REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

LEGISLATIVE IMPACT ASSESSMENT OF THE BRAZILIAN NATIONAL DIGITAL SECURITY AND RESILIENCE PROGRAM: A LAW AND ECONOMICS PERSPECTIVE

AVALIAÇÃO DE IMPACTO LEGISLATIVO DO PROGRAMA BRASILEIRO NACIONAL DE SEGURANÇA E RESILIÊNCIA DIGITAL: UMA PERSPECTIVA DA ANÁLISE ECONÔMICA DO DIREITO

EVALUACIÓN DE IMPACTO LEGISLATIVO DEL PROGRAMA BRASILEÑO NACIONAL DE SEGURIDAD Y RESILIENCIA DIGITAL: UNA PERSPECTIVA DEL ANÁLISIS ECONÓMICO DEL DERECHO

Marcos Cícero Santos Wanderlei
Doctoral Student in Public Administration - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)
M.Sc. in Computer Security - University of Liverpool - UK
ORCID: https://orcid.org/0009-0000-2748-3784
E-mail: cicero.sec@gmail.com

ABSTRACT

The Brazilian National Digital Security and Resilience Program, established by Bill 4,752/2025 (version approved by the Senate's Committee on Constitutional and Justice Affairs in December 2025), features a voluntary adherence architecture for subnational entities that generates structurally predictable incentive failures. Three main failures are identified: (i) free-riding on cybersecurity resilience treated as a public good; (ii) negative externalities from non-compliance that amplify systemic risks; and (iii) uncompensated positive externalities from human capital investment, leading to underinvestment in workforce development. Based on an ex ante Legislative Impact Assessment (LIA) and principles from Law and Economics, this analysis compares the enforcement mechanisms of the EU NIS2 Directive and the U.S. CISA model. It highlights lessons that can be transferred and discusses the limitations of applying these models within the Brazilian federal system. Recommendations are categorized into three levels of intervention—immediate, intermediate, and structural—with suggestions for the suitable legal instruments corresponding to each level. The study contributes to the ex ante diagnosis of incentive failures in Chapter III and to the academic debate on normative redesign compatible with Brazilian federalism.

Keywords: cybersecurity; incentive failures; public goods; legislative impact assessment; fiscal federalism; law and economics.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

RESUMO

O Programa Brasileiro Nacional de Segurança e Resiliência Digital, criado pelo PL 4.752/2025 (versão aprovada pela Comissão de Constituição e Justiça do Senado Federal em dezembro de 2025), adota uma arquitetura de adesão voluntária para entes subnacionais, o que gera falhas de incentivos estruturalmente previsíveis. A análise identifica três falhas principais: (i) o problema do *free-riding* na resiliência cibernética, tratada como um bem público; (ii) externalidades negativas da não conformidade, que ampliam os riscos sistêmicos; e (iii) externalidade positiva do capital humano não compensada, o que gera subinvestimento em capacitação. A partir de uma Avaliação de Impacto Legislativo (AIL) *ex ante* e dos preceitos da Análise Econômica do Direito (AED), comparam-se os mecanismos de *enforcement* da Diretiva NIS2 da União Europeia e do modelo CISA dos Estados Unidos, destacando-se lições transferíveis e limites de transplantação regulatória ao federalismo brasileiro. As recomendações são organizadas em três níveis de intervenção — imediato, intermediário e estrutural —, com indicação do instrumento jurídico adequado para cada proposta. O estudo contribui para o diagnóstico ex ante das falhas de incentivo do Capítulo III e para o debate acadêmico sobre um redesenho normativo compatível com o federalismo brasileiro.

Palavras-chave: cibersegurança; falhas de incentivos; bens públicos; avaliação de impacto legislativo; federalismo fiscal; análise econômica do direito.

RESUMEN

El Programa Brasileño Nacional de Seguridad y Resiliencia Digital, creado por el Proyecto de Ley 4.752/2025 (versión aprobada por la Comisión de Constitución y Justicia del Senado Federal en diciembre de 2025), adopta un régimen de adhesión voluntaria para las entidades subnacionales, lo que genera fallas de incentivos estructurales y previsibles. El análisis identifica tres fallas principales: (i) el problema del *free-riding* en la resiliencia cibernética tratada como un bien público; (ii) externalidades negativas del incumplimiento que amplían los riesgos sistémicos; y (iii) externalidades positivas del capital humano no compensadas, que generan subinversión en capacitación. A partir de una Evaluación de Impacto Legislativo (EIL) *ex ante* y de los preceptos del Análisis Económico del Derecho, se comparan los mecanismos de *enforcement* de la Directiva NIS2 y del modelo CISA, destacando lecciones transferibles y los límites de la trasplantación regulatoria al federalismo brasileño. Las recomendaciones se organizan en tres niveles de intervención — inmediato, intermedio y estructural —, con la indicación del instrumento jurídico adecuado.

Palabras clave: ciberseguridad; fallas de incentivos; bienes públicos; evaluación de impacto legislativo; federalismo fiscal; análisis económico del derecho.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

1. INTRODUCTION

Bill (Projeto de Lei - PL) No. 4,752/2025 establishes the Legal Framework for Cybersecurity and creates the Brazilian National Digital Security and Resilience Program, among other provisions. The cyber threat landscape in the Brazilian public sector underscores the urgency of the matter: in 2025, the federal public sector alone recorded 10,387 cyber incidents and 7,112 data breaches, according to CTIR Gov (BRASIL, 2025).

