Junho de 2026

Nota Técnica

E-SegInfo e SISInfo

Contribuição à Consulta Pública — Brasil Participativo

Internet Society
Capítulo Brasil

Elaboração

Everton Vilhena, Heloísa Fernandes, Humberto Antônio Pedroso, João Falcão, José Arthur Alves, Luiza Dutra, Mark W. Datysgeld, Otávio de Souza Martins, Paulo Rená, Pedro Amaral, Thobias Prado Moura

Diretoria Executiva

Flávio Rech Wagner

Pedro de Perdigão Lana

Thobias Prado Moura

Laura Gabrieli Pereira da Silva

Camila Akemi Tsuzuki

João Falcão

Esta nota técnica constitui contribuição institucional da Internet Society — Capítulo Brasil (ISOC Brasil) à Consulta Pública referente à minuta de Decreto que institui a Estratégia Nacional de Segurança da Informação (E-SegInfo) e o Sistema Integrado de Segurança da Informação (SISInfo).

Sumário

Sumário Executivo

Esta nota técnica reúne as contribuições da Internet Society - Capítulo Brasil (ISOC Brasil) à Consulta Pública sobre a minuta de Decreto que institui a Estratégia Nacional de Segurança da Informação (E-SegInfo) e o Sistema Integrado de Segurança da Informação (SISInfo), no âmbito da Política Nacional de Segurança da Informação (Decreto nº 12.572/2025). O objetivo é apoiar o aperfeiçoamento do texto, propondo a incorporação de salvaguardas técnicas e de garantias de direitos fundamentais alinhadas às melhores práticas internacionais reconhecidas; cada contribuição é apresentada com o respectivo diagnóstico, a proposta de redação e a justificativa técnica e comparada que a fundamenta.

Elemento	Descrição
Instrumento	Minuta de Decreto que institui a E-SegInfo e o SISInfo, submetida a consulta pública na plataforma Brasil Participativo.
Base normativa	Regulamenta a Política Nacional de Segurança da Informação (Decreto nº 12.572/2025) e articula-se com a E-Ciber (Decreto nº 12.573/2025), a PNCiber (Decreto nº 11.856/2023) e a LGPD (Lei nº 13.709/2018).
Âmbito de aplicação	Órgãos e entidades do Poder Executivo Federal (administração direta e indireta), com adesão voluntária dos demais Poderes, do Ministério Público, dos Tribunais de Contas, das Defensorias e dos entes federativos.
Objeto da contribuição	Dispositivos sobre criptografia, divulgação coordenada de vulnerabilidades, software auditável e de código aberto, padrões abertos, soberania sobre dados e proteção de direitos fundamentais.
Natureza	Contribuição institucional de caráter técnico, sem pretensão de parecer jurídico vinculante.

As contribuições do Capítulo organizam-se em oito eixos temáticos. O quadro a seguir resume a natureza de cada conjunto de contribuições e os dispositivos da minuta sobre os quais incidem.

Eixo temático	Natureza	Dispositivos-chave
Criptografia forte e vedação a mecanismos de acesso excepcional	Inclusão proposta	Art. 6º, III; Art. 14, VII
Criptografia de ponta a ponta e mensageria institucional segura	Aperfeiçoamento de redação	Art. 16, VII
Divulgação coordenada de vulnerabilidades e proteção a pesquisadores	Inclusão proposta	Art. 14, VIII

Eixo temático	Natureza	Dispositivos-chave
Software livre, código aberto e auditabilidade	Inclusão proposta	Arts. 14; 16; 28; 29; 30; 35
Padrões abertos, interoperabilidade e soberania sobre dados	Aperfeiçoamento de redação	Art. 16, VII; Art. 28; Art. 35, §2º
Direitos fundamentais, privacidade e vedação à vigilância massiva	Inclusão proposta	Art. 10, VI; Art. 35, §1º
Proteção de dados, notificação de incidentes e metadados	Inclusão proposta	Art. 14, IX e X
Participação multissetorial, consulta pública e transparência	Inclusão proposta	Art. 9º, par. único; Art. 19, VI

1. Introdução

A presente nota técnica é apresentada pela ISOC Brasil no âmbito da consulta pública sobre a minuta de Decreto que institui a Estratégia Nacional de Segurança da Informação (E-SegInfo) e o Sistema Integrado de Segurança da Informação (SISInfo). A minuta regulamenta a Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 12.572, de 4 de agosto de 2025, e integra um conjunto mais amplo de instrumentos normativos que inclui a Estratégia Nacional de Cibersegurança (E-Ciber, Decreto nº 12.573/2025), a Política Nacional de Cibersegurança (PNCiber, Decreto nº 11.856/2023), a Estratégia Nacional de Governo Digital (Decreto nº 12.069/2024) e a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018).

