Structuring Privacy and Information Security Competencies for Public Sector Roles: A Framework for Enhancing Software Quality and LGPD Compliance

Stefano Luppi Spósito
University of Brasília (UnB),
Department of Computer Science
Brasília–DF, Brazil
stefanoluppi@hotmail.com

Kassio Alves
University of Brasília (UnB),
Department of Computer Science
Brasília–DF, Brazil
okassioalves@gmail.com

Rafael Rabelo Nunes
University of Brasília (UnB)
Brasília–DF, Brazil
rafaelrabelo@unb.br

Leonardo Rodrigo Ferreira
Ministry of Management and
Innovation in Public Services
Brasília–DF, Brazil
leonardo.r.ferreira@gestao.gov.br

Edna Dias Canedo
University of Brasília (UnB),
Department of Computer Science
Brasília–DF, Brazil
ednacanedo@unb.br

ABSTRACT

Context: The increasing complexity of digital public services has heightened the need for robust governance mechanisms in privacy and information security, particularly in light of Brazil's General Data Protection Law (LGPD). However, public institutions often lack clearly defined roles, responsibilities, and competencies for professionals managing sensitive data and system security. **Objective:** This study aims to develop a comprehensive competency framework that maps the responsibilities and required knowledge, skills, and abilities (KSAs) for key privacy and information security roles in the Brazilian federal public administration. **Method:** We employed a design science approach, grounded in national regulations (LGPD, PPSI, IN GSI/PR nº 3/2021) and international standards (e.g., ISO/IEC 27701), to analyze legal and normative documents. The process included the identification of 24 institutional roles (8 in privacy, 16 in information security), the modeling of KSAs across three proficiency levels, and the use of the Analytic Hierarchy Process (AHP) to prioritize competencies. **Results:** The resulting framework provides structured competency profiles for each role, supporting training journey design, maturity assessment, and decision-making for role allocation. An interactive online platform makes the full model publicly accessible, offering practical tools for public sector adoption. Key findings highlight overlapping areas between privacy and security domains, reinforcing the need for coordinated institutional efforts. **Conclusion:** By clarifying role expectations and aligning them with legal and technical requirements, the framework supports public organizations in improving their institutional maturity in privacy and security governance. It also contributes to the quality, reliability, and trustworthiness of digital public services through strategic capacity-building.

KEYWORDS

Information Security, Privacy, Competency Framework, Public Sector, LGPD, Software Quality, Training, Governance

1 Introduction

In an era where digital services are central to the delivery of public value, ensuring the quality of software systems used in government has become increasingly dependent on how well those systems manage and protect personal data [3, 16]. The Brazilian General Data Protection Law (LGPD – Law No. 13.709/2018)[2] establishes a legal framework that requires public institutions to implement comprehensive governance mechanisms for the protection of personal data. Although legal compliance is the minimum requirement, effective data protection depends on more than just legal interpretation or technical controls: it requires a competency-based approach to privacy management centered on humans [7, 8, 18].

One of the main challenges facing public institutions is the lack of clearly defined `roles, skills, and responsibilities` related to information security, privacy and data protection [19]. Without a shared understanding of what different stakeholders must know and be able to do, efforts to implement Privacy by Design (PbD), meet software quality standards, or align with international data protection norms such as GDPR [22] or ISO/IEC 27701 [5] may fall short. This lack of clarity affects not only compliance, but also the reliability, maintainability, and security of the systems themselves.

This challenge extends beyond privacy. Public organizations are also required to ensure the protection of institutional information assets, in accordance with national standards for Information Security [21]. In Brazil, Normative Instruction GSI/PR nº 3/2021 [13] establishes a mandatory structure for Information Security governance, including specific roles and responsibilities for risk management, incident response, business continuity, and compliance. As with privacy, the successful implementation of these practices relies heavily on the competencies of the professionals assigned to each role, yet there is limited guidance available on how to structure these competencies or evaluate institutional readiness.

To address this broader issue, a national research project was initiated by the University of Brasília (UnB), in partnership with the Brazilian Ministry of Management and Innovation in Public Services. The initiative aimed to design a structured Privacy and Information Security Competency Framework tailored to the context of the Brazilian federal public sector. Based on legal, normative, and technical documents—including the LGPD [2], guidance from the National Data Protection Authority (ANPD), and the Privacy and Security Program (PPSI)[15]—the research team identified **eight key professional profiles** involved in the treatment of personal data and **sixteen profiles** related to Information Security governance in public organizations.

Each of these profiles was analyzed to map their required competencies across multiple levels of expertise, ranging from basic understanding of privacy and security principles to advanced skills in governance, compliance, and technical implementation. The resulting framework defines these competencies using a structured taxonomy of Knowledge, Skills, and Abilities (KSAs), linking them to the practical responsibilities each role performs. The framework also supports the implementation of training journeys, organizational alignment, and improved collaboration among multidisciplinary teams.

By articulating these competencies in a clear and operational way, this work contributes to the advancement of software quality in public systems—not only through better legal compliance, but through a deeper integration of privacy and security principles into system design, risk management, and decision-making. In doing so, it promotes a systemic view of both privacy and information security as sociotechnical issues, embedded in organizational culture, governance processes, and software lifecycle practices.

This paper presents the development process of the Privacy and Information Security Competency Framework, its structure, and examples of application. We discuss how the framework can support public institutions in achieving higher maturity in governance practices and how it aligns with core attributes of software quality, such as security, privacy, usability, dependability, and transparency.

The remainder of this article is organized as follows. Section 2 presents the background and related work, highlighting existing frameworks, regulatory guidelines, and academic contributions in the areas of privacy and information security competencies. Section 3 details the methodology employed to construct the proposed competency frameworks, including the document analysis, role modeling, definition of knowledge, skills, and abilities (KSAs), and expert validation procedures. Section 4 reports the results of the framework development, including the roles, responsibilities, and competency distributions for privacy and information security domains, as well as the interaction analysis between roles. Section 5 discusses practical implications, recommendations for implementation, training strategies, and maturity indicators for institutional adoption. Section 6 addresses the main threats to the validity of the study and the measures adopted to mitigate them. Finally, Section 7 summarizes the key findings, reinforces the practical contributions of the proposed framework for public sector governance, and outlines promising directions for future research and implementation.

2 Background and Related Work

Privacy and data protection have become important concerns in software quality, particularly in industry and public sector systems that manage large volumes of personal data [16]. International frameworks such as the General Data Protection Regulation (GDPR) [22] and the ISO/IEC 27701 [5] have set benchmarks for privacy governance, including the definition of roles, responsibilities, and competencies across organizations. In Brazil, the General Data Protection Law (LGPD) plays a similar role, emphasizing principles such as purpose limitation, data minimization, transparency, and accountability [17].

Despite the regulatory clarity provided by the LGPD, public institutions in Brazil have faced significant challenges in operationalizing privacy principles due to a lack of knowledge, trained personnel and standardized roles [3, 10–12, 20]. The National Data Protection Authority (ANPD) has issued guidelines defining the responsibilities of key agents such as the Data Protection Officer (DPO), Controller, and Processor, and has highlighted the need for institutional structures to support compliance efforts [9].

