e reforçando princípios que permitem que a Internet continue sendo global e segura..

Objetivo 4: Internet Confiável

5.8 H8 – Confiabilidade, resiliência e conectividade otimizada

✔ Avaliação: Impacto Positivo

A resiliência é apresentada como um objetivo central do projeto. O requisito do Art. 11 para políticas de continuidade e recuperação aborda diretamente a resiliência de serviços digitais governamentais. Além disso, o Art. 2 parágrafos I e XV listam, como objetivos, fortalecer a resiliência cibernética e garantir a continuidade das comunicações digitais mesmo em crise.

Na prática, isso significa que os órgãos federais devem manter várias rotas de conexão, sistemas redundantes e planos de recuperação. Tecnologias como replicação de dados, failover automático e redes definidas por software (SDN) podem ser apoiadas para melhorar a disponibilidade de sistemas governamentais. Além disso, o mecanismo de notificação de incidentes do Art. 12 cria um ciclo de *feedback* que deve melhorar a resiliência coletiva.

5.9 H9 – Prestação de Contas e Responsabilidade

✔ Avaliação: Impacto Positivo

Os requisitos de transparência e responsabilização do Art. 25 para a autoridade nacional estão bem alinhados com este habilitador. A responsabilização em cibersegurança significa que agentes saibam suas obrigações e sofram consequências por falhas. O PL define claramente que gestores públicos serão responsabilizados pela implementação das normas e resposta a incidentes (Art. 2 XIII).

O projeto estabelece poderes de auditoria e fiscalização (Art. 4) que criam mecanismos de responsabilização para entidades dentro de seu escopo. A notificação obrigatória de incidentes (Art. 12) também contribui para a responsabilização ao criar um registro de eventos de segurança e respostas.

Contudo, para reforçar a cadeia de responsabilização recomenda-se também incluir penalidades para fornecedores falhos. Por exemplo, contratos públicos de tecnologia devem ter cláusulas de Service Level Agreement (SLA) que prevejam multas se vulnerabilidades reportadas não forem corrigidas no prazo acordado. Além disso, a transparência fiscal (Art. 26 Capítulo IV) reforça que despesas em cibersegurança serão auditadas, o que induz resultados mensuráveis. Do ponto de vista do usuário, nada muda diretamente; mas para a infraestrutura, isso significa que haverá documentação e prestação de contas.

> *Recomendação: Incluir nos contratos públicos de tecnologia cláusulas de SLA com penalidades para fornecedores que não corrigirem vulnerabilidades reportadas dentro de prazo acordado, reforçando a cadeia de responsabilização além dos agentes públicos.*

5.10 H10 – Privacidade

⚠ Avaliação: Risco baixo com potencial misto

A privacidade apresenta um quadro misto. No lado positivo, o Art. 3, XI lista explicitamente a proteção da privacidade como princípio orientador do Programa Nacional, e o projeto é descrito como operando em harmonia com a Lei Geral de Proteção de Dados (LGPD) do Brasil.

É certo que o projeto não regula diretamente dados pessoais; ainda assim, qualquer aumento na supervisão governamental de redes pode criar preocupações de privacidade. Tecnicamente, recomenda-se tratar a privacidade por design: por exemplo, exigir que sistemas federais usem criptografia para dados sensíveis e coletem apenas o necessário para segurança. Uma medida concreta seria determinar que toda rede governamental use VPNs ou criptografia de ponta a ponta para comunicações internas, seguindo padrões globais. Além disso, como salvaguarda, órgãos de auditoria (internos e CGU) devem atuar para que execuções de vigilância ou coleta de dados sob o PL respeitem a Lei Geral de Proteção de Dados (LGPD).

Portanto, as obrigações de notificação de incidentes (Art. 12), se envolverem o compartilhamento de dados pessoais de indivíduos afetados com a autoridade nacional, devem ter seu escopo cuidadosamente definido para cumprir os princípios de proporcionalidade da LGPD. Os poderes de auditoria e fiscalização da autoridade (Art. 4) sobre sistemas governamentais criam amplo acesso a dados sensíveis que requer salvaguardas legais robustas e mecanismos de supervisão.

> *Recomendação: Exigir que os relatórios de incidentes (Art. 12) utilizem dados anonimizados ou pseudonimizados por padrão, e que os poderes de auditoria (Art. 4) sejam exercidos com salvaguardas explícitas de proporcionalidade alinhadas à LGPD.*

6. Tabela de Impacto

As tabelas a seguir fornecem uma visão consolidada do impacto avaliado do PL 4752/2025 nas Propriedades Críticas do Modo Internet de Interconectividade e nos Habilitadores OGST.