A ISOC Brasil reconhece o mérito da iniciativa. A minuta submetida à consulta organiza de forma coerente a governança da segurança da informação no âmbito federal e oferece base sólida para o seu aperfeiçoamento. É nesse espírito construtivo que o Capítulo apresenta um conjunto de contribuições destinadas a incorporar ao texto salvaguardas técnicas e garantias de direitos fundamentais consolidadas na comunidade técnica e na governança da Internet, entre as quais a vedação ao enfraquecimento deliberado da criptografia, a adoção de criptografia de ponta a ponta, a divulgação coordenada de vulnerabilidades, a preferência por soluções auditáveis e de código aberto e a institucionalização da participação multissetorial. Para cada contribuição, esta nota apresenta o diagnóstico do dispositivo submetido à consulta, a proposta de redação e a justificativa técnica e comparada correspondente.

A análise a seguir adota uma perspectiva técnico-jurídica e está organizada por temas, de modo a evidenciar a coerência entre as diversas ações estratégicas da E-SegInfo e as competências do SISInfo.

Para cada eixo, apresentam-se o diagnóstico do dispositivo submetido à consulta, a proposta de redação e a fundamentação técnica e comparada que a sustenta.

Esta contribuição tem natureza técnica e institucional e **não constitui parecer jurídico vinculante**. As sugestões de redação são oferecidas como subsídio ao debate público e à deliberação do órgão competente.

2. O Decreto submetido à Consulta Pública

2.1 Objeto e âmbito de aplicação

A minuta institui, simultaneamente, a E-SegInfo, instrumento de planejamento estratégico da segurança da informação, e o SISInfo, sistema que organiza, sob a forma de rede, as unidades incumbidas das atividades de governança, gestão e operação da segurança da informação (Art. 1º). Suas disposições aplicam-se aos órgãos e entidades do Poder Executivo Federal, abrangida a administração direta e a indireta, inclusive autarquias, fundações, empresas públicas e sociedades de economia mista (Art. 2º).

A adesão dos demais Poderes, do Ministério Público, dos Tribunais de Contas, das Defensorias Públicas e dos entes federativos é voluntária e realizada mediante ato próprio, preservadas as competências constitucionais e assegurada a diferenciação de tratamento em função do porte e da capacidade institucional (Arts. 3º a 5º). A adesão não implica subordinação hierárquica ao Gabinete de Segurança Institucional da Presidência da República (GSI).

2.2 Definições

O Art. 6º estabelece as definições aplicáveis, entre as quais segurança da informação, sistemas ciberfísicos e cibersegurança. A ISOC Brasil propõe, nesse rol, aperfeiçoar a definição de cibersegurança, hoje formulada como mero "subconjunto" da segurança da informação, e acrescentar uma definição autônoma de criptografia, reconhecida como salvaguarda essencial, com vedação expressa ao seu enfraquecimento deliberado, inclusive por meio de mecanismos de acesso excepcional. Ambas as contribuições são analisadas na seção 4.1.

2.3 A Estratégia (E-SegInfo): eixos e objetivos

A E-SegInfo estrutura-se em quatro eixos temáticos (Art. 7º): (i) cultura e educação; (ii) dados e informações sensíveis; (iii) governança e recursos; e (iv) cooperação nacional e internacional. Seus objetivos gerais (Art. 10) incluem assegurar a soberania nacional e a continuidade dos serviços essenciais e aprimorar a governança do ecossistema nacional de segurança da informação. A ISOC Brasil propõe

acrescentar a esse rol a observância dos direitos fundamentais, com vedação ao uso das medidas de segurança como fundamento para a vigilância massiva (analisada na seção 4.6).

As ações estratégicas de cada eixo (Arts. 12, 14, 16 e 18) detalham os controles e iniciativas a serem implementados, sendo, no eixo de dados e informações sensíveis e no eixo de governança e recursos, que se concentram as principais contribuições de natureza técnica analisadas nesta nota.

2.4 O Sistema (SISInfo): composição e competências

O SISInfo (Arts. 26 a 35) organiza as atividades de segurança da informação sob a forma de sistema, composto por órgão central (a Secretaria de Segurança da Informação e Cibernética do GSI), órgãos setoriais, seccionais, correlatos e federados, além de uma Comissão de Coordenação (Art. 27). As competências do órgão central (Art. 28) abrangem a edição de normas, a promoção da cooperação técnica mediante padrões abertos e documentados e a instituição de catálogo nacional de ferramentas de código livre.