Several Brazilian initiatives have attempted to fill this gap by proposing maturity models and training programs for public servants. Privacy and Security Program (PPSI)[15] developed under the Secretariat for Digital Government (SGD/MGI) provides a foundational framework for implementing privacy and security practices in public organizations. The PPSI includes guidelines for security, governance, technical safeguards, data recovery protocols, and compliance auditing, but until recently, lacked a structured mapping of competencies per organizational role.

Internationally, the ENISA Cybersecurity Skills Framework [4] and the NIST Privacy Framework [1] have underscored the importance of defining roles and knowledge domains to enable workforce development and strategic governance. However, few works provide a detailed, multi-role competency model directly tailored to the public sector's needs under local legislation like the LGPD.

A recent study by Martins et al. [9] investigated the alignment between the competencies required for the Data Protection Officer (DPO) role under LGPD and the learning outcomes of Information Systems undergraduate programs. Using a documental analysis approach, the authors compared the competency framework proposed by the Brazilian National Data Protection Authority (ANPD) with the official curriculum guidelines for Information Systems courses. The study found that although there is partial overlap in technical and managerial competencies—such as information security, governance, and legal compliance—important gaps remain, particularly in competencies related to legal interpretation, data ethics, and risk management. The findings reinforce the need for targeted professional training and curriculum enhancements to support the qualification of DPOs. This work complements our research by focusing on a specific privacy-related role and highlighting the need for structured frameworks that map knowledge, skills, and abilities in public sector contexts.

The study by Spósito et al. [19] proposed a structured training journey aimed at enhancing the competencies of privacy and information security practitioners in Brazil's federal public administration. Grounded in the guidelines of the LGPD and national information security standards, the authors used a multi-step design science approach to identify training needs, organize learning paths, and define content delivery strategies. Their training journey is aligned with institutional roles and emphasizes the progression of knowledge through foundational, intermediate, and advanced modules. The study contributes a practical roadmap for capacity-building in the public sector, supporting both compliance and cultural change. Our work builds upon this by formalizing the competency profiles through a role-based framework that defines knowledge, skills, and abilities (KSAs), and by proposing maturity indicators and individualized learning assessments for broader governance implementation.

Beyond privacy, information security has also received attention in Brazilian public administration through initiatives like the PPSI and the IN GSI/PR nº 3/2021 [13]. These frameworks define key responsibilities such as risk management, incident response, change management, and business continuity. Nonetheless, the lack of a unified competency model hampers effective implementation. Our work extends the current literature by integrating both privacy and information security perspectives into a comprehensive, role-based competency framework tailored to the needs of public sector institutions.

Haqaf and Koyuncu [6] conducted a Delphi study to identify the core competencies required for Information Security Managers (ISMs) across organizational contexts. Based on a comprehensive literature review and feedback from certified security experts worldwide, the authors structured the findings into five main categories encompassing 16 essential skills. These include technical competencies such as network, system, and application security, as well as cryptography. Risk management skills (e.g., risk assessment and mitigation), project management skills (e.g., planning, budgeting, and resource management), and business-oriented skills (e.g., policy development, legal and regulatory compliance, and business continuity management) were also emphasized. Finally, foundational security skills were identified, such as information security governance, incident response, and employee awareness programs. The study reinforces the importance of integrating managerial, technical, and compliance capabilities in the ISM role. These findings complement our work by confirming the need for a multidimensional competency framework, especially in the public sector, where legal obligations and organizational complexity require precise alignment of roles, responsibilities, and professional skills.

A recent comparative study by Rocha and Canedo [16] analyzed the convergence and divergence between major international privacy regulations (GDPR, LGPD, CCPA) and key privacy frameworks (NIST, ISO/IEC 27701). Using a document analysis method, the authors identified critical compliance requirements and mapped them to governance, technical, and organizational dimensions. The study emphasized the need for alignment between legal obligations and operational capabilities, proposing a taxonomy of privacy practices that bridges regulatory expectations and implementation strategies. Their findings reinforce the relevance of structured role-based frameworks for public and private organizations, especially in managing complex regulatory landscapes. This work complements our proposal by providing a macro-level analysis of legal and normative requirements, which our study operationalizes into actionable knowledge, skills, and abilities (KSAs) mapped to institutional roles.

3 Methodology

This study employed a design-oriented research approach to develop two structured competency frameworks—one focused on privacy and the other on information security—within the context of the Brazilian federal public sector. The main goal was to define and validate the knowledge, skills, and abilities (KSAs) required for effective performance of key roles in both domains, aligned with the Brazilian General Data Protection Law (LGPD) [2] and national information security policies such as Normative Instruction GSI/PR No. 3/2021 [13] and the Privacy and Security Information Program (PPSI) [15]. Two research questions (RQ) guided the study:

RQ1.: What are the key roles, responsibilities, and competency levels required for effective data privacy and information security governance in public sector organizations?
Objective: To identify and define strategic professional profiles in both domains, and describe the KSAs required for each role across three levels of proficiency (Basic, Intermediate, Advanced).

RQ2.: How do the identified roles interact to ensure compliance and risk mitigation, and what are the potential gaps or overlaps in responsibilities across privacy and information security domains?
Objective: To analyze the interdependencies and possible redundancies among roles, supporting better alignment and role distribution within public governance structures.

The methodology was structured into four main phases:

(1) **Document Analysis:** We analyzed over sixty official legal, normative instruction, and technical documents from the National Data Protection Authority (ANPD), the Secretariat for Digital Government (SGD/MGI), the Institutional Security Office (GSI/PR), and the PPSI. These included the LGPD, ANPD guidance for data controllers and processors, internal control guidelines, and regulations defining information security roles and responsibilities.

(2) **Role Identification and Modeling:** Based on legal definitions and institutional structures, we identified **eight privacy-related profiles** (e.g., DPO, Controller, Processor, Data Subject) and **sixteen information security profiles** (e.g., InfoSec Manager, Risk Manager, Change Manager, Incident Response Team). For each profile, we extracted role-specific responsibilities, operational tasks, and organizational interfaces.

(3) **Competency Definition:** For each profile, we defined expected KSAs across three proficiency levels (Basic, Intermediate, Advanced). These were categorized into four domains: technical knowledge (e.g., cloud computing, secure storage), regulatory understanding (e.g., consent, accountability), governance and risk (e.g., policy development, continuity planning), and organizational culture (e.g., transparency, collaboration).

(4) **Validation and Structuring:** The resulting frameworks were reviewed and refined through expert validation sessions. Competencies were then organized into training journeys to support capacity-building programs. To prioritize learning paths and training efforts, we adopted the Analytic Hierarchy Process (AHP) [14] in a subsequent phase.

This methodology ensures that the proposed frameworks are legally grounded, contextually adapted to public institutions, and suitable for integration into software quality and governance maturity initiatives—particularly by supporting privacy-aware and security-resilient system design, operation, and oversight.