6.1 Propriedades Críticas

Ref.	Propriedade Crítica	Avaliação	Detalhe
PC1	Infraestrutura Acessível com Protocolo Comum	PREOCUPAÇÃO	Limitada
PC2	Arquitetura Aberta de Blocos Estruturais Interoperáveis e Reutilizáveis	PREOCUPAÇÃO	Moderada
PC3	Gerenciamento Descentralizado e Sistema de Roteamento Distribuído Único	PREOCUPAÇÃO	Limitada
PC4	Identificadores Globais Comuns	NÃO IMPACTO	–

Ref.	Propriedade Crítica	Avaliação	Detalhe
PC5	Rede de Propósito Geral e Tecnologicamente Neutra	PREOCUPAÇÃO	Moderada

6.2 Habilitadores OGST

Ref.	Objetivo	Habilitador	Avaliação	Dir.
H1	Aberta	Acesso Fácil e Irrestrito	MISTO	~
H2	Aberta	Uso irrestrito e fomento ao desenvolvimento de tecnologias para a Internet	PREOCUPAÇÃO	–
H3	Aberta	Desenvolvimento, Gerenciamento e Governança Colaborativos	POSITIVO	+
H4	Global	Alcance Irrestrito	NÃO IMPACTO	–
H5	Global	Capacidade da Rede	POSITIVO	+
H6	Segura	Confidencialidade de dados, informações, dispositivos e aplicativos	POSITIVO	+
H7	Segura	Integridade de dados, informações, dispositivos e aplicativos	POSITIVO	+
H8	Confiável	Confiabilidade, resiliência e conectividade otimizada	POSITIVO	+
H9	Confiável	Prestação de Contas e Responsabilidade	POSITIVO	+
H10	Confiável	Privacidade	MISTO	~

7. Conclusões e Recomendações

7.1 Aspectos Positivos

O PL 4752/2025 contém várias disposições que representam contribuições positivas para a resiliência e confiabilidade da Internet no Brasil:

- Financiamento dedicado para cibersegurança (Art. 26), cuja adequação ao volume de incidentes no escopo da lei deverá ser avaliada com base em dados que permitam dimensionar a demanda efetiva.

- Notificação obrigatória de incidentes (Art. 12) cria responsabilização institucional e permite aprendizado coletivo.

- Governança de riscos da cadeia de suprimentos (Arts. 13–15) aborda um vetor de ameaça contemporâneo crítico.

- Conselhos consultivos multissetoriais (Art. 18) e colaboração como princípio orientador (Art. 3, V) se alinham com melhores práticas de governança da Internet.

- Requisitos de transparência e responsabilização (Art. 25) apoiam a supervisão democrática.

- Alinhamento com a LGPD e privacidade como princípio orientador (Art. 3, XI).

- O projeto evita os padrões legislativos de cibersegurança mais prejudiciais: não há requisitos de backdoor de criptografia, mandatos de filtragem de conteúdo e restrições de roteamento ou obrigações de localização de dados, preservando assim as propriedades fundamentais do Modo Internet de Interconectividade.

7.2 Áreas de Preocupação

As seguintes disposições do PL 4752/2025 criam riscos para a arquitetura aberta e interoperável da Internet e devem ser abordadas durante o processo legislativo:

- Preferências Nacionais de Aquisição de Tecnologia (Art. 14, §1º): O protecionismo econômico em aquisições de tecnologia, se estendido a software e infraestrutura relevantes para segurança, corre o risco de criar pilhas de tecnologia incompatíveis e reduzir a diversidade de componentes interoperáveis disponíveis para entidades públicas brasileiras.

- Poderes Centralizados de Restrição (Art. 4 e Art. 14, §2º): O poder da autoridade nacional de restringir soluções tecnológicas, sem critérios claramente definidos, devido processo ou requisitos de proporcionalidade na legislação primária, cria um mecanismo de *gatekeeping* que poderia ser mal utilizado.

- Índice de Classificação de Risco de Fornecedores (Art. 14, §3º): Sem critérios transparentes e internacionalmente alinhados e mecanismos significativos de recurso, este índice poderia funcionar como uma lista negra efetiva, reduzindo a diversidade tecnológica e criando barreiras para fornecedores internacionais.

