Prioritization Strategy for Measures in the Brazilian Security Framework

Marco Antonio Firmino de Sousa[1], **Douglas Chagas da Silva**[1], **Heder Dorneles Soares**[2]

[1]Departamento de Sistemas de Informação, Universidade Estadual do Tocantins - UNITINS
Tocantins 77020122, Brasil

[2]Instituto Federal de São Paulo – Campus Campos do Jordão
São Paulo - Brasil.

{marco.af,douglas.cs}@unitins.br, heder.dorneles@ifsp.edu.br

Abstract. *This article presents the actions of the Brazilian government to build a sustainable model to address issues of information security, data protection, and privacy. It also presents the leading agencies involved, their responsibilities, and the transversality of their actions within these themes. A national framework is presented that aims to ensure compliance and assess the maturity of the federal administration in these themes, in addition to promoting a culture in these issues and being in compliance with national and international regulations and best practices. In addition, the Analytic Hierarchy Process (AHP) method is applied to a set of controls of the Brazilian framework, seeking to obtain priority measures for these controls. The results demonstrate the importance of correct and efficient judgment necessary to define and prioritize the measures implemented by the institutions in each control.*

1. Introduction

Technological integration and the expansion of digital governance structured on the premises established by the Organization for Economic Cooperation and Development (OECD) and other international institutions with recommendations and best practices for transparent governance, combined with issues involving digital sovereignty, data protection, and information security in the context of cyber warfare, have brought numerous challenges to the Brazilian State [Mukhopadhyay and Jain 2024], [Guamán et al. 2023].

In this sense, the country initiated discussions to provide a regulatory framework to address the different problems. The discussions intensified in 2014 with the approval of Law No. 12,965 of April 23, establishing principles, guarantees, rights, and duties for internet use in Brazil. The law known as the Internet Civil Rights Framework contained several provisions for the protection of personal data and privacy, internet access, net neutrality, protection of connection records and web applications, in addition to the provision of mechanisms to ensure control of connections for auditing purposes and compliance with legal measures.

Furthermore, the publication of the aforementioned law presented aspects related to sovereignty and national security, although the refinement of the rules still needs to be determined. After this period, inspired by European legislation with the creation of the General Data Protection Regulation (GDPR), Law No. 13,709 of August 14, 2018,

known as the General Personal Data Protection Law (LGPD), was created and sanctioned. This law contains several legal provisions for processing personal data and typifies issues related to the international transfer, sharing, consent, anonymization, use, and deletion of personal data. In addition, it regulates minimum security requirements, accountability, and legal obligations related to data processing [Sullivan 2019].

At a global level, the debate on protecting personal data began in Europe, with the Strasbourg Convention as its landmark in 1981. From then on, concerns about the processing of personal data began to be discussed and expressed, leading to the creation of several documents on the subject. However, in 2009, with the Treaty of Lisbon, the right to protect personal data was consolidated as a fundamental right in the European Union. Over the years, new changes and updates have occurred related to protecting personal data in Europe, focusing on the rights of citizens by the private sector and local governments. [Buckley et al. 2024], [Greenleaf 2023].

The discussion on data protection in the United States differs from Europe, starting with the name, which refers to data privacy and not data protection, as in the European Union. It is worth noting that there is no general law for data protection; Instead, separate regulations seek to protect citizens by treating them as consumers. It is important to note that no national agency or authority is responsible for data privacy, and the courts or the Federal Trade Commission (FTC) deal with these issues. [Sullivan 2019], [Tao et al. 2019].

This article presents quantitative research based on applying a multi-criteria decision-making method and public documents made available by the Brazilian government. It also seeks to draw on essential references and best practices, including good data protection and privacy practices, such as OECD principles, ISO/IEC 27701, GDPR, LGPD, ISO/IEC 29100, and other international regulations. Finally, it evaluates a set of measures proposed in three controls proposed in the Brazilian framework [Éllen Renner Ferrão et al. 2023].

Finally, the research question presented is: **How has Brazil compiled controls and best practices to assess and improve the maturity of its agencies in privacy, personal data protection, and information security?**

The Analytic Hierarchy Process (AHP) method was applied in a Brazilian framework based on different tools and regulatory models to answer this research question. The objective is to assist entities in prioritizing the measures to be adopted based on a widely used mathematical model [Guidi et al. 2024], [Guamán et al. 2023].