Methodological note on the legislative object: This analysis examines the version of PL 4,752/2025 approved by the Federal Senate's Committee on Constitutional and Justice Affairs in December 2025, with a favorable report from Senator Hamilton Mourão. It was then forwarded to the Committee on Science and Technology (CCT) for review, where it is currently awaiting a designated rapporteur, with Senator Jorge Seif assigned in February 2026. The entire document was reviewed on June 27, 2026 (BRASIL, 2025).

The audit conducted by the Federal Court of Accounts (TCU), as documented in Plenary Ruling 2,387/2024, revealed that none of the 229 organizations within the Information Technology Resources Administration System (Sisp) assessed had achieved full cybersecurity maturity. This finding substantiates the inclusion of the topic on the High-Risk List of the Federal Public Administration (TCU, 2024a). Although Sisp is primarily oriented toward the federal sphere, this outcome serves as an indirect indicator of greater severity at the subnational level, which generally has lower fiscal, technical, and institutional capacities. The report also identifies the principal risks faced by these entities.

The relevance of a preliminary assessment of economic incentives lies in the fact that cybersecurity problems stem not only from technical aspects but also from incentive structures. Anderson and Moore (2006) emphasized that security failures are, to a large extent, incentive failures. In this sense, the central thesis holds that the voluntary-participation architecture of Chapter III generates under-adherence imbalances that are structurally predictable in light of the economic theory of public goods and network externalities.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

According to Meneguin and Bugarin (2017), this scenario exemplifies the trade-off between short- and long-term efficiency: voluntariness diminishes immediate political costs during legislative approval but undermines the norm's social efficacy and the advancement of systemic cyber resilience.

This study contributes to *ex ante* analysis of the incentive failures outlined in Chapter III of Bill 4,752/2025 and proposes alternatives for normative restructuring that align with the principles of Brazilian federalism. Consequently, it enriches the academic discourse on Legislative Impact Assessment in the context of cybersecurity public policy.

2. LITERATURE REVIEW

2.1. The Economics of Cybersecurity

Cybersecurity economics, which emerged in the early 2000s, recognizes that it encompasses more than technical concerns—it also involves economic considerations, including incentives. Gordon and Loeb (2002) demonstrated that, in some models, the best level of security investment should not surpass 36.8% of the expected loss. It is essential to recognize that this finding is contingent upon their particular model and should not be regarded as a universal constraint. Instead, it indicates that when the optimal security level for society exceeds the choices individuals make independently, private underinvestment ensues.

Bauer and Van Eeten (2009) identified market failures in cybersecurity—including network externalities, information asymmetries, and collective-action problems—that lead to underinvestment. In voluntary initiatives such as the one proposed by PL 4,752/2025, information asymmetry is significant: the national authority cannot directly verify the entities' levels of compliance.

Anderson and Moore (2006) showed that in interconnected systems, individual incentives are insufficient to achieve the socially optimal level of security, because benefits generate positive externalities for third parties, while failures propagate costs across the network. This framework directly relates to substantive legistics—the concept denoting the analysis of the effectiveness and substantive quality of normative

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

instruments, beyond their formal validity—because social effectiveness depends on the quality of legislation, not merely its existence.

Meneguin (2010) states that legislative impact assessment should evaluate whether the behavior of those regulated is appropriate, whether the legislation meets its goals, and whether the benefits outweigh the costs. Meneguin and Bugarin (2017) further developed this idea by highlighting the trade-off between immediate and long-term efficiency: regulations that ease approval processes might jeopardize the development of resilient institutional capacities.

2.2. Public Goods Theory and Social Choice

Cyber resilience in interconnected infrastructures exhibits hybrid traits: it is partly non-rivalrous and not fully excludable, aligning with Buchanan's (1965) notion of a club good. The key insight comes from Bergstrom, Blume, and Varian's (1986) study, which formally shows that voluntary provision of a public good leads to a Nash equilibrium level below the socially optimal level. This issue is especially concerning in large, diverse groups—such as the roughly 5,570 Brazilian municipalities with varying fiscal capacities—where such underprovision is more problematic.

Chapter III's challenge is not just technical; it also involves combining the varied preferences of thousands of agents to build collective cyber resilience. No voluntary mechanism can meet all the criteria of collective rationality outlined by the theory, further supporting the likelihood of underprovision.

2.3. Network Externalities and the Topology of Interdependence

Shapiro and Varian (1999) describe network externalities as situations in which the value of a service depends on the number of users. In digital security, Varian (2004) formalized the problem of interdependent security (IDS): in connected systems, each participant's level of security depends on the investments of the other participants. Hirshleifer (1983) and Varian (2004) presented three aggregation topologies: *"weakest link"*, in which security is defined by the least protected agent; *"best-shot"*, by the most protected agent; and *"summation"*, by the linear sum of investments.

Brazil's federative digital infrastructure exhibits predominantly *"weakest link"* characteristics, especially in systems shared across spheres of government.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

Municipalities with access to platforms such as the Integrated Financial Administration System (SIAFI), the Electronic Information System (SEI), or the Gov.br portal can serve as vectors for incidents that affect the entire federal network, regardless of other entities' maturity levels.

It is worth noting that different federal systems operate under distinct topologies—some with *"best-shot"* characteristics—and that the "*weakest link"* classification applies, more precisely, to subsystems of centralized authentication, intergovernmental transfers, and shared databases. The absence of detailed empirical data on the topology of each specific system is acknowledged as a limitation of this analysis.

2.4. Free-Riding, Externalities, and Conceptual Distinctions

The theory of *free-riding*, set out by Olson (1965), suggests that in larger groups, the individual contribution to a common good tends to diminish. Böhme and Moore (2009) demonstrated empirically that voluntary security programs often exhibit lower-than-expected adherence, especially when compliance costs are evident and immediate while the benefits remain diffuse and long-term.