4 Results

4.1 RQ1. What are the key roles, responsibilities, and competency levels required for effective data privacy and information security governance in public sector organizations?

To address RQ1, we developed two structured competency frameworks—one for privacy governance and another for information security—each tailored to the regulatory and operational context of the Brazilian federal public sector. Together, they encompass a total of **24 professional profiles** (8 in privacy and 16 in information security), each associated with specific responsibilities and mapped to required knowledge, skills, and abilities (KSAs) across three levels of proficiency: Basic, Intermediate, and Advanced.

4.1.1 Privacy Competency Framework. The *Privacy Competency Framework* defines eight strategic roles involved in the lifecycle of personal data processing in accordance with the LGPD and ANPD guidelines. These roles are: *Data Protection Officer (DPO), Controller, Processor, Data Subject, Support Team to the DPO, Senior Management, Internal Control Officer*, and *End User*. They represent a diverse range of stakeholders with distinct responsibilities in ensuring legal compliance, technical implementation, organizational alignment, and user awareness.

For each role, the framework articulates KSAs that span domains such as legal interpretation (e.g., lawful basis for processing), privacy principles (e.g., Privacy by Design), IT and data governance, and ethical responsibilities. This competency mapping helps organizations understand what is expected from each actor involved in the implementation of privacy measures, and supports training and professional development. Table 1 summarizes these roles and their responsibilities.

A total of 136 unique competencies were identified and distributed across five proficiency levels, reflecting the progression of knowledge, skills, and abilities (KSAs) required for effective performance in privacy role. At the foundational end, 34 competencies were categorized as *Beginner*, focusing on basic awareness and understanding of core principles. The *Basic* and *Intermediate* levels included 36 competencies each, covering more structured knowledge of legal, organizational, and technical domains. At the upper tiers, 20 competencies were mapped to the *Advanced* level, emphasizing governance, risk management, and interdepartmental coordination, while 10 highly specialized competencies were assigned to the *Expert* level, requiring deep domain expertise, critical thinking, and strategic decision-making capabilities. This distribution enables the design of targeted training journeys and supports institutions in building progressive learning paths based on employee roles and institutional maturity.

To support the practical adoption of the proposed framework, an interactive online version is publicly available at: https://competencias-privacidade.vercel.app/. This platform provides detailed access to all mapped roles related to privacy, including their respective responsibilities (activities and obligations), individual competencies (technical and multidisciplinary knowledge), and organizational competencies (mastery of applicable laws and standards). The site serves as a reference tool for public institutions and professionals aiming to implement structured training journeys, assess institutional readiness, and align role expectations with the LGPD and other regulatory frameworks.

4.1.2 Information Security Competency Framework. In parallel, the *Information Security Competency Framework* outlines 16 roles based on the official responsibilities defined in IN GSI/PR No. 3/2021 and complementary institutional guidelines such as the PPSI. These roles include *Information Security Manager, User, Internal Control Unit Head, Senior Management 1, Senior Management 2, ICT Manager, Business Continuity Management Agent*, among others. They are distributed across operational, tactical, and strategic levels and are necessary to ensure confidentiality, integrity, availability, and resilience of government systems.

These profiles were mapped with a focus on governance, risk assessment, incident response, secure systems operation, cloud and media management, and institutional control. Each role is associated with a set of KSAs reflecting required technical expertise, regulatory familiarity, and decision-making capabilities. Table 2 presents a detailed overview of these roles and their main responsibilities.

In this framework, a total of **123 distinct competencies** were identified and distributed across five proficiency levels. The distribution is as follows: 11 competencies at the *Expert* level, 36 at the *Advanced* level, 36 at the *Intermediate* level, 19 at the *Basic* level, and 21 at the *Beginner* level. This updated mapping reflects a consolidated and focused articulation of the key knowledge areas required to fulfill institutional responsibilities, without redundancy. The higher concentration of foundational competencies reinforces the need for broad awareness and cross-cutting training among all public servants, while the competencies at the higher levels serve as anchors for specialized training for high-responsibility roles such as Information Security Manager, Compliance Officer, and Business Continuity Agent.

All identified competencies and role-based mappings for information security are publicly available in an interactive online platform: https://competencias-seguranca.vercel.app/. This platform provides full access to: (i) Responsibilities – detailed descriptions of activities and obligations per role; (ii) Individual Competencies – multidisciplinary technical knowledge, skills, and abilities (KSAs); and (iii) Organizational Competencies – institutional-level understanding of relevant legislation, standards, and governance mechanisms. The platform is designed to support self-assessment, training planning, and institutional benchmarking.

RQ.1 Summary: The study identified 24 strategic professional profiles—8 related to data privacy and 16 to information security—based on Brazilian regulations such as the LGPD and IN GSI/PR nº 3/2021. Each profile was mapped to a structured set of knowledge, skills, and abilities (KSAs) across three proficiency levels. The competency frameworks support role clarity, training design, and personnel evaluation. They also help align institutional responsibilities with legal and technical requirements, promoting the quality and trustworthiness of public digital services.

Table 1: Profiles and Responsibilities in Privacy

Profile	Main Responsibilities
1. Data Protection Officer (DPO)	Acts as a communication channel between the organization, data subjects, and the data protection authority; ensures compliance with LGPD; manages the privacy governance program.
2. Data Controller	Defines the purposes and legal bases for processing personal data; ensures the rights of data subjects are respected; designates the DPO; supervises processing activities.
3. Data Processor	Processes personal data on behalf of the Controller; follows documented instructions; ensures the implementation of appropriate technical and organizational security measures.
4. Data Subject	Has rights guaranteed under LGPD, such as access, correction, deletion, portability, and revocation of consent; must be informed about the processing of their data.
5. Support Team to the DPO	Assists the DPO in managing interactions with the ANPD and data subjects; helps document compliance activities, perform impact assessments, and organize training sessions.
6. Senior Management	Ensures the implementation of privacy governance structures; approves policies and reports; provides the necessary human, financial, and technological resources for compliance.
7. Internal Control Unit Head	Monitors and supervises the activities of the first line of defense; ensures alignment with privacy and data protection requirements; supports audits, risk management, and training.
8. User	Accesses and processes personal data within systems; must comply with privacy and data protection policies; ensures security and transparency in data handling activities.

4.2 RQ2. How do the identified roles interact to ensure compliance and risk mitigation, and what are the potential gaps or overlaps in responsibilities across privacy and information security domains?

The analysis of RQ2 focused on the interplay between the 24 professional profiles mapped in the two competency frameworks. By examining the distribution of competencies across roles, we observed several important patterns of interdependence, coordination, and redundancy that influence the effectiveness of privacy and information security governance in public institutions.

First, a clear area of intersection was found in roles that participate in both privacy and security domains—particularly the *Senior Management*, *Internal Control Unit*, and *End Users*. These profiles are required to demonstrate competencies related to both privacy principles (e.g., data subject rights, lawful processing) and security operations (e.g., data classification, incident reporting). This overlap reflects the dual responsibility of leadership and frontline personnel in upholding legal and operational standards across governance layers.