2. Digital Governance and Sustainable Development

The OECD highlights the importance of ethical and transparent management in its guidelines on the corporate governance of state-owned companies [Ayala-Rivera et al. 2024]. In this sense, Brazil has sought to advance in the face of these challenges. Institutions such as the Office of the Comptroller General of the Union (CGU) and the Court of Auditors of the Union (TCU) assist in this role, especially in preparing recommendations and documents and monitoring governance and compliance policies [Peixoto et al. 2023],[Belli et al. 2023].

In addition, the regulatory framework discussed in the section 2.1 complements

the responsibilities of the bodies that make up the federal public administration. In addition to administrative reforms to improve governance and compliance according to OECD criteria, the Ministry of Management and Innovation (MGI) is one of these initiatives. It proposed several advances and good governance practices by applying different tools, models, and frameworks in federal public administration.

2.1. Regulatory and Institutional Framework

Brazil has been working to structure a robust regulatory and institutional agenda to address the challenges of data protection, privacy, and information security. We highlight the efforts coordinated by the National Data Protection Authority (ANPD), the Institutional Security Office (GSI), the National Information Security Policy (PNSI), and the LGPD. Each institution has specific responsibilities to ensure the correct application of the regulatory agenda in inspecting, monitoring, and developing proposals and projects on these topics [Belli et al. 2023], [Peixoto et al. 2023].

The ANPD regulates the LGPD, defines minimum requirements for protecting personal data, and instructs sanctioning processes to investigate conduct and responsibilities regarding data subjects' rights. In addition, it promotes the development of a culture of protection and privacy that is aligned with international standards. Concerning information security, the GSI manages the PNSI and monitors the projects, teams, actions, and solutions developed by the Ministry of Management and Innovation (MGI).

It is worth noting that the PNSI was established in 2018 to ensure the integrity, availability, confidentiality, and authenticity of information nationally. The policy makes developing and implementing the Information Security Policy (POSIN) mandatory in all federal administration bodies. It is also mandatory to create an Information Security Management Committee (CGSI) that supervises and monitors the application of the POSIN and establishes the bodies' capacities to face problems and incidents related to data security and protection.

2.2. PPSI

The Information Privacy and Security Program (PPSI) consists of controls that aim to improve, evaluate, and verify federal public administration bodies' adequacy in maturity and resilience in data security and privacy.

The Brazilian government's Digital Government Secretariat of the MGI maintains the framework. The program presents a methodological structure that defines and maintains privacy and information security controls. The controls are organized into thematic areas encompassing the participating bodies' governance, maturity, technology, people, and critical information systems. The controls are generally arranged based on recommendations from frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO/IEC 29100, ISO/IEC 27701, and the LGPD itself [Éllen Renner Ferrão et al. 2023],[Mukhopadhyay and Jain 2024], [Thomas et al. 2022].

In Brazil, the framework is adopted by an ordinance expressly providing for what is provided in art. 8th of Ordinance SGD/MGI No. 852, of March 28, 2023, defines the objectives, mandatory controls, procedures, good practices, and models related to the topic. The MGI structure also includes the Integrated Cybersecurity Center for Digital Government (CISC) and the Center of Excellence in Privacy and Information Security

(CEPS), both of which are operational units responsible for coordinating teams for the prevention, treatment, and response to cyber incidents and promoting a culture of privacy and information security in agencies and entities.

This article explicitly considers privacy and data protection controls, namely controls 21, 25, and 27. The measurements for each of the controls are provided below. The choice was motivated by issues inherent to national sovereignty and the federal government's data governance policy, inspired by documents by international institutions such as the UN, World Bank, and OECD.