For greater analytical precision, this report distinguishes four phenomena that may coexist in Chapter III but are distinct in nature: (i) **free-riding through benefit without contribution**—the non-adhering entity benefits from the resilience generated by adherents without bearing the costs; (ii) **negative externality through risk imposition**—the non-adhering entity imposes systemic risks on the others by remaining a vulnerable vector; (iii) **moral hazard**—after adherence, the national authority has limited capacity to verify whether the declared compliance is effective, creating an incentive for formal adherence without substantive implementation; and (iv) **adverse selection**—adherence tends to attract entities that are already motivated and have greater capacity, leaving out precisely the most vulnerable ones. These roles may coexist, but they require distinct regulatory instruments to be addressed.

The positive externalities of human capital in cybersecurity are worth highlighting: when professionals are trained by one organization, they benefit the entire network through knowledge spillovers. However, the training costs are borne solely by the investing entity. Since Becker (1964), the human capital literature indicates that

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

investments in general training produce positive externalities that investors do not fully capture, resulting in widespread underinvestment.

3. METHODOLOGY AND ANALYTICAL APPROACH

This study adopts a qualitative, interpretive, and theoretically analytical approach, grounded in an interdisciplinary literature review spanning information economics, public goods theory, and law and economics. The conceptual foundation aligns with the methodological guidelines for *ex ante* Legislative Impact Assessment (LIA) and the principles of Law and Economics (L&E).

The LIA protocol detailed in this report adheres to the procedures outlined by Meneguin (2010) and Meneguin and Silva (2017):

(1) Definition of the regulatory problem: identification of the market and government failures that justify legislative intervention, focusing on the underprovision of cybersecurity in federative contexts.

(2) Objectives of the norm: contrasting the stated objectives of Chapter III with the instruments adopted.

(3) Affected groups: mapping direct addressees — including mandatory federal public administration, voluntary subnational entities, and the private sector — as well as indirectly affected groups like citizens and providers of digital public services.

(4) Regulatory alternatives: comparative analysis with international frameworks (NIS2 and CISA) to identify enforcement alternatives and assess their transferability to the Brazilian context.

(5) Exploratory cost-benefit analysis: considering the ex ante nature and the lack of comprehensive empirical data on municipal compliance, a qualitative analysis of the compliance costs associated with Article 11 is conducted, incorporating exploratory estimates of adherence scenarios.

(6) Implementation risks: identification of the incentive mechanisms that may produce effects contrary to the objectives of the norm.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

(7) Federative impacts: assessment of the fiscal and administrative heterogeneity among subnational entities and its implications for voluntary adherence.

(8) Monitoring indicators: critical analysis of the evaluation criteria set out in Art. 23, emphasizing the operationalization of the outcome subsections (III, IV, and VIII) through the definition of a baseline, numerical targets, and sectoral benchmarks.

The analytical scope of this work is limited to Chapter III of PL 4,752/2025 (Arts. 6 to 25), with complementary analysis of Art. 26 (Chapter IV), a funding provision directly linked to the Program. The remaining chapters are not covered. The assessment of regulatory incentives is conducted by contrasting them with secondary institutional evidence and data from the TCU, IBGE, and CTIR Gov. Other methodological limitations are detailed in Section 7.

4. ANALYSIS OF THE NATIONAL DIGITAL SECURITY AND RESILIENCE PROGRAM

4.1. Mapping the Normative Architecture of Chapter III

Chapter III of PL 4,752/2025 (Arts. 6 to 25) structures the Program with differentiated participation according to the nature of the entity. Art. 6 establishes the Program within the direct and indirect federal public administration. Art. 7 permits the voluntary adherence of states, the Federal District, and municipalities by means of an instrument of adherence. Art. 8 authorizes the participation of private and third-sector organizations through cooperation agreements. Arts. 13 to 15 (Section V) establish supply-chain risk governance obligations, requiring participating entities to assess suppliers, subcontractors, and technology partners. Art. 18 (Section VII) institutes the intergovernmental coordination structure through permanent councils, forums, and working groups. This differentiation of regimes is the core of the incentive problem under analysis: the mandatory requirement applies only to the federal sphere, while subnational entities—which operate systems integrated with federal networks—remain subject to an optional regime.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

Table 1 below organizes the principal provisions of Chapter III, highlighting the normative content, the addressee, the nature of the obligation, the incentives provided, the monitoring mechanisms, and the principal incentive risks identified.

Table 1 — Normative analysis of PL 4,752/2025: Chapter III (Arts. 6–25) and Art. 26 (Ch. IV)

Art.	Normative content	Addressee	Nature	Incentive provided	Monitoring	Incentive risk
Art. 6	Program established within the direct and indirect FPA	Federal public admin.	Obligation (scope of application)	—	National cybersecurity authority (Arts. 22–24)	Low: direct enforceability for the FPA
Art. 7	Voluntary adherence of states, the FD, and municipalities through an instrument of adherence	Subnational entities	Discretionary ("may adhere")	Priority access to the FNSP (Art. 16)	Instrument of adherence	High: free-riding; adverse selection
Art. 8	Participation of private and third-sector organizations	Private sector / CSOs	Discretionary (cooperation agreements, covenants, or partnerships)	Cooperation agreements	Instruments of adherence	High: private underprovision
Art. 9	Objectives of the Program (I–VIII)	All participants	Programmatic norm	—	—	No corresponding enforcement instrument
10	Operational instruments (sectoral plans, monitoring, voluntary adherence with incentives and counterparts)	All participants	Operational guideline	"Incentives and counterparts" (subsection V)	—	Low: incentives and counterparts are provided for but not specified