- Tensões de Privacidade (Art. 4, Art. 12): Os poderes de fiscalização e auditoria da autoridade e as obrigações de notificação de incidentes exigem salvaguardas explícitas compatíveis com a LGPD para prevenir coleta e compartilhamento de dados desproporcionais.

- Ausência de Disposições sobre Divulgação Coordenada de Vulnerabilidades: O PL não prevê mecanismos de proteção a pesquisadores de segurança de boa-fé nem prazos para correção de vulnerabilidades por fabricantes. Essa lacuna pode desincentivar a pesquisa independente de segurança, prolongar a exposição a vulnerabilidades críticas em infraestrutura compartilhada da Internet e enfraquecer a cadeia de defesa cibernética em suas fases mais precoces.

7.3 Recomendações Legislativas

Com base nesta análise, as seguintes emendas legislativas específicas e medidas de implementação são recomendadas para fortalecer o alinhamento do PL 4752/2025 com os princípios do Modo Internet de Interconectividade:

#	Dispositivo	Recomendação
R1	Art. 14, §1º (Preferências de Aquisição)	Substituir preferências baseadas exclusivamente em origem nacional por requisitos de certificação de segurança reconhecidos, sejam internacionais (Common Criteria, ISO 27001, FIPS 140-3) ou nacionais, desde que baseados em critérios técnicos objetivos e aplicados de forma não discriminatória a todos os fornecedores. Adicionalmente, considerar a inclusão de requisitos de tratamento de dados críticos em território nacional como critério complementar de segurança, alinhado com a LGPD e com práticas internacionais de proteção de dados sensíveis.
R2	Art. 14, §2º (Poderes de Restrição)	Definir na legislação primária a lista exaustiva de fundamentos para restrições de tecnologia. Exigir consulta multissetorial prévia (conselhos do Art. 18) e avaliação de proporcionalidade antes de impor restrições. Criar um processo de recurso expedito.
R3	Art. 14, §3º (Índice de Risco de Fornecedores)	Exigir que a metodologia de classificação seja desenvolvida em processo multissetorial do Art. 18, publicada antecipadamente e alinhada com estruturas de risco internacionais (NIST SP 800-161, ENISA). Exigir relatórios públicos anuais e auditorias independentes de decisões de classificação.
R4	Art. 4 (Escopo da Autoridade)	Esclarecer na legislação primária que os poderes normativos da autoridade se aplicam exclusivamente a entidades da administração pública federal inscritas no Programa. Qualquer extensão a entidades do setor privado deve exigir autorização parlamentar separada.

#	Dispositivo	Recomendação
R5	Art. 5 (Padrões Mínimos)	Exigir explicitamente que todos os padrões mínimos de cibersegurança adotados pela autoridade sejam compatíveis com padrões da Internet da IETF, ISO e ITU-T. Os padrões não devem exigir protocolos proprietários ou excluir soluções de código aberto.
R6	Arts. 12 e 4 (Notificação e Auditoria)	Especificar que relatórios de incidentes devem usar dados técnicos anonimizados ou pseudonimizados por padrão. Estabelecer requisitos de supervisão judicial para acesso da autoridade a informações pessoalmente identificáveis. Exigir *Data Protection Impact Assessments* (DPIAs) para as funções principais de processamento de dados da autoridade.
R7	Art. 18 (Conselhos Multissetoriais)	Elevar conselhos consultivos a status de consulta obrigatória para todas as decisões normativas que afetem a arquitetura da Internet, incluindo restrições de tecnologia, normas da cadeia de suprimentos e padrões mínimos. Exigir que recomendações dos conselhos sejam publicadas ao lado das decisões da autoridade.
R8	Novo dispositivo (divulgação coordenada de vulnerabilidades e Protocolos de Infraestrutura)	Incluir disposições sobre Divulgação Coordenada de Vulnerabilidades com *safe harbors* para pesquisadores de boa-fé e prazos para correção por fabricantes. Incorporar nos padrões mínimos (Art. 5) a exigência de adoção de protocolos de segurança na camada de infraestrutura da Internet (RPKI, DNSSEC, TLS 1.3, IPv6) como requisitos obrigatórios para entidades participantes do Programa.
R9	Art. 3º (Definições)	Adicionar definição de criptografia forte nos seguinte termos: “algoritmos, protocolos e implementações criptográficas que atendam, cumulativamente, aos seguintes requisitos: a) ofereçam nível de segurança compatível com o estado da arte reconhecido por organismos internacionais de padronização (IETF, NIST, ISO/IEC) e pela comunidade técnica, conforme regulamentação da autoridade competente; b) não contenham vulnerabilidades intencionais, mecanismos de acesso excepcional (*backdoors*) ou funcionalidades que permitam a terceiros, incluindo o próprio desenvolvedor, contornar os mecanismos de proteção criptográfica; c) permitam, quando aplicável, a verificação independente de conformidade por meio de auditoria técnica, revisão por pares e/ou publicação do código-fonte.