O Art. 35 institui o sistema estruturante do SISInfo, prevendo, entre suas funções, o catálogo e o compartilhamento de ferramentas de código livre, salvaguardas para o eventual emprego de inteligência artificial e a hospedagem em infraestrutura que assegure a soberania sobre os dados tratados. O quadro a seguir sintetiza a arquitetura do Decreto.

Capítulo	Conteúdo	Artigos
I — Disposições Preliminares	Objeto, âmbito de aplicação, adesão voluntária e definições.	Arts. 1º a 6º
II — Da E-SegInfo	Disposições gerais, eixos temáticos, papéis e responsabilidades, instrumentos de planejamento.	Arts. 7º a 25
III — Do SISInfo	Disposições gerais, composição, competências, articulação com sistemas estruturadores e sistema estruturante.	Arts. 26 a 35
IV — Disposições Finais e Transitórias	Prazos, articulação com E-Ciber, Governo Digital e LGPD, alterações normativas e vigência.	Arts. 36 a 42

3. Síntese das Contribuições

As contribuições da ISOC Brasil propõem a incorporação de novos dispositivos à minuta e, em pontos específicos, o aperfeiçoamento da redação submetida à consulta. Em síntese, propõe-se:

- incluir a vedação a mecanismos de acesso excepcional (*backdoors*) e o reconhecimento da criptografia forte como controle de base, mediante a definição de criptografia (Art. 6º, III) e a ação estratégica correspondente (Art. 14, VII);
- qualificar a mensageria institucional entre agentes públicos (Art. 16, VII), exigindo padrões abertos, criptografia de ponta a ponta por padrão, código auditável e auditorias independentes;
- instituir política de divulgação coordenada de vulnerabilidades, com salvaguardas (*safe harbor*) a pesquisadores de segurança de boa-fé (Art. 14, VIII);
- incorporar referências a software livre, código aberto, auditabilidade e segurança da cadeia de suprimentos ao longo do texto (Arts. 14, 16, 28, 29, 30 e 35);
- definir o conceito de soberania sobre dados de modo a privilegiar padrões abertos, interoperabilidade e salvaguardas jurisdicionais, evitando leituras que imponham localização compulsória incompatível com a arquitetura da Internet (Art. 35, §2º; Art. 28, VIII; Art. 16, VII);
- assegurar a proteção de direitos fundamentais, em especial a vedação à vigilância massiva, e exigir supervisão humana significativa no uso de inteligência artificial (Art. 10, VI; Art. 35, §1º);
- incluir a notificação de incidentes e a minimização de metadados, em alinhamento à LGPD e às competências da ANPD (Art. 14, IX e X);
- institucionalizar a participação multissetorial e a consulta pública prévia e reforçar a transparência por meio do relatório anual (Art. 9º, par. único; Art. 19, VI; Art. 18, VI).

4. Análise e Contribuições por Tema

4.1 Criptografia forte e vedação a mecanismos de acesso excepcional

✓ Proposta de inclusão

A minuta, em seu rol de definições (Art. 6º), qualifica a cibersegurança como "subconjunto" da segurança da informação e não reconhece a criptografia como categoria normativa. A ISOC Brasil propõe substituir "subconjunto" por "domínio especializado e interdependente", prevenindo fricção com a PNCiber (Decreto nº 11.856/2023) e a E-Ciber (Decreto nº 12.573/2025), e acrescentar definição autônoma de criptografia como salvaguarda essencial, com vedação expressa ao seu enfraquecimento deliberado, inclusive por meio de mecanismos de acesso excepcional (Art. 6º, III), reproduzindo a mesma vedação entre as ações estratégicas do eixo de dados e informações sensíveis (Art. 14, VII). Há consenso técnico

de que não existe forma de inserir um mecanismo de acesso excepcional, comumente denominado *backdoor*[1].

A inclusão é coerente com a finalidade declarada da Estratégia de assegurar a soberania nacional e a proteção das infraestruturas críticas: a criptografia robusta é, simultaneamente, instrumento de proteção do cidadão, de continuidade dos serviços públicos e de defesa do próprio Estado. No direito comparado, a distinção entre os domínios de segurança da informação e de cibersegurança é reforçada pela atribuição de competências a autoridades setoriais, como em Portugal (ANACOM) e no Chile, e o reconhecimento normativo da criptografia ancora o controle de maior retorno na proteção de dados e comunicações.

Para ampliar a segurança jurídica, sugere-se reforçar a articulação entre a definição (Art. 6º, III) e a ação estratégica (Art. 14, VII), de modo a deixar inequívoco que a vedação alcança não apenas a previsão de backdoors, mas também a imposição de custódia ou compartilhamento compulsório de chaves e o enfraquecimento de algoritmos reconhecidos pela comunidade técnica.