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

Art.	Normative content	Addressee	Nature	Incentive provided	Monitoring	Incentive risk
11	Commitments of adherents: local plans, ETIRs (own or consortium-based), training, reporting, participation in forums	Adhering to subnational entities	Obligation conditional on adherence	—	Self-reporting / Art. 12	Medium: post-adherence moral hazard; formal compliance without substantive implementation
12	Mandatory notification of relevant incidents in accordance with the criteria, deadlines, and procedures of the national authority	Adhering entities (FPA and subnational)	Obligation for adherents	—	National cybersecurity authority	Medium: adverse signaling effect; adverse selection through reputational exposure
13–15	Supply-chain risk governance: assessment of suppliers and subcontractors (Art. 13); compliance of acquired technological solutions and a national supplier maturity index (Art. 14); reporting of supply-chain-originated incidents (Art. 15)	Adhering bodies and entities	Obligation	National supplier maturity index (Art. 14, § 3)	National cybersecurity authority	Medium: expands the compliance surface; additional cost for entities with lower technical capacity
16–17	Priority access to the FNSP is conditioned on evidence of prepared plans, established teams, and adherence to	Adhering entities	Financial incentive	Priority access to the FNSP	Documentary evidence (Art. 17)	Medium: "priority" access ≠ exclusive; uncertainty as to the volume and timing of transfers

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

Art.	Normative content	Addressee	Nature	Incentive provided	Monitoring	Incentive risk
	national guidelines (Art. 17)					
18	Establishment of permanent councils, forums, and working groups at the national, regional, and local levels	All participants	Coordination structure	—	Reports of the national authority	Low: a necessary basis for intergovernmental coordination
19–21	Human capital: training, research, and innovation in cybersecurity ("shall endeavor")	Entities and the private sector	Best-efforts obligation/ guideline	—	—	High: uncompensated positive externality; attrition of professionals to the private sector
22–24	Monitoring and evaluation: 11 criteria, including outcome metrics (subsection III: mean response time; IV: reduction of incidents; VIII: resource efficiency) and process metrics (subsections I, II, V–VII, IX–XI)	All	Reporting obligation	—	Periodic reports of the national authority	Medium: outcome criteria (subsections III, IV, VIII) lack baseline data and benchmarks not defined in the bill
25	Transparency and control: annual report of revenues/expenditures, internal and external auditing, public portal,	Bodies responsible for the resources	Transparency obligation	—	Internal/external auditing; social oversight	Low: necessary accountability mechanism; effectiveness depends on the capacity of oversight bodies

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

Art.	Normative content	Addressee	Nature	Incentive provided	Monitoring	Incentive risk
	social oversight					
26*	Funding: 3% of the FNSP and 2% of fixed-odds betting revenues allocated to cybersecurity (amends Law 13,756/2018)	Public fund	Budgetary allocation (Ch. IV)	Funding base	Budget-execution reports	Uncertain: subject to actual budget execution

Source: Prepared by the authors based on PL 4,752/2025 (CCJ/SF version, Dec. 2025).

4.2. A Legistic Critique: The Voluntariness of Art. 7 as a Norm of Low Social Effectiveness

Social effectiveness is distinct from legal effectiveness: the norm in Art. 7 is valid, yet the incentives it creates are insufficient to alter behavior. The expression "may adhere" grants the subnational entity the prerogative to decide on adherence without adequate mechanisms to modify the municipal manager's opportunity cost. In complying with Art. 11. The manager forgoes actions in areas of more immediate political return, such as health, education, and infrastructure.

This legislative choice exemplifies the trade-off noted by Meneguin and Bugarin (2017): the pursuit of short-term political approval may compromise the long-term effectiveness of public policy. A norm with low social effectiveness is not neutral—it occupies space on the regulatory agenda and may create the illusion that the problem has been solved (signaling effect), which can delay deeper and more effective reforms.

4.3. The Problem of Free-Riding and Underprovision

The cyber resilience generated by adhering entities also benefits non-adherents. When a state adopts a Computer Security Incident Response Team (CSIRT), systemic risk across the entire federal network decreases, including for neighboring municipalities that do not participate. The bill has no effective exclusion mechanism: Art. 16 grants priority, though not exclusive, access to the FNSP—a

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

classic case of voluntary underprovision of public goods, as described by Bergstrom, Blume, and Varian (1986).

Information asymmetry aggravates the problem along two paths: (i) adverse selection at entry—municipalities with lower technical maturity tend to underestimate risks, while the most capable and already motivated ones adhere preferentially; and (ii) post-adherence moral hazard—the national authority has limited capacity to verify whether the declared compliance is substantive or merely formal. Data from IBGE's MUNIC 2024 indicate that only 60% of Brazil's 5,570 municipalities had an IT structure, with 54.4% having permanent IT staff and 50.4% having a Data Processing Center (IBGE, 2025).

These data must be interpreted with caution: MUNIC 2024 measures the existence of a structure, not its cybersecurity maturity. The underreporting of incidents in subnational entities—itself a reflection of the absence of monitoring structures—implies that the available data underestimate the real risk.

4.4. Externalities of Non-Compliance and Self-Reinforcing Cycles

Each entity that does not participate in the Program imposes a negative externality on those that do, thereby acting as a risk vector for lateral movement attacks. This dynamic generates a self-reinforcing cycle: participants must invest ever more to protect not only themselves but also to compensate for the vulnerabilities of non-participants, thereby raising compliance costs and reducing the appeal of adherence for others.