#	Dispositivo	Recomendação
R10	Art. 3º (Diretrizes)-	Adicionar vedação de backdoors criptográficos: "XVI – proteção da integridade criptográfica: nenhuma norma, regulamento ou decisão administrativa poderá: a) exigir a inclusão de vulnerabilidades, mecanismos de acesso excepcional ou funcionalidades de interceptação em sistemas, aplicações ou protocolos que utilizem criptografia; b) obrigar a custódia, o depósito ou o compartilhamento de chaves criptográficas privadas com terceiro; c) determinar o enfraquecimento, a substituição ou a não adoção de algoritmos, protocolos ou implementações criptográficas reconhecidos pela comunidade técnica internacional, ou influenciar o estabelecimento de padrões criptográficos senão para promover maior nível de segurança; d) impedir ou restringir o uso de criptografia de ponta a ponta por parte de usuários, entidades públicas ou prestadores de serviço."
R11	Art. 5º (Padrões Mínimos)	Adicionar requisitos criptográficos específicos: "§ 2º Os padrões mínimos de cibersegurança de que trata o caput deverão incluir requisitos para proteção criptográfica, observados os seguintes princípios: I – para dados em trânsito: utilização de protocolos de comunicação segura que garantam confidencialidade, autenticidade e forward secrecy, conforme os padrões abertos vigentes reconhecidos pelos organismos internacionais de padronização; II – para dados em repouso: utilização de algoritmos de criptografia simétrica reconhecidos internacionalmente, com gerenciamento seguro do ciclo de vida das chaves criptográficas, incluindo geração, armazenamento, rotação e destruição; III – para infraestrutura crítica: adoção de mecanismos de segurança nas camadas de infraestrutura da Internet, incluindo autenticação de origem de rotas, integridade de resoluções de nomes de domínio e suporte à versão mais recente do protocolo de Internet, conforme padrões desenvolvidos nos fóruns técnicos competentes. § 3º A autoridade competente publicará e manterá atualizada, em prazo não superior a 12 meses da entrada em vigor desta Lei e revisada ao menos a cada 24 meses, lista de referência com os algoritmos, protocolos e parâmetros técnicos que atendam aos requisitos do § 2º, observadas as

#	Dispositivo	Recomendação
		recomendações dos organismos de padronização da Internet (IETF), do NIST, da ISO/IEC e de outros organismos reconhecidos."
R12	Novo dispositivo (Divulgação Coordenada de Vulnerabilidades)	Adicionar Seção XI ao Capítulo III: "Art. 25-A. A autoridade competente instituirá programa de divulgação coordenada de vulnerabilidades, observados os seguintes princípios: I – proteção legal de pesquisadores de segurança que identifiquem e reportem vulnerabilidades de boa-fé, em conformidade com as políticas de divulgação coordenada publicadas pela autoridade; II – estabelecimento de prazos proporcionais à severidade da vulnerabilidade para que fabricantes e desenvolvedores implementem correções, conforme classificação de criticidade definida em regulamento; III – publicação de políticas claras e acessíveis sobre escopo, metodologia permitida, canais de reporte e critérios de boa-fé; IV – vedação de sanções administrativas, civis ou penais contra pesquisadores que atuem em estrita conformidade com as políticas de divulgação coordenada, ressalvadas as hipóteses de dolo ou de desvio manifesto do escopo autorizado; V – incentivo à participação de entidades brasileiras em comunidades internacionais de resposta a incidentes e de divulgação de vulnerabilidades. Parágrafo único. Os prazos de que trata o inciso II serão fixados em regulamento, ouvidos os conselhos consultivos de que trata o art. 18, e revisados periodicamente à luz das melhores práticas internacionais."
R13	Art. 14, §1º (Preferências Nacionais)-	Modificar redação para: "§ 1º A priorização de fornecedores e tecnologias no âmbito do Programa deverá observar, de forma cumulativa, critérios objetivos e não discriminatórios baseados em: I – conformidade demonstrável com padrões técnicos de segurança reconhecidos por organismos internacionais de padronização; II – rastreabilidade e transparência da cadeia de suprimentos, incluindo a identificação de componentes críticos e suas dependências; III – capacidade de auditoria independente e de verificação de integridade dos componentes de *software* e *hardware*; IV – avaliação de risco jurisdicional baseada em critérios técnicos e objetivos, considerando o arcabouço jurídico aplicável ao