Control 21 - Governance Measures

- 21.1: Does the agency adopt measures to adapt its processes and activities related to the processing of personal data to current privacy and data protection laws/regulations?
- 21.2: Has the agency prepared and disclosed its Institutional Data Privacy Program, established in Art. 50 of the LGPD?
- 21.3: Are the roles and responsibilities of employees involved in processing personal data established and communicated?
- 21.4: Does the agency provide the person in charge with the resources necessary to implement the LGPD and direct access to senior management?
- 21.5: Does the agency determine the responsibilities and respective roles for processing personal data with the joint controller(s) involved?
- 21.6: Does the agency disclose the policies and operational procedures for protecting personal data to its internal and external employees?
- 21.7: Are the legal, regulatory, and contractual requirements related to privacy understood and addressed through good practice and governance rules published by the institution?
- 21.8: Is a defined organizational risk tolerance clearly expressed and communicated to the agency's stakeholders within the scope of personal data processing operations?
- 21.9: Have indicators been defined to measure the agency's results and performance in implementing the Institutional Data Privacy Program?
- 21.10: Has the agency established a team that monitors the technical vulnerabilities of services that process personal data?

Control 25 - Data Management

- 25.1: Does the agency configure systems to record the date personal data is collected, created, updated, deleted, or archived?
- 25.2: Does the agency limit the amount of processing of personal data in its custody?
- 25.3: Does the agency define and document the objectives of minimizing the processing of personal data in its custody?
- 25.4: Are the data kept in an interoperable and structured format for shared use, to implement public policies, provide public services, decentralize public activity, and disseminate and provide access to information by the general public?
- 25.5: Are there procedures to ensure that when the agency processes the data subject's data, it follows the hypotheses in article 15 of the LGPD?
- 25.6: Does the institution use appropriate techniques or methods to ensure the secure deletion or destruction of personal data (including originals, copies, and archived records) to prevent their recovery?

- 25.7: Does the organization assess whether personal data is retained (stored) for the time strictly necessary to fulfill the purposes of personal data processing that have been identified?
- 25.8: Does the organization implement in the service the detection of the expiration of the retention period and automatic notification that the possibility of deleting personal data must be evaluated after the purposes have been fulfilled?
- 25.9: Does the organization block and adopt protective measures to exempt personal data from further processing when the purposes informed to the data subject are achieved, but retention is required by applicable laws?

Control 27 - Data Sharing and Transfer

- 27.1: Does the agency identify the sharing of personal data carried out with third-party operators and other institutions by Articles 26 and 27 of the LGPD, including which personal data were disclosed, to whom, at what time, and for what purpose?
- 27.2: Does the agency identify the international transfers of personal data carried out by Chapter V of the LGPD, including which personal data were disclosed, to whom, at what time, and for what purpose?
- 27.3: Does the agency adopt a formalization and registration process when sharing personal data, identifying the object and purpose, legal basis, and duration of the processing?
- 27.4: Does the agency request a formal description of the personal data protection measures adopted by the entities with whom it shares personal data?
- 27.5: Does the agency comply with the provisions of Articles 33-36 of the LGPD regarding international transfers of personal data?

3. Application of the AHP Method

The AHP method was applied to analyze and evaluate the measures mentioned in section 1. The method uses hierarchical levels to solve the problem: in its simplest version, the main objective of the problem is at the top of the hierarchy; at the level immediately below, the criteria used to achieve the main objective are listed; and at the lowest level, the viable alternatives to be evaluated are listed [Guidi et al. 2024].

The method uses the fundamental scale to express the relative importance (degree of preference) between the control measures considered, as shown in Table 1. Considering the judgments provided by the decision-making unit and some basic operations implemented by the method, the alternative that presents the most significant weight, after considering the priority of each measure, is chosen as the best. It is also possible to verify whether the judgments made present logical consistency. The method can generally be summarized in the following steps illustrated in Figure 1 [Guidi et al. 2024].

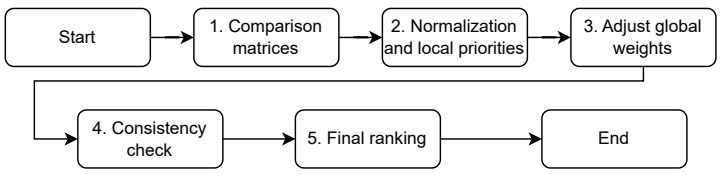

Figure 1. AHP Workflow

Table 1. Saaty Fundamental Scale

Intensity of Importance	Verbal Definition
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2, 4, 6, 8	Intermediate values between the importances