The TCU's High-Risk List documents the growth of incidents within Sisp, from 3,402 in 2022 to 5,302 in 2024 (TCU, 2024b). Two methodological caveats are warranted: first, Sisp covers only direct federal public administration—the data are not directly extrapolable to subnational entities, although evidence of low federal maturity constitutes an indirect indicator of a potentially more difficult situation in municipalities. Second, the growth in the figures may reflect either a real increase in incidents or an improvement in detection and notification capabilities; both explanations are consistent with the argument of systemic fragility.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

The bill lacks a specific pricing method for this negative externality. Regulatory options include mandatory cyber insurance with premiums based on compliance levels, systemic-risk levies, cross-subsidies, and liability rules for cascading damages. Anderson et al. (2013) and Romanosky (2016) offer methods for estimating the social cost of cyber incidents that could guide the development of these mechanisms.

4.5. The Human Capital Externality in Cybersecurity

Chapter III highlights, in Section VIII (Arts. 19–21), the importance of human capital, but it does not establish mechanisms to compensate for the positive *spillovers* generated by investors. When a municipality trains civil servants in cybersecurity (Art. 11, III), these professionals benefit the entire network by sharing good practices. However, the training investment falls entirely on the investing entity, which frequently loses these professionals to the private sector or to agencies with more attractive remuneration.

This dynamic reproduces Becker's (1964) classic problem of investment in general human capital: the agent who finances training does not capture all the returns. The scarcity of national data on the cybersecurity professional deficit in the public sector, turnover, and attrition to the private sector constitutes a recognized empirical gap, addressed in Section 7 as an object of future research.

The combination of *free-riding*, unpriced negative externalities, and underinvestment in human capital constitutes the triple incentive failure that undermines the Program's social effectiveness.

4.6. The Signaling Effect in Mandatory Notification

Art. 12 requires participants to inform the national authority about incidents. While this can enhance collective threat intelligence, it might also increase information asymmetry between those who comply and those who do not: only transparent entities become visible on the risk map, while non-adherents remain opaque. This may create an incentive for reputation-conscious entities to avoid adhering, configuring adverse selection.

Mandatory notification plays a vital role in threat intelligence and systemic coordination. Evidence from national and international systems shows that the lack of

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

such notifications weakens the collective response. The goal of regulation should not be to abolish notification but to shield notifiers from undue reputational damage. Ways to balance informational benefits with reduced risk include: (i) protecting reputation and anonymizing incident reports; (ii) establishing a safe harbor that shields entities from sanctions when they report voluntarily and promptly; (iii) implementing tiered disclosure rules based on incident severity; and (iv) differentiating between sanctions for negligence or intentional concealment and protection for those who report promptly.

5. COMPARATIVE ANALYSIS: INTERNATIONAL REGULATORY FRAMEWORKS

5.1. NIS2 — European Directive 2022/2555

The NIS2 Directive (EU, 2022), adopted in December 2022 with a transposition deadline for Member States of October 2024, establishes the cybersecurity regulatory framework for 18 critical sectors of the European Union. Its architecture differs substantially from the Brazilian voluntary model along five dimensions relevant to this analysis:

(i) Sectoral scope and classification criteria: NIS2 classifies entities as "essential" or "important" based on objective size criteria—more than 50 employees or turnover exceeding EUR 10 million—and sector of activity. This objectivity eliminates discretion in defining the scope, in contrast to the optional adherence to Art. 7.

(ii) Risk-management obligations: Entities must adopt technical and organizational measures proportionate to the risks, including security policies, incident management, business continuity, and supply-chain security—the functional equivalent of Art. 11, but with a mandatory character.

(iii) Notification regime with defined deadlines: Significant incidents must be notified within 24 hours (early warning), with a detailed report within 72 hours. This tiering reduces informational asymmetry without overly exposing notifiers.

(iv) Differentiated supervision: Essential entities are subject to ex ante supervision (regular audits, inspections, continuous monitoring); important entities are subject to ex post supervision triggered by evidence of non-

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

compliance. This differentiation is economically efficient, concentrating regulatory resources where systemic risk is greater.

(v) Sanctions and liability: Fines of up to EUR 10 million or 2% of annual global turnover for essential entities (EUR 7 million or 1.4% for important entities), in addition to the personal liability of senior management for compliance with security obligations (Art. 20 of the Directive). Senior management's liability increases the individual cost of non-compliance, reducing moral hazard.

NIS2 addresses free-riding by making compliance mandatory across sectors: it clearly defines who must comply and enforces sanctions with immediate, tangible consequences. This approach removes the economic incentive to free-ride, which public goods theory suggests would otherwise cause underprovision. It aligns with the condition highlighted by Bergstrom, Blume, and Varian (1986) for preventing voluntary underprovision: eliminating the option to opt out.

5.2. CISA — Cybersecurity and Infrastructure Security Agency (USA)

The U.S. model operates under two distinct regimes that must be differentiated for purposes of comparison with the Brazilian context:

For civilian federal agencies, CISA issues *Binding Operational Directives* (BODs)—binding directives with specific compliance deadlines. This dimension of the model is not directly comparable to the Brazilian subnational scenario, since it operates within a relationship of federal administrative hierarchy.

For states and local governments (*State, Local, Tribal, and Territorial*—SLTT), the central mechanism is the *State and Local Cybersecurity Grant Program* (SLCGP), administered in partnership with FEMA. This program conditions access to federal resources on the submission of a State Cybersecurity Plan and compliance with minimum criteria defined in the *Cybersecurity Performance Goals* (CPGs). The CPGs are measurable security targets—such as implementing multifactor authentication and maintaining asset inventories—that entities must progressively demonstrate.