Redação sugerida (Art. 14, VII): *"a adoção de criptografia forte e atualizada como controle de base na proteção de dados e comunicações, inclusive criptografia de ponta a ponta quando aplicável, vedada a introdução de mecanismos de acesso excepcional, a custódia ou o compartilhamento compulsório de chaves privadas e o enfraquecimento de algoritmos ou protocolos reconhecidos pela comunidade técnica internacional".*

4.2 Criptografia de ponta a ponta e mensageria institucional segura

✓ Aperfeiçoamento de redação

A minuta prevê a adoção de "plataforma nacional como mecanismo institucional seguro para mensageria entre agentes públicos" (Art. 16, VII), iniciativa positiva cujo qualificativo "seguro", contudo, carece de conteúdo normativo. Sem requisitos, há risco de plataforma sem criptografia de ponta a ponta, de solução proprietária e fechada com dependência tecnológica (lock-in) e de ausência de auditoria independente, uma plataforma mal especificada pode ser menos segura do que soluções baseadas em protocolos abertos consolidados. A ISOC Brasil propõe dar nova redação ao inciso VII, exigindo padrões e protocolos abertos e interoperáveis, criptografia de ponta a ponta por padrão, código auditável, submissão a auditorias de segurança independentes e vedação a mecanismos de acesso excepcional.

A criptografia de ponta a ponta assegura que o conteúdo das comunicações seja cifrado na origem e decifrado apenas no destino, sem que intermediários, inclusive o provedor, tenham acesso ao texto em

[1] Há consenso técnico, expresso de forma seminal no relatório "Keys Under Doormats" (Abelson, H. et al., 2015), de que mecanismos de acesso excepcional à criptografia introduzem vulnerabilidades sistêmicas exploráveis por qualquer adversário, sendo incompatíveis com a segurança das comunicações.

claro; e a exigência de código auditável e de auditorias independentes deriva do princípio de que a confiança em uma solução criptográfica resulta da possibilidade de verificação por terceiros, e não de sua opacidade. O exemplo do Tchap, mensageria do governo francês desenvolvida pela DINUM com a ANSSI, construída sobre o protocolo aberto Matrix, com criptografia de ponta a ponta, federação entre órgãos e código aberto, e de uso tornado obrigatório na administração por circular do Primeiro-Ministro em julho de 2025 — demonstra que "plataforma nacional" e "padrões abertos" não são antagônicos: foram justamente a interoperabilidade e a auditabilidade do protocolo aberto os critérios de soberania e segurança que orientaram a escolha.

Sugere-se apenas explicitar que as auditorias independentes incluam a publicação de seus resultados em formato acessível, ressalvadas as informações cuja divulgação possa comprometer a própria segurança, reforçando a transparência sem prejuízo da proteção dos sistemas.

4.3 Divulgação coordenada de vulnerabilidades e proteção a pesquisadores

✓ Proposta de inclusão

A minuta, em seu eixo de dados e informações sensíveis, não prevê política de divulgação coordenada de vulnerabilidades (CVD) nem salvaguardas a pesquisadores de segurança de boa-fé, prática reconhecida internacionalmente, nas normas ISO/IEC 29147 e 30111[2], como pilar da resiliência defensiva. A ISOC Brasil propõe instituir essa política e explicitar a proteção (*safe harbor*) aos pesquisadores que atuem de boa-fé. Sem segurança jurídica, pesquisadores tendem a não reportar falhas por receio de responsabilização, o que prolonga a exposição de sistemas públicos a vulnerabilidades conhecidas. Trata-se de modelo já consolidado, a França criou porto seguro legal para o relato de boa-fé desde 2016 (art. L.2321-4 do Código de Defesa), a Diretiva NIS2 tornou a CVD obrigatória na União Europeia, com base de dados mantida pela ENISA, Portugal previu a despenalização de pesquisadores éticos de boa-fé ao transpor a NIS2 e o Chile previu proteção equivalente em seu Marco Legal de Cibersegurança.

Redação sugerida (complemento ao Art. 14, VIII): *"... assegurada a não responsabilização administrativa, civil ou penal de pesquisadores que atuem em estrita conformidade com a política de divulgação coordenada publicada pela autoridade competente, ressalvadas as hipóteses de dolo ou de desvio manifesto do escopo autorizado".*

[2] A divulgação coordenada de vulnerabilidades é objeto das normas ISO/IEC 29147 (Vulnerability disclosure) e ISO/IEC 30111 (Vulnerability handling processes), que consolidam boas práticas internacionais para o recebimento, o tratamento e a divulgação responsável de vulnerabilidades.