Table 2. Pair-wise comparison matrix for Control 21

	21.1	21.2	21.3	21.4	21.5	21.6	21.7	21.8	21.9	21.10
21.1	1	3	5	7	5	3	5	3	5	7
21.2	1/3	1	3	5	3	2	3	2	3	5
21.3	1/5	1/3	1	3	2	3	2	3	3	5
21.4	1/7	1/5	1/3	1	1/3	3	1	2	2	3
21.5	1/5	1/3	1/2	3	1	5	3	5	5	7
21.6	1/3	1/2	1/2	1	1/3	1	1	3	3	5
21.7	1/5	1/3	1/2	3	1/2	3	1	2	3	5
21.8	1/7	1/5	1/3	1/2	1/5	2	1/3	1	1	2
21.9	1/5	1/3	1/2	2	1/2	3	1	1	1	2
21.10	1/7	1/5	1/3	1/2	1/3	2	1/2	1/2	1	1

Experts in the PPSI framework determined the total weights assigned to each control through consultation with the MGI. In addition, the measures' relevance in the overall context of the problem is considered. **Control 21: 0.34, Control 25: 0.19, and Control 27: 0.47.**

3.1. Operations Details

The comparison matrix for each PPSI control group considered Saaty's importance scale. Tables 2, 3, and 4 indicate the relative preference of importance between the measures for each control.

After comparing the measures, we normalized the data. Next, we calculate the local priorities (PMLs). Table 5 summarizes the evaluation results for each of the controls

Table 3. Pair-wise comparison matrix for Control 25

	25.1	25.2	25.3	25.4	25.5	25.6	25.7	25.8	25.9
25.1	1	3	5	7	5	7	3	5	7
25.2	1/3	1	3	5	3	5	2	3	5
25.3	1/5	1/3	1	3	2	3	2	3	3
25.4	1/7	1/5	1/3	1	1/3	3	1	2	2
25.5	1/5	1/3	1/2	3	1	5	3	5	5
25.6	1/7	1/5	1/3	1/3	1/5	1	1/3	1/2	1
25.7	1/3	1/2	1/2	1	1/3	3	1	3	2
25.8	1/5	1/3	1/3	1/2	1/5	2	1/3	1	2
25.9	1/7	1/5	1/3	1/2	1/5	1	1/2	1/2	1

Table 4. Pair-wise comparison matrix for Control 27

	27.1	27.2	27.3	27.4	27.5
27.1	1	3	5	7	5
27.2	1/3	1	3	5	3
27.3	1/5	1/3	1	3	3
27.4	1/7	1/5	1/3	1	1/3
27.5	1/5	1/3	1/3	3	1

assessed. It presents the PMLs, the global weights, and the global priorities calculated for all measures.

Table 5. Consolidation of Global Priorities

Measure	PML	Global Weight	Global Priority
21.1	0.15	0.34	0.0510
21.2	0.12	0.34	0.0408
21.3	0.10	0.34	0.0340
21.4	0.08	0.34	0.0272
21.5	0.11	0.34	0.0374
21.6	0.09	0.34	0.0306
21.7	0.10	0.34	0.0340
21.8	0.07	0.34	0.0238
21.9	0.12	0.34	0.0408
21.10	0.10	0.34	0.0340
25.1	0.33	0.19	0.0627
25.2	0.18	0.19	0.0342
25.3	0.11	0.19	0.0209
25.4	0.06	0.19	0.0114
25.5	0.13	0.19	0.0247
25.6	0.03	0.19	0.0057
25.7	0.08	0.19	0.0152
25.8	0.05	0.19	0.0095
25.9	0.03	0.19	0.0057
27.1	0.49	0.47	0.2303
27.2	0.24	0.47	0.1128
27.3	0.14	0.47	0.0658
27.4	0.05	0.47	0.0235
27.5	0.09	0.47	0.0423

3.2. Consistency Verification

The AHP requires consistency in pairwise comparisons to ensure the reliability of priorities. Consistency is verified by calculating each control's Consistency Index (CI) and Consistency Ratio (CR). The steps for the calculation are detailed below:

3.2.1. Governance

Step 1: Multiply the original matrix by the priority vector (PML).