The relevant lesson for Brazil is not adopting BODs, which serve as a tool of the federal administrative hierarchy, but rather the SLCGP model. This approach involves

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

attaching conditionalities to specific federal funding, influencing the opportunity cost of noncompliance without enforcing mandates that conflict with the Constitution. Unlike the incentive outlined in Article 16 of the bill, which provides priority access to uncertain resources, the SLCGP model associates already budgeted and anticipated resources, as identified by the subnational manager, with minimum compliance. This approach renders the cost of non-compliance immediate and tangible.

5.3. Comparative Synthesis

Table 2 — Comparative synthesis: PL 4,752/2025, NIS2, and CISA

Dimension	PL 4,752/2025 (Brazil)	NIS2 (EU)	CISA/SLCGP (USA)
Subnational scope	Voluntary (Art. 7)	Mandatory by sector and size	Conditionalities on grants (SLCGP)
Enforcement	Absence of sanctions	Fines up to 2% of turnover + management liability	BODs (federal); CPG targets + conditionalities (SLTT)
Incentive to adhere	Priority access to the FNSP (uncertain)	Legal obligation + sanction for non-compliance	Conditioned access to federal resources (SLCGP)
Externality pricing	Nonexistent	Fines + personal liability	Indirect, via conditionalities
Human capital	Voluntary training (Arts. 19–21)	Governance responsibility (Art. 20); mandatory training of teams	CPGs with workforce metrics
Measurable targets	Mixed criteria: process (subsections I, II, V–VII, IX–XI) and outcome (subsections III, IV, and VIII of Art. 23); baseline and benchmarks lacking	Technical metrics by sector + notification deadlines	CPGs with specific, measurable indicators
Supervision	Not specified in Chapter III	Ex ante (essential); ex post (important)	Periodic reports + review of the state plan

Sources: NIS2: Directive (EU) 2022/2555 (EU, 2022); CISA: CISA (2023) and SLCGP Program Guidance; bill: BRASIL (2025). Prepared by the authors.

5.4. Transferable Lessons and the Limits of Regulatory Transplantation

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

The comparative analysis reveals that NIS2 and CISA operate in institutional contexts that are substantially distinct from those in Brazil, calling for caution in transplanting instruments.

As to **transferable lessons**: (i) the SLCGP model of conditionalities on voluntary funding is institutionally compatible with Brazilian federalism, since it operates through inducement—not mandate—respecting municipal autonomy while altering the opportunity cost of non-adherence; (ii) the tiering of regulatory supervision (ex ante for critical entities, ex post for the others) under NIS2 is economically efficient and can be adapted using criteria of size and system criticality; (iii) the objectivity of the scope criteria—combining size and sector—eliminates ambiguities that reduce the cost of compliance for entities.

As to the **limits of transplantation**: (i) NIS2 operates in a context of shared European sovereignty, with digital-governance frameworks integrated among Member States that do not exist in Brazilian federalism; (ii) the SLCGP presupposes robust federal fiscal capacity and a grant system with consolidated governance, structures that differ from Brazilian intergovernmental transfers; (iii) NIS2's monetary sanctions calculated on global turnover are appropriate for the European private sector but require adaptation to the Brazilian public-sector context, where entities do not have "turnover" in the same sense; (iv) the personal liability of senior management (Art. 20 of NIS2) requires, in the Brazilian context, articulation with the legal regime governing public servants and the oversight exercised by the Courts of Accounts. Claiming that fines alone "solve" free-riding is misleading: the success of sanctions relies heavily on enforcement capacity and the strength of regulatory institutions, which vary greatly across different contexts.

6. DISCUSSION: IMPLICATIONS AND RECOMMENDATIONS

The following recommendations are arranged into three intervention levels, specifying the suitable legal instrument, the responsible authority, and the complexity of implementation. This hierarchy seeks to distinguish measures that can be implemented immediately from those requiring legislative amendments or broader structural reforms.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

6.1. Level 1: Immediate, Low-Cost Measures

These measures can be implemented in the short term, by regulation or infra-legal normative act, without altering the text of the bill:

(a) Outcome metrics in Art. 23 (instrument: regulation by the national authority): Art. 23 lists eleven evaluation criteria that combine process indicators (subsections I, II, V, VI, VII, IX, X, XI) and outcome metrics (subsection III: mean response and recovery time; subsection IV: reduction in the number and impact of incidents; subsection VIII: efficiency and impact of public resources). The problem is not the absence of outcome metrics, but the absence of baseline data, numerical targets, and sectoral benchmarks that would make these criteria operationalizable. Regulation is recommended that defines, for subsections III, IV, and VIII: (i) a standardized collection methodology and a mandatory initial reference period; (ii) annual targets differentiated by the entity's size and risk profile; and (iii) minimum performance thresholds tied to the priority access to the FNSP provided for in Art. 17, preventing managers from maximizing formal adherences without demonstrating measurable progress.

(b) Reputational protection and safe harbor for notification (instrument: normative instruction from the national authority): Regulate Art. 12, ensuring that the prompt and voluntary notification of incidents yields regulatory protection, not sanction. Include a provision for the statistical anonymization of notified data in public reports, preserving its informational value without exposing individual transparent entities.

(c) Shared threat intelligence platform (instrument: ministerial ordinance / technical-cooperation covenant): Create a channel for sharing indicators of compromise (IoCs) among adhering entities, reducing the individual cost of monitoring and increasing the return on adherence.

6.2. Level 2: Intermediate Regulatory Measures

These measures require changes to the bill itself or to complementary legislation, as well as broader inter-institutional coordination:

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

(a) Conditionalities on voluntary transfers and digital-transformation programs (instrument: decree and ministerial ordinance; body: MGI/Casa Civil): Tie access to resources from federal programs for digital transformation, administrative modernization, and data interoperability to minimum compliance with the requirements of Art. 11. Unlike constitutional transfers, such as those of the SUS—whose earmarking raises constitutional problems and may produce regressive effects in the most vulnerable municipalities—voluntary transfers and modernization covenants have no constitutionally protected earmark and represent an institutionally more appropriate vector of inducement.