4.4 Software livre, código aberto e auditabilidade

⚠ Proposta de inclusão e harmonização

O eixo de governança e recursos não contempla a segurança da cadeia de suprimentos, hoje um dos principais vetores de comprometimento de sistemas públicos (ataques via fornecedores e dependências de software). A ISOC Brasil propõe incorporar requisitos de segurança da cadeia de suprimentos[3], avaliação de fornecedores, transparência sobre os componentes de software e preferência por soluções auditáveis e de código aberto, e disseminar, ao longo do texto, o compartilhamento e a curadoria de ferramentas de código livre (Arts. 14, 16, 28, 29, 30 e 35). No plano comparado, a segurança da cadeia de suprimentos é requisito expresso da Diretiva NIS2 e do novo Regime Jurídico da Cibersegurança de Portugal (Decreto-Lei nº 125/2025). Recomenda-se, ademais, harmonizar a terminologia, que ora emprega "código aberto", ora "código livre", e esclarecer que a preferência por soluções auditáveis e de código aberto não exclui soluções proprietárias que admitam verificação independente por mecanismos equivalentes, evitando restrição indevida à concorrência.

Redação sugerida (complemento ao Art. 16, VIII): *"... incluindo a exigência de inventário de componentes de software (SBOM), a rastreabilidade de dependências e a preferência, em igualdade de condições técnicas e de segurança, por soluções auditáveis e de código aberto, sem exclusão de soluções proprietárias que admitam verificação independente por mecanismos equivalentes".*

4.5 Padrões abertos, interoperabilidade e soberania sobre dados

⚠ Aperfeiçoamento de redação

A competência de promover a interoperabilidade entre os sistemas estruturadores (Art. 28, VIII) é adequada, mas silente quanto ao meio: interoperabilidade sem padrões abertos tende a converter-se em integração proprietária e em dependência tecnológica. De igual modo, a exigência de hospedagem em infraestrutura que "assegure a soberania sobre os dados" (Art. 35, §2º) é legítima para dados sensíveis e classificados, mas o termo, lido de forma ampla como localização territorial obrigatória, pode servir de precedente a mandatos de localização no setor privado contrários à Internet aberta, impedir arquiteturas modernas e auditadas e a cooperação internacional de resposta a incidentes, e confundir armazenamento territorial com segurança efetiva.

A ISOC Brasil propõe qualificar a interoperabilidade pela preferência por padrões abertos e documentados (Art. 28, VIII) e definir a soberania sobre os dados como controle jurisdicional e técnico

[3] Sobre segurança da cadeia de suprimentos de software e inventário de componentes (SBOM), ver NIST SP 800-218 (Secure Software Development Framework) e as iniciativas da Open Source Security Foundation (OpenSSF).

sobre o seu acesso e tratamento, assegurado por um conjunto de salvaguardas técnicas, organizacionais e jurisdicionais, qualificação de provedores, gestão nacional de chaves criptográficas, controle de acesso, autonomia tecnológica e adoção de padrões abertos e auditáveis, e não pela mera territorialização do armazenamento (Art. 35, §2º). O modelo de referência é a qualificação SecNumCloud ("cloud de confiança") da ANSSI francesa, que assegura a soberania por requisitos de segurança, governança e controle jurisdicional do provedor: é o conjunto de salvaguardas, e não o lugar físico do dado, que garante a soberania, preservada a cooperação técnica internacional.

Redação sugerida (reforço ao Art. 35, §2º): *"... assegurada a soberania sobre os dados, compreendida como controle jurisdicional e técnico sobre o seu acesso e tratamento, mediante salvaguardas que privilegiem padrões abertos e interoperáveis e que não imponham fragmentação da infraestrutura comum da Internet nem obstem a cooperação internacional de resposta a incidentes".*

4.6 Direitos fundamentais, privacidade e vedação à vigilância massiva

✓ Proposta de inclusão

O rol de objetivos gerais da E-SegInfo concentra-se em capacidades de Estado (soberania, continuidade, governança) e não reproduz, no plano estratégico, o princípio de garantia de direitos fundamentais que rege a PNSI matriz (art. 3º, III, do Decreto nº 12.572/2025), uma estratégia de segurança sem objetivo expresso de proteção de direitos tende a privilegiar o controle em detrimento das liberdades. A ISOC Brasil propõe acrescentar ao Art. 10 objetivo que assegure a observância dos direitos fundamentais, em especial a privacidade, a proteção de dados pessoais e a liberdade de expressão, vedada a utilização das medidas de segurança como fundamento para a vigilância massiva, para a restrição desproporcional de direitos ou para o enfraquecimento das salvaguardas técnicas essenciais (Art. 10, VI). A vedação é formulada de modo principiológico, de forma a alcançar, além da criptografia, o anonimato legítimo, a segurança desde a concepção e os controles que impedem o tratamento desproporcional de dados.