The result is the weighted sum vector for each measure. The Table 6 shows the calculated weighted sums, priorities (PML), and their quotients:

Table 6. Calculation of λ_{max} for Control 21

Measure	Weighted Sum	PML	Quotient
21.1	1.51	0.15	10.07
21.2	1.22	0.12	10.17
21.3	1.03	0.10	10.30
21.4	0.84	0.08	10.50
21.5	1.17	0.11	10.64
21.6	0.93	0.09	10.33
21.7	1.03	0.10	10.30
21.8	0.74	0.07	10.57
21.9	1.22	0.12	10.17
21.10	1.03	0.10	10.30

Step 2: Calculate λ_{max}.

$$\lambda_{\text{max}} = \frac{\sum(\text{Quotient})}{n} \tag{1}$$

$$\lambda_{\text{max}} = \frac{\sum_{i=1}^{10} x_i}{10} = 10.34, \tag{2}$$

$$\text{where } x_i = \begin{bmatrix} 10.07 & 10.17 & 10.30 & 10.50 & 10.64 \\ 10.33 & 10.30 & 10.57 & 10.17 & 10.30 \end{bmatrix} \tag{3}$$

Step 3: Calculate the Consistency Index (CI).

$$CI = \frac{\lambda_{\text{max}} - n}{n - 1} \tag{4}$$

$$CI = \frac{10.34 - 10}{10 - 1} = \frac{0.34}{9} \approx 0.038 \tag{5}$$

Step 4: Calculate the Consistency Ratio (CR).

$$CR = \frac{CI}{RI} \tag{6}$$

$$CR = \frac{0.038}{1.49} \approx 0.025 \tag{7}$$

Conclusion: Since $CR < 0.1$, the matrix is consistent.

3.2.2. Data Management

The same process is applied to Control 25. The results are summarized below:

$\lambda_{\text{max}} = 9.68$

$$CI = \frac{\lambda_{\text{max}} - n}{n-1} = \frac{9.68 - 9}{9-1} = 0.085 \tag{8}$$

$$CR = \frac{CI}{RI} = \frac{0.085}{1.45} \approx 0.059 \tag{9}$$

Conclusion: The matrix for Control 25 is consistent since $CR < 0.1$.

3.2.3. Data Sharing and Transfer

For Control 27, the calculated values are as follows:

$\lambda_{\text{max}} = 5.28$

$$CI = \frac{\lambda_{\text{max}} - n}{n-1} = \frac{5.28 - 5}{5-1} = 0.071 \tag{10}$$

$$CR = \frac{CI}{RI} = \frac{0.071}{1.12} \approx 0.064 \tag{11}$$

Conclusion: The matrix for Control 27 is consistent since $CR < 0.1$.

All matrices (Control 21, Control 25, and Control 27) are consistent, with $CR < 0.1$ for each.

4. Results and Discussion

This section presents the AHP method's results for controls 21, 25, and 27 of the PPSI. The objective was to obtain the prioritization of the measures to be implemented by the agencies. We considered the weights defined by an expert and the recommendations suggested by the PNSI and the LGPD.

Figure 5 presents the ranking of the priority measures for Control 21. The method's results link the need for the agency to adapt to the processes and activities related to the processing of personal data by the regulatory framework in force in Brazil. In addition, it demonstrates the need to develop and disseminate the institutional data privacy program, which denotes the concern with strengthening the culture of data security and privacy.

Next, it shows the need to define the Key Performance Indicator (KPIs) to evaluate the performance of implementing the institutional internal privacy program. These are the three main measures for this control (21.1, 21.2, and 21.9). The other measures follow the ranking and can be seen in the description presented in

For Control 25, illustrated in Figure 3, we observe that the method output focuses on how the PPSI framework addresses how personal data is collected, created, updated, deleted, or archived. This highlights the concern with data governance and compliance with the LGPD. Thus, aspects such as limiting the amount of data processing held by the

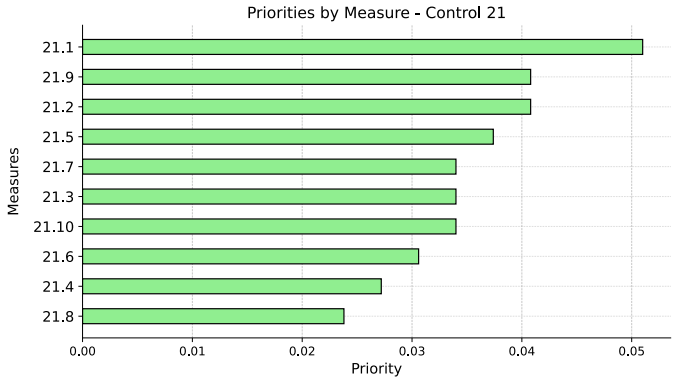

Figure 2. Priorities by Measure - Control 21

agency and issues related to the legal hypotheses for treating such data must be considered. The final ranking considers the other measures according to the priorities obtained by the method.