(b) Subsidies differentiated by fiscal capacity (instrument: FNSP regulation; body: MJSP): Model FNSP support (Arts. 16 and 26) as a function of municipal fiscal capacity—measured by net current revenue per capita—prioritizing municipalities with less capacity to bear the costs of Art. 11. This differentiation prevents the Program from being captured by the most capable entities, which would adhere regardless of the incentive.

(c) Objective criteria for progressive mandatoriness (instrument: amendment of the bill; body: National Congress): Extend mandatoriness gradually to larger municipalities, defined by combined objective criteria: a population above 500,000 inhabitants, net current revenue above a threshold to be defined by regulation, access to critical federal systems (SIAFI, SEI, Gov.br), and personal-data processing at scale. A phased implementation schedule is proposed: (i) municipalities with more than 500,000 inhabitants, within 24 months of the law's approval; (ii) municipalities between 100,000 and 500,000 inhabitants, within 48 months; (iii) other municipalities with access to critical federal systems, within 72 months.

(d) Intermunicipal cybersecurity consortia (instrument: amendment of the bill and of consortium legislation; body: MGI and states): Regulate the possibility for municipalities to form intermunicipal consortia for the joint fulfillment of Art. 11, especially the creation of shared ETIRs. This model reduces the per capita cost of compliance for small municipalities, making adherence economically viable without compromising the technical quality of the teams.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

6.3. Level 3: High-Impact Structural Reforms

These measures involve structural changes that require broad intergovernmental coordination, adjustments to careers and legal regimes, and medium- to long-term implementation timelines:

(a) Centralized funding mechanism for human capital (instrument: FNSP Law and regulation; body: MJSP and ENAP): Create retention grants tied to a minimum period of service by the trained civil servant at the entity of origin, funded by the FNSP. Implement shared intermunicipal training platforms to minimize unit training costs. These mechanisms partially internalize the positive externality of human capital, making investment in training fiscally rational for municipalities.

(b) Liability for systemic risk (instrument: specific bill; body: AGU/CGU): Study the feasibility of a liability rule for entities that, by not adhering to the Program and not adopting minimum security standards, contribute causally to incidents with systemic impact. This reform requires detailed constitutional analysis, especially regarding federal autonomy and due process of law. As a preliminary step, it is recommended that the AGU and the TCU publish a technical study on the limits of and instruments for liability within Brazilian digital federalism.

(c) Cyber insurance with an incentive structure (instrument: resolution of a regulatory authority; body: SUSEP): Promote, in coordination with SUSEP, the development of the cyber-insurance market, with premiums differentiated according to the level of compliance. The variation in premiums serves as a mechanism for private pricing of the negative externality, creating a market incentive that complements regulatory instruments.

7. LIMITATIONS

This analysis presents limitations that must be considered in interpreting its results and recommendations:

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

(i) Ex ante nature and absence of calibrated empirical data: The parameters relating to the cost of compliance are subject to future regulations not yet published, and the estimate of subnational adherence uses theoretical models that require calibration with empirical data that are not available. The scenarios presented are indicative of structural risks, not precise quantitative forecasts.

(ii) Scope restricted to Chapter III: The analysis does not cover the remaining chapters of PL 4,752/2025, which may contain provisions affecting the incentives analyzed. A complete legislative impact assessment of the bill would require an integrated analysis of all chapters.

(iii) Data on municipal capacity: MUNIC 2024 measures the existence of IT structures, but not cybersecurity maturity. The absence of specific data on maturity, IT budgets, and incident history in subnational entities precludes the construction of quantitative adherence scenarios by municipal size.

(iv) Underreporting and measurement bias: CTIR Gov incident data reflect exclusively the records of the entities that report them, subject to detection and notification bias. The growth in the figures may indicate a real increase in attacks, an improvement in detection capabilities, or an expansion of the reporting scope—distinctions that the available data do not allow one to disentangle.

(v) Simplified comparative analysis: The comparison with NIS2 and CISA was conducted on the basis of primary documents and the available literature. A more detailed analysis of the national transposition process for NIS2 across Member States and of the SLCGP's empirical results could refine the identified lessons.

(vi) Legislative dynamism: The legislative process of PL 4,752/2025 was ongoing as of the consultation date. Subsequent changes may substantially alter the object under analysis, necessitating a revision of the conclusions.

An ex post evaluation using a causal methodology—comparing maturity and incidence indicators between adhering and non-adhering entities after

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

implementation—will be essential to verify the predictions raised here and to guide any redesign of the Program.

8. CONCLUSION

Chapter III of PL 4,752/2025 establishes the National Digital Security and Resilience Program, but its incentive architecture is inconsistent with its stated objectives. Although it seeks cyber resilience (Art. 9), it resorts to voluntary mechanisms (Arts. 7–8) for subnational entities which, according to the economic theory of public goods, tend to produce structural under-adherence. Three failures were identified: (i) free-riding in the provision of resilience as a public good; (ii) unpriced negative externalities of non-compliance; and (iii) an uncompensated positive externality of human capital. These failures are interdependent and self-reinforcing.

The voluntariness of Art. 7 favors rapid political approval—the short-term efficiency of Meneguin and Bugarin (2017)—to the detriment of long-term systemic resilience. Information asymmetry, potentially exacerbated by Art. 12, may lead to adverse selection in adherence. In systems with *"weakest link"* characteristics, such as the federal government's centralized authentication systems, the adherence of the most capable entities does not compensate for the vulnerability of the weaker ones.