#	Dispositivo	Recomendação
		fornecedor em matéria de acesso governamental a dados e sistemas. § 2º Os critérios de que trata o § 1º aplicam-se igualmente a fornecedores nacionais e estrangeiros, sendo vedada a discriminação baseada exclusivamente na origem geográfica do fornecedor ou da tecnologia. § 3º A metodologia de avaliação dos critérios será desenvolvida com a participação dos conselhos multissetoriais de que trata o art. 18, publicada previamente e revisada ao menos a cada 24 meses. V — disponibilidade do código-fonte para auditoria independente, com preferência, em igualdade de condições técnicas e de segurança, para soluções distribuídas sob licenças de software livre ou de código aberto reconhecidas pela Open Source Initiative (OSI). Parágrafo único. A preferência por soluções de código aberto de que trata o inciso V não exclui soluções proprietárias que demonstrem conformidade com os demais critérios e que permitam auditoria independente por mecanismos equivalentes."

8. Conclusão

O PL 4752/2025 reflete um esforço legítimo e necessário para fortalecer a postura nacional de cibersegurança do Brasil. Os objetivos centrais do projeto, melhorar a resiliência de sistemas digitais governamentais, estabelecer uma capacidade coordenada de resposta a incidentes e construir expertise nacional de cibersegurança, estão alinhados tanto com melhores práticas internacionais quanto com a visão da Internet Society para uma Internet segura e confiável.

No entanto, o impacto do projeto na Internet não é uniformemente positivo. As preferências nacionais de aquisição de tecnologia (Art. 14, §1º) e os poderes centralizados de restrição de tecnologia (Art. 4, Art. 14, §2º–3) introduzem riscos para a arquitetura aberta e interoperável que torna a Internet globalmente valiosa. Essas disposições, se implementadas sem salvaguardas adequadas, poderiam fragmentar o ecossistema tecnológico do Brasil, reduzir o acesso à diversidade global de blocos estruturais interoperáveis e estabelecer um precedente para *gatekeeping* tecnológico justificado por cibersegurança.

Os riscos identificados não são inerentes aos objetivos do projeto, uma vez que eles surgem de escolhas específicas de implementação que podem ser abordadas através de emendas legislativas

direcionadas. As recomendações na Seção 7 fornecem um roteiro concreto para fortalecer o alinhamento do projeto com os princípios do Modo Internet de Interconectividade sem comprometer seus objetivos de cibersegurança.

A Internet Society encoraja legisladores, a autoridade nacional designada e *stakeholders* da sociedade civil a se engajarem com esta análise como parte do processo legislativo. Um arcabouço de cibersegurança projetado desde o início com respeito aos princípios de arquitetura da Internet será mais eficaz, mais durável e mais compatível com o papel do Brasil como ator líder na governança global da Internet.

Anexo I - Glossário de Termos Técnicos

Termo	Definição utilizada
Criptografia End-to-End (E2EE – End-to-End Encryption)	Modelo de comunicação em que os dados são cifrados no dispositivo de origem e decifrados apenas no dispositivo de destino, sem que intermediários (incluindo provedores de serviço) tenham acesso ao conteúdo em texto claro.
Gatekeeping	Controle centralizado exercido por uma entidade (pública ou privada) sobre o acesso a tecnologias, mercados ou infraestruturas, podendo limitar a diversidade de soluções disponíveis e a competição
Neutralidade Tecnológica	Princípio segundo o qual a rede não discrimina com base em tecnologia, protocolo ou aplicação utilizados, permitindo que a Internet sirva a propósitos não previstos no momento de seu projeto.
Divulgação Coordenada de Vulnerabilidades (CVD – Coordinated Vulnerability Disclosure)	Processo estruturado de reporte responsável de falhas de segurança, no qual o pesquisador notifica o fabricante antes da divulgação pública, permitindo a correção da vulnerabilidade dentro de prazos acordados.
DNSSEC (Domain Name System Security Extensions)	Conjunto de extensões de segurança ao protocolo DNS que autentica as respostas de consultas de nomes de domínio por meio de assinaturas digitais, prevenindo ataques como envenenamento de cache DNS.
RPKI (Resource Public Key Infrastructure)	Infraestrutura de chaves públicas que permite a validação criptográfica da origem de anúncios de rotas BGP (Border Gateway Protocol), prevenindo o sequestro de rotas e o redirecionamento malicioso de tráfego na Internet.
Perfect Forward Secrecy (PFS – Sigilo Prospectivo Perfeito)	Propriedade de protocolos criptográficos que garante que as chaves de sessão derivadas não podem ser comprometidas retroativamente, mesmo que a chave privada de longo prazo do servidor seja posteriormente exposta.