Regarding Control 27, the measure related to sharing personal data with third parties and other institutions is strongly prioritized. This reveals the understanding of the purposes and hypotheses of treatment, in addition to geopolitical issues related to national data sovereignty. Thus, we verify the framework's concern with aspects related to international data transfers and other data-sharing measures. The completed ranking is presented in Figure 4.

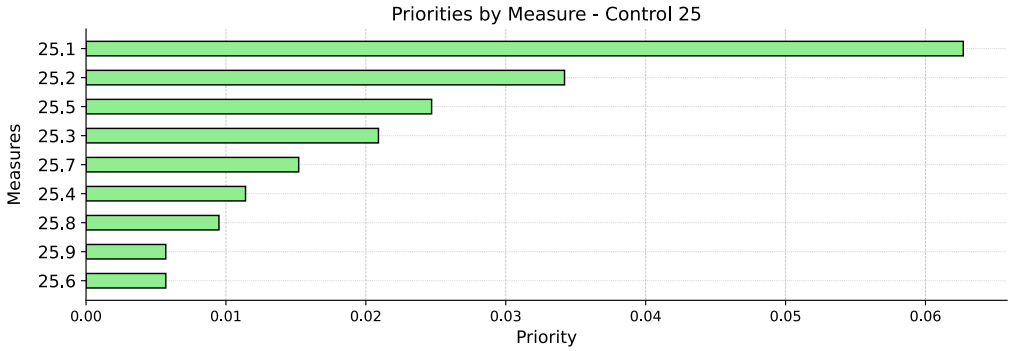

Figure 3. Priorities by Measure – Control 25

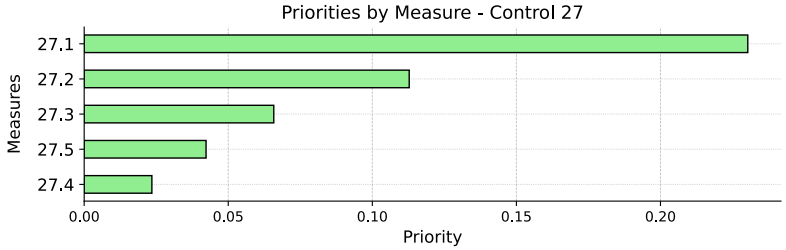

Figure 4. Priorities by Measure – Control 27

Finally, Figure 5 presents the global priorities for the three controls evaluated. We can observe that, with a substantial difference from the other measures, the first mea-

sure of Control 27, related to identifying the sharing of personal data with third parties, followed by issues related to the international transfer of data, is measured with higher priorities. This denotes the geopolitical concerns related to the topic worldwide, especially in countries of different economic blocs, such as BRICS and the European Union. This analysis is not part of the scope of this paper but can be evaluated in [Tao et al. 2019].