The Program represents an institutional advance by filling a normative gap, establishing supply-chain risk governance (Arts. 13–15), creating an intergovernmental coordination structure through councils and forums (Art. 18), and defining funding mechanisms (Art. 26). These elements constitute a necessary yet insufficient foundation for systemic cyber resilience.

The recommendations, arranged into three intervention levels, aim to address root causes: conditionalities on voluntary transfers to change managers' opportunity costs; subsidies tailored to fiscal capacity; progressive mandatoriness based on clear criteria; and funding strategies for the human-capital externality. A primary concern is the ambiguity between legal validity and tangible social impact: the Program may be legally enforceable and operative, yet remain ineffective in mitigating systemic cyber risks.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

REFERENCES

ANDERSON, R.; BARTON, C.; BÖHME, R.; CLAYTON, R.; VAN EETEN, M.; LEVI, M.; MOORE, T.; SAVAGE, S. Measuring the Cost of Cybercrime. In: BÖHME, R. (ed.). The Economics of Information Security and Privacy. Berlin: Springer, 2013. p. 265-300. DOI: 10.1007/978-3-642-39498-0_12.

ANDERSON, R.; MOORE, T. The economics of information security. Science, v. 314, n. 5799, p. 610-613, 2006. DOI: 10.1126/science.1130992.

BAUER, J. M.; VAN EETEN, M. J. G. Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options. Telecommunications Policy, v. 33, n. 10-11, p. 706-719, 2009.

BECKER, G. S. Human Capital: A Theoretical and Empirical Analysis, with Special Reference to Education. New York: Columbia University Press, 1964.

BERGSTROM, T.; BLUME, L.; VARIAN, H. On the Private Provision of Public Goods. Journal of Public Economics, v. 29, n. 1, p. 25-49, 1986.

BÖHME, R.; MOORE, T. The Iterated Weakest Link: A Model of Adaptive Security Investment. In: WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS), 7., 2009, London. Proceedings... London: UCL, 2009. Disponível em: https://weis2009.econinfosec.org. Acesso em: 2 jun. 2026.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Estatísticas de incidentes, 2020–2025. Brasília: GSI/PR, 2025. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 22 mai. 2026.

BRASIL. Congresso Nacional. Senado Federal. Projeto de Lei nº 4.752, de 2025. Institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018. Brasília: Senado Federal, 2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/170613. Acesso em: 27 jun. 2026.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

BRASIL. Tribunal de Contas da União (TCU). Acórdão nº 2.387/2024 – Plenário. Avaliação de controles de cibersegurança nas organizações do Sisp. Processo TC 010.390/2024-3. Brasília: TCU, 2024a.

BRASIL. Tribunal de Contas da União (TCU). Lista de Alto Risco da Administração Pública Federal: 2ª edição. Brasília: TCU, 2024b. Disponível em: https://sites.tcu.gov.br/listadealtorisco/. Acesso em: 2 mai. 2026.

BUCHANAN, J. M. An Economic Theory of Clubs. Economica, v. 32, n. 125, p. 1-14, 1965.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). State and Local Cybersecurity Grant Program: Program Guidance. Washington, DC: DHS/CISA, 2023. Disponível em: https://www.cisa.gov/grants/state-and-local-cybersecurity-grant-program. Acesso em: 2 jun. 2026.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2023. Luxembourg: Publications Office of the European Union, 2023.

GORDON, L. A.; LOEB, M. P. The Economics of Information Security Investment. ACM Transactions on Information and System Security, v. 5, n. 4, p. 438-457, 2002.

HIRSHLEIFER, J. From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods. Public Choice, v. 41, n. 3, p. 371-386, 1983.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Pesquisa de Informações Básicas Municipais: MUNIC 2024. Rio de Janeiro: IBGE, 2025. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/saude/10586-pesquisa-de-informacoes-basicas-municipais.html. Acesso em: 3 jun. 2026.

MENEGUIN, F. B. Avaliação de impacto legislativo no Brasil. Brasília: Senado Federal, Consultoria Legislativa, 2010.

MENEGUIN, F. B.; BUGARIN, T. T. S. O Dilema entre a Eficiência de Curto e de Longo Prazo no Ordenamento Jurídico e o Impacto no Crescimento Econômico. Revista Direito Público, v. 13, n. 74, p. 119-145, 2017.

REMUNOM
ISSN 2178-6925

Received: 27/05/2026 - **Accepted:** 29/06/2026
Vol: 13.14
DOI: 10.66104/re2nmt33
Pages: 1-26

MENEGUIN, F. B.; SILVA, R. S. (org.). Avaliação de impacto legislativo: cenários e perspectivas para sua aplicação. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2017.

OLSON, M. The Logic of Collective Action: Public Goods and the Theory of Groups. Cambridge, MA: Harvard University Press, 1965.

ROMANOSKY, S. Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity, v. 2, n. 2, p. 121-135, 2016. DOI: 10.1093/cybsec/tyw001.

SHAPIRO, C.; VARIAN, H. R. Information Rules: A Strategic Guide to the Network Economy. Boston: Harvard Business School Press, 1999.

UNIÃO EUROPEIA (UE). Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (Diretiva NIS 2). Jornal Oficial da União Europeia, L 333, 27 dez. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2555. Acesso em: 2 jun. 2026.

VARIAN, H. System Reliability and Free Riding. In: CAMP, L. J.; LEWIS, S. (ed.). Economics of Information Security. Boston: Kluwer Academic Publishers, 2004. p. 1-15.