BGP (Border Gateway Protocol)	Protocolo de roteamento inter-domínio que permite a troca de informações de alcance entre sistemas autônomos na Internet. Vulnerabilidades no BGP podem permitir o sequestro de rotas e o redirecionamento de tráfego.
CSIRT (Computer Security Incident Response Team)	Equipe especializada em receber, analisar e responder a incidentes de segurança cibernética, coordenando ações de mitigação e recuperação.
Cyber Kill Chain	Modelo desenvolvido pela Lockheed Martin que descreve as sete etapas sequenciais de um ataque cibernético: reconhecimento, armação, entrega, exploração, instalação, comando e controle, e ações sobre o objetivo.
TLS (Transport Layer Security)	Protocolo criptográfico que garante a confidencialidade e integridade das comunicações na Internet. A versão 1.3 (TLS 1.3), publicada em 2018, é a versão mais recente e segura, sendo recomendada como padrão mínimo.
Zero Trust (Confiança Zero)	Modelo de segurança cibernética (NIST SP 800-207) que elimina a confiança implícita em qualquer componente da rede, exigindo verificação contínua de identidade, dispositivo e contexto para cada acesso a recursos.

Anexo II – Análise de Compatibilidade Internacional

Marco	Dimensão	Convergência	Observação
NIS2 (UE)	Notificação obrigatória de incidentes	**CONVERGENTE**	Art. 12 do PL. Sem prazos escalonados equivalentes (24h/72h da NIS2).
NIS2 (UE)	Governança de cadeia de suprimentos	**CONVERGENTE**	Arts. 13–15 do PL endereçam riscos da cadeia de suprimentos.
NIS2 (UE)	Designação de autoridade nacional	**CONVERGENTE**	Art. 4 designa autoridade com poderes normativos, fiscalização e auditoria.
NIS2 (UE)	Requisitos setoriais diferenciados	**LACUNA**	A NIS2 diferencia entidades essenciais e importantes. O PL não adota classificação setorial equivalente.
NIS2 (UE)	Cooperação transfronteiriça	**LACUNA**	A NIS2 cria o EU-CyCLONe. O PL menciona cooperação internacional (Art. 3º, X), mas sem mecanismos operacionais.
DORA (UE)	Resiliência operacional digital	**PARCIAL**	Arts. 5 e 13–15 abordam padrões e riscos, mas sem a especificidade do DORA para o setor financeiro.
DORA (UE)	Testes de resiliência	**LACUNA**	Sem previsão de testes de penetração obrigatórios. Art. 5 pode abranger via regulamentação.
DORA (UE)	Supervisão de terceiros críticos de TIC	**LACUNA**	O DORA estabelece supervisão direta de provedores críticos. PL não possui mecanismo equivalente.
GDPR (UE)	Segurança do processamento (Art. 32)	**PARCIAL**	O PL referencia a LGPD (Art. 3º, XI), mas sem articular requisitos técnicos equivalentes ao Art. 32.
GDPR (UE)	DPIA e Privacy by Design (Arts. 35, 25)	**LACUNA**	Sem previsão de avaliações de impacto nem de proteção de dados por concepção para a autoridade.
GDPR (UE)	Articulação com autoridade de dados	**LACUNA**	Sem mecanismos formais de coordenação entre a autoridade de cibersegurança e a ANPD.

Marco	Dimensão	Convergência	Observação
Cooperação	Redes internacionais de CSIRTs	**LACUNA**	Sem participação obrigatória em comunidades globais (FIRST, CSIRTs regionais).
Cooperação	Interoperabilidade com sistemas de alerta	**LACUNA**	Sem requisitos de interoperabilidade com plataformas globais de compartilhamento de ameaças.
Cooperação	Exercícios internacionais conjuntos	**LACUNA**	Art. 3º, X menciona cooperação, mas sem participação institucionalizada em exercícios.