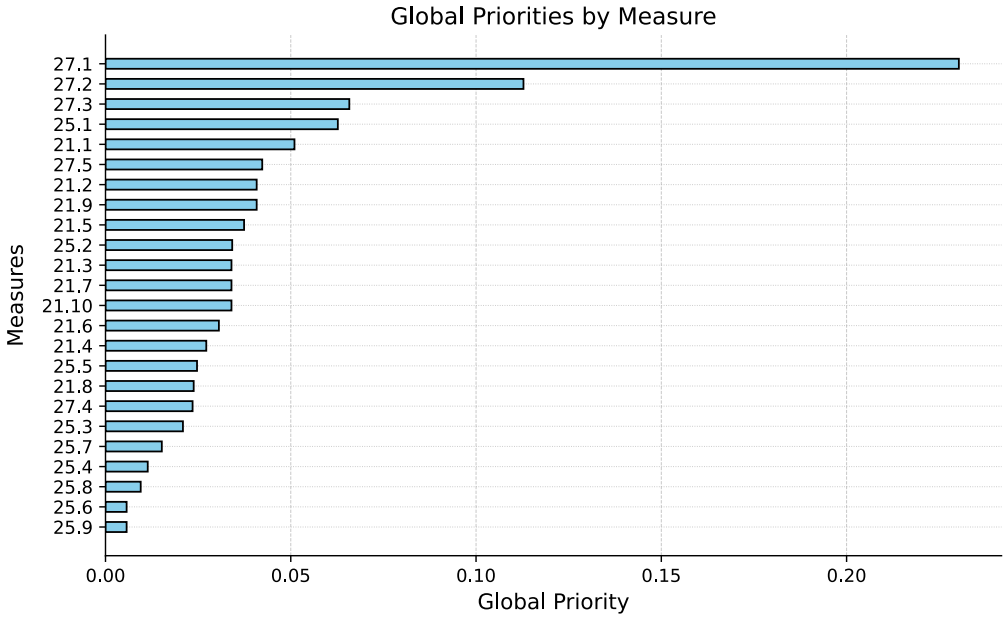

Figure 5. Global Priorities by Measure

In addition, we can observe that the order of the questions to evaluate the maturity of the agencies in the different themes was natively designed in the framework, demonstrating an interest in "Privacy-by-design". Information on this type of methodology can be obtained in [Ayala-Rivera et al. 2024].

5. Conclusion

This paper provides an overview of how Brazil has structured its information security, data protection, and privacy regulatory agenda. We present the leading institutions involved in this process and their responsibilities and actions in the different areas. The role of ANPD, GSI, and MGI in the government structure is highlighted.

In addition, the PPSI framework, a Brazilian initiative to assess the maturity and resilience of federal public administration bodies, was presented. The framework aims to promote a national privacy and data security culture and ensure the administration complies with the regulatory framework.

Next, we applied the AHP method to the measures defined by three crucial PPSI controls, aiming to identify the priority measures and assist in their implementation. The AHP method proved to be quite flexible in solving the problem, an inherent characteristic that makes it one of the most widely used multicriteria decision-making methods in academia and the market. The method's results highlighted aspects of international data transfer and sharing as critical issues to be addressed, demonstrating the topic's importance today from a political and national sovereignty perspective.

Finally, we verified the topic's importance for different countries and economic blocs. Studying the topic involves analyzing geopolitical and social issues, among other things. Due to the number of variables inherent to the topic, this transversality makes it complex. Thus, it verifies the need for new studies and a deeper understanding of the topics.

References

Ayala-Rivera, V., Portillo-Dominguez, A. O., and Pasquale, L. (2024). Gdpr compliance via software evolution: Weaving security controls in software design. *Journal of Systems and Software*, 216.

Belli, L., Curzi, Y., and Gaspar, W. B. (2023). Ai regulation in brazil: Advancements, flows, and need to learn from the data protection experience. *Computer Law and Security Review*, 48.

Buckley, G., Caulfield, T., and Becker, I. (2024). How might the gdpr evolve? a question of politics, pace and punishment. *Computer Law and Security Review*, 54.

Greenleaf, G. (2023). Global data privacy laws 2023: 162 national laws and 20 bills. *SSRN Electronic Journal*.

Guamán, D. S., Rodriguez, D., del Alamo, J. M., and Such, J. (2023). Automated gdpr compliance assessment for cross-border personal data transfers in android applications. *Computers and Security*, 130.

Guidi, G., Goffo, G., and Violante, A. C. (2024). Application of the analytic hierarchy process (ahp) method to identify the most suitable approach for managing irradiated graphite. *Nuclear Engineering and Technology*.

Mukhopadhyay, A. and Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, 74.

Peixoto, M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., and Gorschek, T. (2023). The perspective of brazilian software developers on data privacy. *Journal of Systems and Software*, 195.

Sullivan, C. (2019). Eu gdpr or apec cbpr? a comparative analysis of the approach of the eu and apec to cross border data transfers and protection of personal data in the iot era. *Computer Law and Security Review*, 35:380–397.

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., and Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, 98:660–671.

Thomas, L., Gondal, I., Oseni, T., and Firmin, S. S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers and Security*, 116.

Éllen Renner Ferrão, S., Silva, G. R. S., Canedo, E. D., and Mendes, F. F. (2023). Supplementary material for towards a taxonomy of privacy requirements based on the lgpd and iso/iec 29100.