No mesmo sentido, o emprego de inteligência artificial pelo sistema estruturante, tal como submetido à consulta, vem acompanhado de cláusula genérica ("observados os requisitos de segurança, transparência, proteção de dados pessoais e proteção de informações classificadas"), insuficiente diante do risco de desvio de finalidade, de decisões automatizadas e de perfilamento de agentes públicos. A ISOC Brasil propõe dar nova redação ao Art. 35, §1º, para impor limitação de finalidade, necessidade e proporcionalidade, vedar o uso para vigilância massiva ou perfilamento e assegurar a supervisão humana significativa nas decisões que afetem direitos, a elaboração de relatório de impacto à proteção de dados pessoais e a articulação com a ANPD, em conformidade com a LGPD e com o princípio da proporcionalidade.

Confere-se, assim, coerência vertical com a PNSI e com a Constituição (art. 5º, X, XII e LXXIX), incorporando o consenso de que segurança e direitos são complementares. Sugere-se, ademais, que a vedação à vigilância massiva do Art. 10, VI seja referenciada expressamente no Art. 35, §1º, de modo a vincular de forma inequívoca o desenho do sistema estruturante aos objetivos gerais da Estratégia.

4.7 Proteção de dados, notificação de incidentes e minimização de metadados

⚠ Proposta de inclusão e alinhamento

O eixo de resiliência e o sistema de gestão de incidentes (ReGIC) tratam da resposta interna, mas a minuta é silente quanto à notificação às autoridades competentes e, sobretudo, à comunicação às pessoas afetadas em caso de violação de dados pessoais — obrigação legal (art. 48 da LGPD) e componente de confiança pública. A ISOC Brasil propõe acrescentar ao Art. 14 a notificação tempestiva de incidentes às autoridades competentes e, havendo violação de dados pessoais, a comunicação à ANPD e aos titulares afetados (Art. 14, IX), bem como a mitigação de riscos associados à coleta, ao armazenamento e ao tratamento de metadados de comunicações, com minimização de dados e devido processo legal para o acesso a tais registros (Art. 14, X).

A inclusão dos metadados é particularmente relevante: embora frequentemente tratados como dados acessórios, os metadados de comunicação revelam padrões de comportamento, relações e localização, seu acesso descontrolado pode ser tão invasivo quanto o do próprio conteúdo, e seu tratamento desproporcional pode configurar forma de vigilância. Quanto à notificação, a prática internacional faz da tempestividade elemento central da resiliência: a NIS2 fixa prazos escalonados (alerta em 24 horas, notificação em 72 horas e relatório final em um mês) e o Chile exige o reporte de incidentes críticos em três horas ao CSIRT Nacional.

Recomenda-se alinhar a notificação de incidentes aos parâmetros já consolidados na regulação da ANPD, evitando duplicidade de obrigações, e explicitar que os relatórios de incidente devem, por padrão, utilizar dados técnicos anonimizados ou pseudonimizados. **Redação sugerida (complemento ao Art. 14, IX):** *"... observados os prazos, formatos e procedimentos definidos pela Agência Nacional de Proteção de Dados, utilizando-se, por padrão, dados técnicos anonimizados ou pseudonimizados na comunicação entre órgãos".*

4.8 Participação multissetorial, consulta pública e transparência

✓ Proposta de inclusão

A minuta determina que as edições e revisões da E-SegInfo sejam "subsidiadas" por representantes da sociedade civil, do setor acadêmico e do setor privado (Art. 9º), mas não estabelece mecanismo,

periodicidade ou transparência, a participação fica indeterminada e, na prática, facultativa, o que fragiliza a legitimidade e a qualidade técnica da Estratégia. A ISOC Brasil propõe acrescentar parágrafo único ao Art. 9º, para que as edições e revisões sejam precedidas de consulta pública e contem com mecanismo permanente de participação multissetorial, assegurada a publicidade das contribuições recebidas e a motivação quanto ao seu acolhimento ou rejeição. A previsão institucionaliza a participação que, de fato, orientou a construção da PNCiber e da E-Ciber e que caracteriza o modelo multissetorial de governança da Internet, do qual o Brasil é referência.

Em complemento, a ISOC Brasil propõe que o relatório anual de implementação da E-SegInfo seja publicado em formato acessível aos cidadãos e com indicadores objetivos de maturidade por órgão e entidade (Art. 19, VI), conferindo transparência e *accountability* à política, e que se fortaleça a participação em redes técnicas de resposta a incidentes e em organismos de padronização abertos (Art. 18, VI). Esse aporte alinha a cooperação aos canais que efetivamente operam a defesa cibernética transfronteiriça — as comunidades técnicas, as redes de resposta a incidentes (CSIRTs), o FIRST e os organismos de padronização abertos —, coerentes com as propriedades de uma Internet globalmente conectada.