Second, the mapping revealed functional dependencies among specialized roles. For example, the *Data Protection Officer (DPO)* relies on inputs from roles such as the *ICT Manager*, *Information Security Risk Management Agent*, and *Compliance Assessment Agent* to maintain accurate data inventories, assess risks, and ensure secure processing environments. Similarly, the *Information Security Manager* must coordinate with the *Controller* and *Support Team to the DPO* when implementing access controls or investigating data breaches. These inter-role dependencies require structured collaboration and well-defined communication protocols, which are not always explicit in current institutional practices.

Third, some roles appear in both frameworks but with different emphases. For instance, *Senior Management* is expected to approve governance policies in both domains but must demonstrate deeper legal understanding in privacy and broader strategic oversight in security. The *Internal Control Unit*, similarly, monitors compliance across both areas but engages more actively in risk monitoring and audit activities in security contexts. These variations suggest the need for differentiated training even within shared roles.

Fourth, we identified potential gaps in accountability, especially in roles responsible for digital communication and cloud environments. While the *Secure Social Media Use Agent* and the *Profile Administration Team* are clearly defined in the security framework, there are no direct privacy equivalents responsible for ensuring lawful processing in these channels. This highlights a governance gap where privacy risks may be insufficiently addressed in communication platforms unless cross-role collaboration is formally established.

Finally, there is notable asymmetry in the granularity of the two frameworks. The information security structure defines highly specialized roles (e.g., Change Manager, Incident Response Team, Business Continuity Agent), while the privacy framework tends to be broader, consolidating multiple responsibilities within fewer profiles (e.g., the DPO encompasses legal, operational, and governance duties). This structural difference reflects the current maturity of each domain in public institutions and underscores the importance of progressively refining privacy-related roles as implementation advances.

In summary, the cross-domain interactions demand coordinated governance strategies and integrated training plans. Our findings reinforce the need for institution-wide strategies to map overlapping responsibilities, promote shared accountability, and facilitate joint monitoring of privacy and security risks. The interaction diagram (Figure 1) visualizes these connections and can be used to guide organizational restructuring or internal policy alignment.

The interactions illustrated in Figure 1 highlight the practical interdependencies between privacy and information security roles in public governance. Shared actors such as *Senior Management*, *ICT Manager*, and *Internal Control Unit* serve as communication and coordination bridges between the two domains. Their responsibilities span both legal compliance (e.g., LGPD) and operational

Table 2: Information Security Profiles and Their Responsibilities

Profile	Main Responsibilities
1. Information Security Manager	Coordinates the information security policy; appoints responsible agents; approves plans and reports; promotes training; interacts with senior management and the Institutional Security Office; oversees compliance, risks, change management, business continuity, and cloud security.
2. User	All individuals who interact with systems handling sensitive or classified data; must follow security policies and good practices.
3. Internal Control Unit Head	Part of the second line of defense; supervises the first line; ensures the effectiveness of internal controls; supports risk management and compliance processes.
4. Senior Management 1	Approves policies, reports, and regulatory documents; appoints managers and compliance agents; ensures resource allocation and staff training; responsible for implementing mandatory security controls.
5. Senior Management 2	Same responsibilities as Senior Management 1 (may represent additional executive leadership).
6. ICT Manager	Plans and implements secure and privacy-aware ICT solutions; supports the Information Security Manager and the Data Protection Officer; participates in criticality assessment models.
7. IT Team	Civil servants working directly or indirectly with information security; implement and maintain critical infrastructure and systems.
8. Cyber Incident Response Team (ETIR)	Handles cybersecurity incident response; composed of technically qualified staff; autonomy level must be formally defined; follows guidelines from the Governmental Cyber Incident Response Center.
9. Information Asset Management Agent	Identifies, classifies, and assesses information assets; identifies threats and vulnerabilities; consolidates reports on asset security.
10. Change Management Agent (InfoSec)	Collaborates with the technical group; drafts and monitors change evaluation and approval documents; ensures audit trail of the process.
11. Compliance Assessment Agent	Develops compliance verification plans and reports; evaluates the adherence of security procedures; issues technical compliance opinions.
12. Information Security Risk Management Agent	Prepares the risk management plan and reports on the identification, analysis, evaluation, and treatment of information security risks.
13. Business Continuity Management Agent (InfoSec)	Evaluates and supervises the business continuity plan; proposes improvements; promotes a continuity culture in the context of information security.
14. Security and Accreditation Manager	Manages classified information; initiates accreditation processes; authorizes access to restricted areas.
15. Institutional Social Media Management Team	Creates, edits, and deletes official social media profiles; removes content that may pose a security risk; generates monthly usage and incident reports.
16. Secure Social Media Use Agent	Monitors safe practices in institutional social media use; ensures compliance with internal regulations; promotes a culture of secure digital behavior; reports incidents to the Information Security Manager.

assurance (e.g., incident response), reinforcing the need for joint training and integrated decision-making. The separation of domain-specific roles (blue for privacy, green for security) also reveals the potential for specialized capacity-building pathways, while drawing attention to shared responsibilities that demand synchronized efforts across organizational units.

The analysis of the competency matrices revealed a structured and scalable set of knowledge requirements that support the development of role-specific training strategies across the public sector (see Figure 2). In total, 123 unique competencies were identified for information security roles, and 136 for privacy-related roles, distributed across five proficiency levels. The privacy domain showed concentration in the lower and intermediate levels—suggesting a need to strengthen foundational knowledge while progressively advancing capabilities toward strategic and expert domains. In return, information security roles had 36 intermediate-level and advanced-level competencies, reflecting a broad need for a in-depth knowledge across institutional actors. The layered structure of this framework allows organizations to adopt incremental capacity-building strategies, starting with mass-level training for baseline

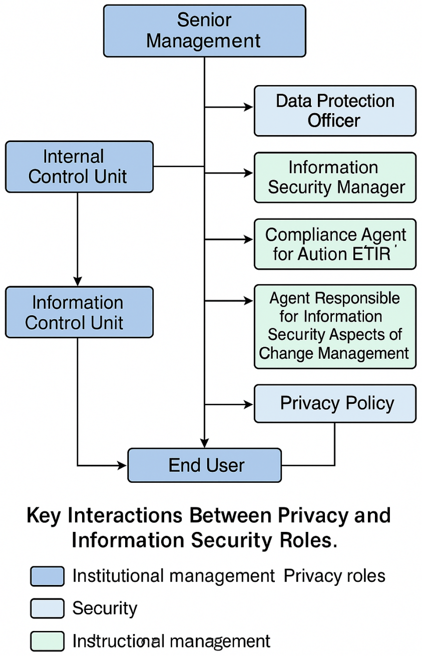

Senior Management
Data Protection Officer
Internal Control Unit
Information Security Manager
Compliance Agent for Aution ETIR
Information Control Unit
Agent Responsible for Information Security Aspects of Change Management
Privacy Policy
End User
Key Interactions Between Privacy and Information Security Roles.
Institutional management Privacy roles
Security
Instructional management

Figure 1: Key Interactions Between Privacy and Information Security Roles. Roles from privacy (blue), security (green), and institutional management (dark blue) interact to ensure coordinated governance across domains.

awareness and progressing toward targeted up skilling for specialized roles such as Information Security Managers, Risk Officers, and Compliance Agents. Furthermore, the mapping of each competency to specific profiles allows for role-based planning and individualized progression through training journeys. This alignment between role, knowledge domain, and proficiency level is important for enabling institutions to monitor maturity growth, address capability gaps, and foster a culture of continuous learning in privacy and security governance.