Sugere-se, como reforço, que o mecanismo permanente de participação multissetorial seja consultado não apenas nas revisões da Estratégia, mas também na edição das normas técnicas mais relevantes do SISInfo que afetem a arquitetura da Internet, assegurando coerência entre o nível estratégico e o normativo.

5. Quadro Consolidado de Contribuições

O quadro a seguir consolida as contribuições, indicando o dispositivo da minuta e a proposta correspondente. As propostas de inclusão acrescentam novos dispositivos ao texto; as de aperfeiçoamento sugerem ajustes pontuais de redação.

#	Dispositivo	Contribuição / Redação sugerida
C1	Art. 6º, III	Incluir definição de criptografia como salvaguarda essencial, com vedação ao enfraquecimento deliberado e a mecanismos de acesso excepcional.
C2	Art. 14, VII	Incluir a criptografia forte e a criptografia de ponta a ponta como controle de base, estendendo a vedação à custódia ou compartilhamento compulsório de chaves e ao enfraquecimento de algoritmos reconhecidos.
C3	Art. 16, VII	Aperfeiçoar o inciso sobre mensageria institucional, exigindo padrões abertos, criptografia de ponta a ponta por padrão, código auditável e auditorias independentes, com publicação dos resultados, ressalvada a segurança.

#	Dispositivo	Contribuição / Redação sugerida
C4	Art. 14, VIII	Instituir a política de divulgação coordenada de vulnerabilidades e explicitar a salvaguarda (*safe harbor*) a pesquisadores de boa-fé, ressalvado o dolo ou desvio de escopo.
C5	Art. 16, VIII e IX	Consolidar a referência a software auditável e de código aberto, incluir o inventário de componentes (SBOM) e a segurança da cadeia de suprimentos, e esclarecer que a preferência não exclui soluções proprietárias com verificação equivalente.
C6	Arts. 28, X; 29, VI; 30, IV; 35, VI	Harmonizar a terminologia ("código livre" / "código aberto") e incluir o catálogo nacional de ferramentas, com critérios de curadoria, licenciamento, auditoria e interoperabilidade.
C7	Art. 28, III e VIII	Qualificar a cooperação técnica e a interoperabilidade entre sistemas estruturadores pela preferência por padrões abertos e documentados.
C8	Art. 35, §2º	Definir a soberania sobre dados como controle jurisdicional e técnico, com salvaguardas que privilegiem padrões abertos e não imponham fragmentação da Internet nem obstem a cooperação internacional.
C9	Art. 10, VI e Art. 35, §1º	Incluir a observância dos direitos fundamentais e a vedação à vigilância massiva; qualificar o uso de inteligência artificial com supervisão humana significativa, relatório de impacto e articulação com a ANPD.
C10	Art. 14, IX e X	Incluir a notificação de incidentes, em alinhamento à ANPD e com uso padrão de dados anonimizados ou pseudonimizados, e a minimização de metadados com devido processo legal para acesso.
C11	Art. 9º, par. único; Art. 18, VI; Art. 19, VI	Incluir a consulta pública prévia e o mecanismo permanente de participação multissetorial, a participação em organismos de padronização abertos e o relatório anual de transparência.

6. Conclusão

A minuta de Decreto que institui a E-SegInfo e o SISInfo representa um avanço qualificado na política pública de segurança da informação do País e oferece base sólida para o seu aperfeiçoamento. As contribuições reunidas nesta nota propõem incorporar ao texto salvaguardas técnicas robustas, vedação a mecanismos de acesso excepcional, criptografia de ponta a ponta, divulgação coordenada de vulnerabilidades, software auditável e de código aberto, segurança da cadeia de suprimentos, padrões abertos e soberania sobre dados, e garantias de direitos fundamentais, em linha com as melhores práticas internacionais e com o modelo multissetorial de governança da Internet.

As contribuições combinam propostas de inclusão de novos dispositivos e aperfeiçoamentos pontuais de redação, sempre acompanhados do respectivo diagnóstico e da justificativa técnica e comparada. Em especial, propõe-se inscrever a vedação inequívoca a backdoors e o reconhecimento da criptografia

forte, instituir a divulgação coordenada de vulnerabilidades com proteção a pesquisadores de boa-fé, incorporar a segurança da cadeia de suprimentos e a preferência por software auditável e de código aberto, definir a soberania sobre dados em chave compatível com a Internet global e institucionalizar os mecanismos de participação multissetorial e de transparência.

A ISOC Brasil coloca-se à disposição para colaborar com o aprofundamento técnico de qualquer dos pontos abordados e reitera seu compromisso com uma Internet aberta, globalmente conectada, segura e confiável, da qual a segurança da informação do Estado é parte indissociável.