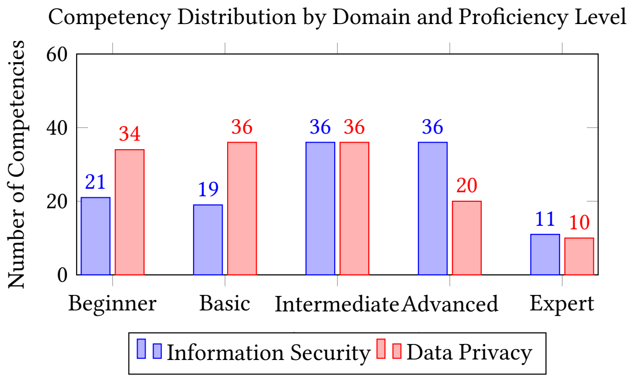


Figure 2: Comparison of the number of mapped competencies by proficiency level for information security and data privacy roles.

RQ.2 Summary: The analysis of interactions between privacy and information security roles revealed critical overlaps in institutional governance, particularly involving senior management, internal control units, and ICT managers. These actors bridge responsibilities across both domains, highlighting the need for integrated training and coordinated decision-making. The results also indicate potential gaps in collaboration and competency alignment, which may affect the effectiveness of risk management and compliance. A visual interaction map was developed to support organizational planning.

4.3 Online Self-Assessment of Knowledge Level

To complement the competency frameworks, we developed a publicly accessible digital platform[1] that enables civil servants to assess their current level of knowledge in privacy-related competencies. This self-assessment tool is part of the broader training journey proposed for the Brazilian federal public administration and is aligned with the roles and responsibilities defined in the LGPD and national privacy governance guidelines.

Upon accessing the platform, users are invited to select their professional profile—such as Data Protection Officer, Controller, Processor, Internal Control Officer, or Senior Management—and provide information about their academic background, professional experience, language certifications, and technical skills. The system presents a set of structured questions that cover individual and organizational competencies in areas including Information Technology, Privacy by Design, Legislation, Risk and Compliance, and Privacy Strategies (see Figure 3).

Each competency area is weighted using the Analytic Hierarchy Process (AHP), a decision-making technique that allows the relative importance of criteria to be incorporated into the final score [14]. After completing the questionnaire, the system calculates a total knowledge score, expressed both as an absolute value and a percentage, along with detailed results by area (Figure 4).

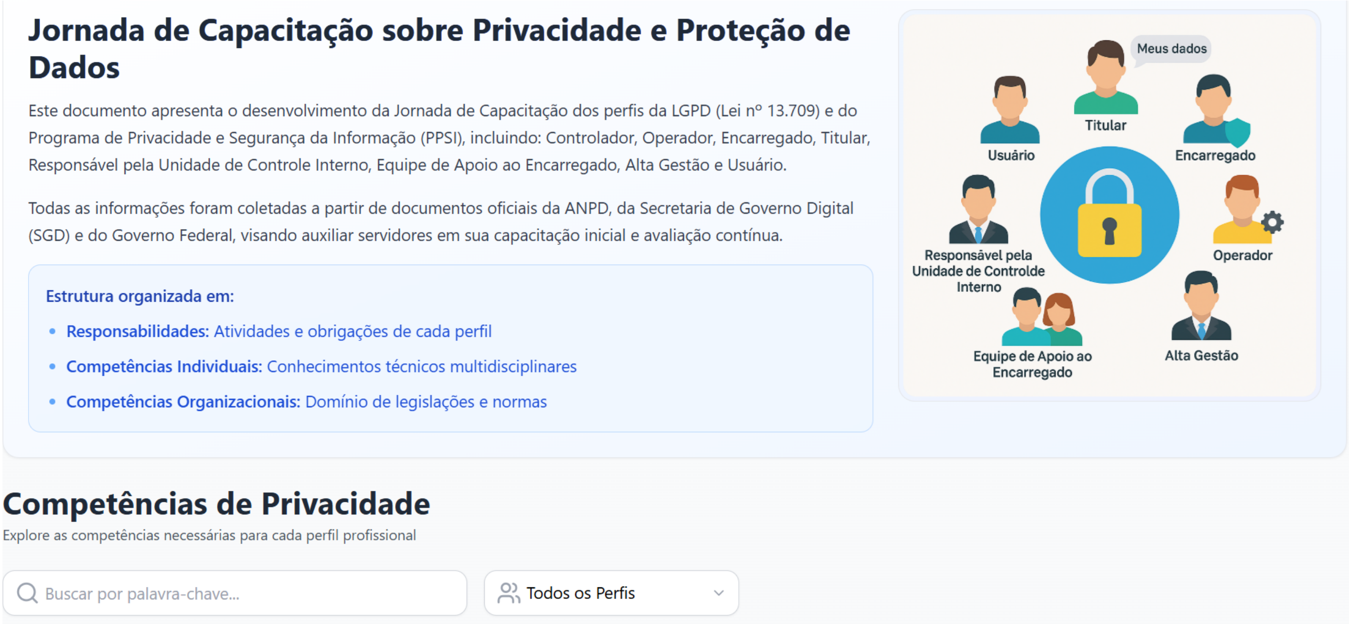
This mechanism serves two main purposes. First, it supports civil servants in identifying individual skill gaps and planning their personalized training paths. Second, it enables public institutions to conduct diagnostics of organizational knowledge maturity, helping decision-makers prioritize investments in capacity-building and compliance readiness. The integration of AHP ensures that strategic competencies—such as legal interpretation or risk management—receive appropriate emphasis, while the visual breakdown helps users understand their strengths and weaknesses.

The platform thus operationalizes the competency framework by providing a dynamic, role-based, and data-driven tool for capacity-building in public sector privacy governance.

5 Discussion and Practical Implications

The competency frameworks and interaction analysis presented in this study offer a multi-dimensional foundation for improving governance practices, compliance assurance, and software quality in the public sector. Beyond mapping roles and responsibilities, the

[1] https://competencias-privacidade.vercel.app/



Jornada de Capacitação sobre Privacidade e Proteção de Dados

Este documento apresenta o desenvolvimento da Jornada de Capacitação dos perfis da LGPD (Lei nº 13.709) e do Programa de Privacidade e Segurança da Informação (PPSI), incluindo: Controlador, Operador, Encarregado, Titular, Responsável pela Unidade de Controle Interno, Equipe de Apoio ao Encarregado, Alta Gestão e Usuário.

Todas as informações foram coletadas a partir de documentos oficiais da ANPD, da Secretaria de Governo Digital (SGD) e do Governo Federal, visando auxiliar servidores em sua capacitação inicial e avaliação contínua.

Estrutura organizada em:

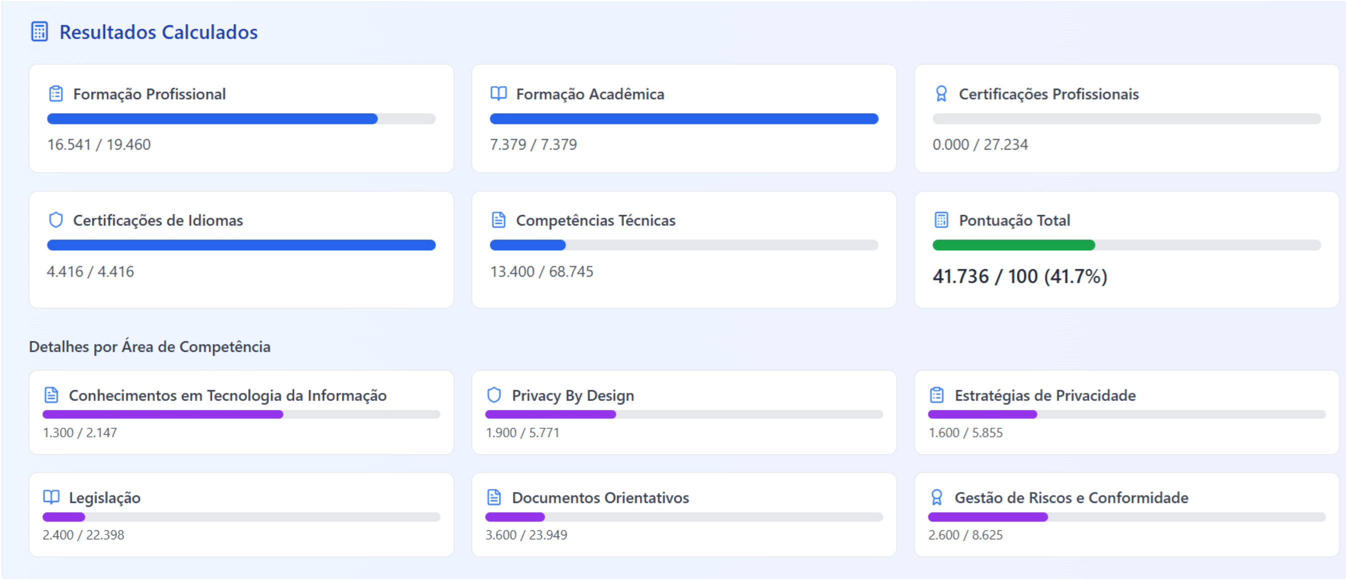
- **Responsabilidades:** Atividades e obrigações de cada perfil
- **Competências Individuais:** Conhecimentos técnicos multidisciplinares
- **Competências Organizacionais:** Domínio de legislações e normas

Meus dados
Titular
Usuário
Encarregado
Responsável pela Unidade de Controlde Interno
Operador
Equipe de Apoio ao Encarregado
Alta Gestão

Competências de Privacidade

Explore as competências necessárias para cada perfil profissional

Figure 3: Training Journey Interface – Overview of Privacy Roles and Areas



Resultados Calculados

Formação Profissional	16.541 / 19.460
Formação Acadêmica	7.379 / 7.379
Certificações Profissionais	0.000 / 27.234
Certificações de Idiomas	4.416 / 4.416
Competências Técnicas	13.400 / 68.745
Pontuação Total	41.736 / 100 (41.7%)

Detalhes por Área de Competência

Conhecimentos em Tecnologia da Informação	1.300 / 2.147
Privacy By Design	1.900 / 5.771
Estratégias de Privacidade	1.600 / 5.855
Legislação	2.400 / 22.398
Documentos Orientativos	3.600 / 23.949
Gestão de Riscos e Conformidade	2.600 / 8.625

Figure 4: Calculated Knowledge Score by Area

frameworks enable strategic decision-making in human resource development, institutional diagnostics, and risk prevention. This section presents practical recommendations for implementing the models, proposes maturity indicators, and discusses how public institutions can integrate these structures into their broader digital governance ecosystems.

5.1 From Frameworks to Action: Implementing Training Journeys

The structured definition of Knowledge, Skills, and Abilities (KSAs) allows institutions to translate abstract regulatory demands into actionable training pathways. We propose the implementation of personalized *training journeys* aligned with role-specific responsibilities and institutional maturity. These journeys follow a modular design—**Basic**, **Intermediate**, and **Advanced**—mapped directly to the competencies defined in the frameworks.

This modular architecture is important in the public sector, where heterogeneous staff profiles, resource constraints, and evolving responsibilities demand scalable and adaptable training structures. Foundational modules may focus on mass awareness—e.g., LGPD principles or good security practices for end users—while advanced tracks can deepen capabilities in governance, risk management, and secure system design. Importantly, the training structure should not be static: journeys must evolve alongside changes in legislation, threat landscapes, and technological infrastructures.

A practical implementation strategy includes:

1. **Competency diagnosis:** Conduct assessments to identify current skill levels and gaps per employee or role cluster.
2. **Journey design:** Tailor content based on organizational unit, exposure to personal data, and criticality of the role (e.g., DPOs and Risk Officers).
3. **Adaptive delivery:** Use synchronous formats (e.g., workshops), asynchronous e-learning, and immersive simulations to meet diverse learning needs.
4. **Institutional support:** Ensure managerial sponsorship and allocate protected time for learning to reduce dropout rates and fatigue.

5.2 Knowledge Maturity and Strategic Indicators

Operationalizing training efforts requires a way to measure progress. The frameworks support the construction of **knowledge maturity indicators**, enabling decision-makers to monitor and steer institutional capacity-building. We propose the following set of indicators:

- **Coverage Indicator:** Proportion of mapped roles for which staff have completed competency-aligned training.
- **Depth Indicator:** Average proficiency level achieved across roles (e.g., percentage reaching Advanced).
- **Volatility Indicator:** Frequency of staff turnover in critical roles affecting continuity of knowledge.
- **Progress Indicator:** Differential in KSA scores before and after training interventions.
- **Risk Gap Indicator:** Number of critical responsibilities allocated to untrained or partially qualified personnel.

These indicators can be used in dashboards to monitor performance across departments and serve as input for audit reports, maturity assessments, and funding prioritization.