Anexo I — Glossário de Termos Técnicos

Termo	Definição utilizada
Criptografia de ponta a ponta (E2EE)	Modelo de comunicação em que os dados são cifrados no dispositivo de origem e decifrados apenas no de destino, sem que intermediários — inclusive o provedor — tenham acesso ao conteúdo em texto claro.
Mecanismo de acesso excepcional (backdoor)	Funcionalidade que permite a terceiros contornar a proteção criptográfica de um sistema. Há consenso técnico de que não pode ser limitada a agentes autorizados, ampliando a superfície de ataque para qualquer adversário.
Divulgação coordenada de vulnerabilidades (CVD)	Processo estruturado de reporte responsável de falhas de segurança, no qual o pesquisador notifica a organização antes da divulgação pública, permitindo a correção dentro de prazos acordados.
Safe harbor (salvaguarda)	Proteção jurídica que afasta a responsabilização de pesquisadores de segurança que atuem de boa-fé e em conformidade com a política de divulgação coordenada, ressalvado o dolo ou desvio de escopo.
Software livre / código aberto	Software cujo código-fonte é disponibilizado para uso, estudo, modificação e redistribuição, permitindo auditoria independente e reduzindo a dependência de fornecedores específicos.
Inventário de componentes de software (SBOM)	Lista estruturada dos componentes e dependências que integram um software, essencial para a rastreabilidade, a gestão de vulnerabilidades e a segurança da cadeia de suprimentos.
Padrões abertos	Especificações técnicas públicas, desenvolvidas em processos abertos e implementáveis sem restrições, que asseguram a interoperabilidade entre sistemas e a longevidade das soluções.
Metadados de comunicação	Dados sobre uma comunicação (origem, destino, horário, duração, localização) que, embora não revelem o conteúdo, podem expor padrões de comportamento e relações, exigindo minimização e devido processo legal para acesso.
Minimização de dados	Princípio segundo o qual apenas os dados estritamente necessários à finalidade devem ser coletados e tratados, reduzindo riscos à privacidade e à segurança.

Termo	Definição utilizada
Sistemas ciberfísicos	Sistemas que integram componentes computacionais, redes, sensores e processos físicos, capazes de monitorar, controlar ou influenciar objetos e infraestruturas no mundo físico.
Soberania sobre dados	Controle jurisdicional e técnico sobre o acesso e o tratamento de dados, assegurado por salvaguardas técnicas, organizacionais e jurisdicionais, sem se confundir com a mera exigência de localização física.
Relatório de impacto à proteção de dados (RIPD)	Documento que descreve os tratamentos de dados pessoais que podem gerar riscos a direitos e as medidas para mitigá-los, exigido em operações de maior risco, como o emprego de inteligência artificial.

Anexo II — Quadro de Referência Normativa

Instrumento	Relação com a minuta	Observação
Decreto nº 12.572/2025 (PNSI)	Norma regulamentada	A E-SegInfo e o SISInfo concretizam a Política Nacional de Segurança da Informação; os objetivos da PNSI serão alcançados pela Estratégia (Art. 7º, §1º).
Decreto nº 12.573/2025 (E-Ciber)	Articulação suplementar	A E-SegInfo atua de forma suplementar e especializada em relação à cibersegurança (Art. 37, I).
Decreto nº 11.856/2023 (PNCiber)	Definições correlatas	As definições de cibersegurança da minuta operam sem prejuízo das constantes na Política Nacional de Cibersegurança (Art. 6º).
Decreto nº 12.069/2024 (Gov. Digital)	Articulação suplementar	A E-SegInfo atua de forma suplementar em relação ao governo digital (Art. 37, II).
Lei nº 13.709/2018 (LGPD)	Articulação e limite	Notificação de violação de dados à ANPD e aos titulares (Art. 14, IX); relatório de impacto e articulação com a ANPD no uso de IA (Art. 35, §1º); atuação suplementar (Art. 37, III).
Lei nº 12.965/2014 (Marco Civil)	Referência sistêmica	A proteção da privacidade, a liberdade de expressão e a vedação à vigilância massiva (Art. 10, VI) dialogam com os fundamentos e princípios do Marco Civil da Internet.
Decreto nº 10.748/2021 (ReGIC)	Norma alterada	A Rede Federal de Gestão de Incidentes Cibernéticos passa a constituir subsistema do SISInfo (Art. 39).

Instrumento	Relação com a minuta	Observação
Decreto nº 7.845/2012 (Inf. classificada)	Norma alterada	Institui-se o Subsistema de Segurança da Informação Classificada no âmbito do SISInfo (Art. 40).