5.3 Strategic Adoption and Integration with Public Sector Reforms

Adopting the frameworks is not only a technical challenge, but also a governance opportunity. Institutions can embed these models into strategic HR management (e.g., recruitment, promotions, performance appraisals), audit checklists, and digital transformation roadmaps. Notably, the frameworks support alignment with national initiatives such as the Privacy and Security Program (PPSI), Digital Government Plan (PDG), and Integrated Public Services System (SISP).

Successful adoption requires:

- **Policy integration:** Embed role-based competencies into internal regulations and standard operating procedures (SOPs).
- **Organizational alignment:** Link competencies with departmental missions—e.g., legal units with privacy governance; IT with secure development.
- **Incentive structures:** Reward up-skilling through certifications, recognition programs, or advancement pathways.
- **Monitoring councils:** Establish privacy and information security governance committees to oversee training and maturity evolution.

5.4 Scaling and Replicability Across Government Sectors

Although this study focused on the federal administration, the frameworks are replicable in state and municipal governments. This is especially relevant given the heterogeneity in privacy and security maturity across Brazil's federative units. By using shared competency definitions and assessment instruments, governments can standardize benchmarks while tailoring journeys to local realities. To support scaling, we propose:

- **Public repositories:** Maintain open-access catalogs of roles, KSAs, training content, and case studies.
- **National LMS integration:** Deploy journeys through ENAP [2], EV.G [3], and other federal learning platforms with SCORM [4] or xAPI [5] compliance.
- **Cross-agency collaboration:** Encourage peer-learning across agencies through communities of practice and knowledge-sharing events.

5.5 Cultural Transformation and the Sociotechnical Challenge

Ultimately, privacy and security governance is not only a legal obligation but a cultural and sociotechnical transformation. The competency frameworks clarify the human dimension of this shift, empowering individuals at all levels of the organization to understand their roles in safeguarding public trust. To catalyze this transformation, institutions must frame privacy and security as enablers of digital quality—not constraints. This requires inclusive leadership, transparent communication, and continuous investment in people.

The frameworks, by structuring the required knowledge landscape, offer a bridge between policy, technology, and organizational behavior. When embedded into strategic planning, they enable a virtuous cycle: improved training leads to stronger governance, which enhances system quality and user trust—feeding back into institutional resilience and service excellence.

6 Threats to Validity

This section discusses potential threats to the validity of our study, following the classification proposed by Wohlin et al. [23], including

[2] urlhttps://enap.gov.br/pt/
[3] urlhttps://www.escolavirtual.gov.br/
[4] urlhttps://scorm.com
[5] https://xapi.com/

threats to internal, construct, external, and conclusion validity. We also present mitigation strategies adopted to reduce their impact.

Construct validity concerns whether the methods and instruments accurately capture the concepts being investigated. In this study, the definition of roles, responsibilities, and KSAs was based on legal and normative documents (e.g., LGPD, PPSI, IN GSI/PR nº 3/2021) and interpreted by the research team. A possible threat lies in subjective interpretation of textual norms or potential omissions in the source material. To mitigate this, we used triangulation of sources (laws, decrees, institutional guides), consulted multiple researchers with expertise in information security and privacy governance, and cross-referenced definitions with prior academic literature. Additionally, the frameworks were validated through expert analysis from practitioners in public sector digital governance.

Internal validity refers to whether the conclusions drawn about causal relationships are correct. Since our study does not involve controlled experiments or cause-effect testing, this threat is less prominent. However, there is a risk that the mapping between roles and competencies may have been influenced by implicit biases or incomplete role understanding. To reduce this risk, we applied a systematic analysis of each profile's formal responsibilities and adopted iterative reviews during the competency mapping phase. Furthermore, we applied AHP to bring structure and transparency to the prioritization of KSAs, reducing arbitrariness.

External validity concerns the generalizability of the results to other contexts. While our frameworks are tailored to the Brazilian federal public administration, similar roles and responsibilities exist in other countries and public agencies. Nonetheless, organizational structures, legal terminology, and maturity levels may vary significantly. To mitigate this threat, the frameworks were grounded in internationally recognized principles (e.g., GDPR, ISO/IEC 27701), and we designed the role-competency structure to be adaptable. Future work includes replication of this model in different government levels (state, municipal) and potential adaptation to private-sector use cases.

Conclusion validity relates to the reliability of the conclusions drawn from the data. As our study includes qualitative mapping and does not rely on statistical hypothesis testing, there is limited risk of type I or II statistical errors. However, there is a threat that conclusions may not be replicable or that competency assignments may be inconsistently interpreted. To address this, we documented our methodology transparently, included detailed competency definitions, and made the resulting framework publicly accessible via an online platform at: https://competencias-privacidade.vercel.app/ and https://competencias-seguranca.vercel.app/. This transparency supports peer review, community feedback, and future updates.

7 Conclusion

This study proposed a role-based competency framework to enhance privacy and information security governance in Brazil's federal public administration. Grounded in national legislation (LGPD), regulatory instruments (PPSI, IN GSI/PR nº 3/2021), and international standards (e.g., ISO/IEC 27701), the framework identifies key institutional roles, maps their responsibilities, and defines the knowledge, skills, and abilities (KSAs) required at different levels of proficiency.

By modeling **8 strategic roles in privacy** and **16 in information security**, the framework delivers a comprehensive and actionable view of the organizational landscape responsible for protecting personal data and ensuring secure digital services. The competency models serve not only as guidance for role clarification but also as a foundation for scalable training programs, performance evaluation, institutional benchmarking, and workforce planning.

Key contributions of this work include:

- A structured mapping of KSAs aligned with regulatory expectations and operational responsibilities;
- A methodology for building training journeys tailored to different maturity levels;
- A visual interaction model identifying interdependencies and potential governance gaps across roles;
- Practical indicators to monitor knowledge maturity and support strategic decision-making.

The availability of an interactive online platform[6] [7] extends the reach of the framework, enabling public managers, policymakers, and practitioners to explore and adopt its components in a modular and accessible way. The platform also fosters transparency and collaborative improvement through community engagement.

By approaching privacy and security not merely as compliance imperatives, but as institutional capabilities, this research advances the understanding of how human capital and organizational structure impact the quality, reliability, and trustworthiness of public digital services. The framework aligns with software quality principles such as security, maintainability, transparency, and user trust—key attributes in modern governance.

Future work includes pilot implementations in public agencies, empirical evaluation of training journeys, and adaptation of the framework to other levels of government and organizational contexts. We also aim to integrate the competency models with digital maturity assessments and service design initiatives to reinforce the role of privacy and security as strategic enablers of digital transformation in the public sector.

Acknowledgment

This study was financed in part by the Project No. TED 33/2023 “Pesquisa Aplicada em Privacidade e Segurança da Informação na Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital" – Diretoria de Privacidade e Segurança da Informação (DPSI)/Centro de Excelência em Privacidade e Segurança (CEPS)/ Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação (MGI) em Serviços Públicos do Governo Federal; and Conselho Nacional de Desenvolvimento Científico e Tecnológico CNPq (Grant 300883/2025-0).

REFERENCES

[1] Meghan Anderson, Dylan Gilbert, and Nakia Grayson. April 14, 2025. NIST Privacy Framework 1.1. *National Institute of Standards and Technology* (April 14, 2025). https://doi.org/10.6028/NIST.CSWP.40.ipd

[2] Brasil. 2018. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da República Federativa do Brasil* 1 (2018), 1–23. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[3] Edna Dias Canedo, Angélica Toffano Seidel Calazans, Ian Nery Bandeira, Pedro Henrique Teixeira Costa, and Eloisa Toffano Seidel Masson. 2022. Guidelines

[6] https://competencias-privacidade.vercel.app/

[7] https://competencias-seguranca.vercel.app/

adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requir. Eng.* 27, 4 (2022), 545–567. https://doi.org/10.1007/S00766-022-00391-7

[4] ENISA European Union Agency for Cybersecurity. 2022. European Cybersecurity Skills Framework Role Profiles. *ENISA* 1 (2022), 1–45. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

[5] International Organization for Standardization (ISO). 2019. ISO/IEC 27701: 2019 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines, ISO.

[6] Husam Haqaf and Murat Koyuncu. 2018. Understanding key skills for information security managers. *International Journal of Information Management* 43 (2018), 165–172.

[7] Guntur Budi Herwanto, Fajar J. Ekaputra, Gerald Quirchmayr, and A Min Tjoa. 2024. Toward a Holistic Privacy Requirements Engineering Process: Insights From a Systematic Literature Review. *IEEE Access* 12 (2024), 47518–47542. https://doi.org/10.1109/ACCESS.2024.3380888

[8] Lennart Kiss and Rachelle Sellung. 2025. Human-centered design of a privacy assistant and its impact on perceived transparency and intervenability. *i-com* 24, 1 (2025), 159–172. https://doi.org/10.1515/ICOM-2024-0064

[9] Maria Martins, Yuska Aguiar, and Juliana Saraiva. 2025. Assessment of Competences for LGPD DPO through ANPD Standard and Information Systems Curriculum. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação* (Recife/PE). SBC, Porto Alegre, RS, Brasil, 565–574. https://doi.org/10.5753/sbsi.2025.246585

[10] Aryely Matos, Mario Patrício, Maria Isabel Nicolau, Edna Dias Canedo, Juliana Alves Pereira, and Anderson Uchôa. 2025. Data Privacy in Software Practice: Brazilian Developers' Perspectives. *Journal of Internet Services and Applications* 16, 1 (Jun. 2025), 299–319. https://doi.org/10.5753/jisa.2025.5302

[11] Mariana Maia Peixoto, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo, and Tony Gorschek. 2023. The perspective of Brazilian software developers on data privacy. *J. Syst. Softw.* 195 (2023), 111523. https://doi.org/10.1016/J.JSS.2022.111523

[12] Mariana Maia Peixoto, Tony Gorschek, Daniel Méndez, Carla Silva, and Davide Fucci. 2025. The Perspective of Agile Software Developers on Data Privacy. *J. Softw. Evol. Process.* 37, 2 (2025). https://doi.org/10.1002/SMR.2755

[13] Augusto Heleno Ribeiro Pereira. 2021. Instrução Normativa GSI/PR Nº 3, DE 28 DE MAIO DE 2021. *PRESIDÊNCIA DA REPÚBLICA* 1 (2021), 1–13. https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN03_consolidada.pdf

[14] M. Arya Putra Pratama, Augustina Asih Rumanti, and Yudha Prambudia. 2024. Prioritizing Indicator of Knowledge Management Capability for Small Medium Industries (SMIs) Using an Analytical Hierarchy Process (AHP). In *Proceedings of the 2024 10th International Conference on Frontiers of Educational Technologies, ICFET 2024, Malacca, Malaysia, June 14-16, 2024*. ACM, https://doi.org/10.1145/3678392.3678415, 160–164. https://doi.org/10.1145/3678392.3678415

[15] MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. 2024. PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI), Versão 1.1.4. *PRESIDÊNCIA DA REPÚBLICA* 1 (2024), 1–178. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

[16] Lucas Dalle Rocha and Edna Dias Canedo. 2025. Optimizing Compliance: Comparative Study of Data Laws and Privacy Frameworks. *Journal of Internet Services and Applications* 16, 1 (Jul. 2025), 431–452. https://doi.org/10.5753/jisa.2025.5247

[17] Lucas Dalle Rocha, Geovana Ramos Sousa Silva, and Edna Dias Canedo. 2023. Privacy Compliance in Software Development: A Guide to Implementing the LGPD Principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023, Tallinn, Estonia, March 27-31, 2023*, Jiman Hong, Maart Lanperne, Juw Won Park, Tomás Cerný, and Hossain Shahriar (Eds.). ACM, https://doi.org/10.1145/3555776.3577615, 1352–1361. https://doi.org/10.1145/3555776.3577615

[18] Marco Saltarella, Giuseppe Desolda, Rosa Lanzilotti, and Vita Santa Barletta. 2024. Translating Privacy Design Principles Into Human-Centered Software Lifecycle: A Literature Review. *Int. J. Hum. Comput. Interact.* 40, 17 (2024), 4465–4483. https://doi.org/10.1080/10447318.2023.2219964

[19] Stefano Spósito, Fernando Moreira, and Edna Canedo. 2025. Designing a Training Journey for Privacy and Information Security Practitioners in the Federal Public Administration. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação* (Recife/PE). SBC, Porto Alegre, RS, Brasil, 95–104. https://doi.org/10.5753/sbsi.2025.246040

[20] Stefano Luppi Spósito, João Francisco Gomes Targino, Geovana Ramos Sousa Silva, Laerte Peotta, Daniel de Paula Porto, Fábio Lúcio Lopes Mendonça, and Edna Dias Canedo. 2025. A Comprehensive Review of Techniques, Methods, Processes, Frameworks, and Tools for Privacy Requirements. *Journal of Internet Services and Applications* 16, 1 (Aug. 2025), 508–529. https://doi.org/10.5753/jisa.2025.5252

[21] Lídia Tomaz, Patrícia Oliveira, and Éder Gualberto. 2024. Investigação da ferramenta Keycloak na Mitigação de Incidentes Cibernéticos: Uma Abordagem Integrada com o Programa de Privacidade e Segurança da Informação (PPSI). In *Anais Estendidos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais* (São José dos Campos/SP). SBC, Porto Alegre, RS, Brasil, 201–204. https://doi.org/10.5753/sbseg_estendido.2024.243301

[22] European Union. 2018. General Data Protection Regulation (GDPR). *Intersoft Consulting, Accessed on October 24, 2019* 1, 1 (2018), 1–100. https://gdpr-info.eu/

[23] Claes Wohlin, Per Runeson, Martin Höst, Magnus C. Ohlsson, Björn Regnell, and Anders Wesslén. 2012. *Experimentation in Software Engineering*. Springer, https://doi.org/10.1007/978-3-642-29044-2. https://doi.org/10.1007/978-3-642-29044-2