Designing a Training Journey for Privacy and Information Security Practitioners in the Federal Public Administration

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

Fernando Rocha Moreira
University of Brasília (UnB)
Brasília–DF, Brazil
frochamoreira@gmail.com

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

Abstract

Context: The Ministry of Management and Innovation in Public Services (MGI) leads the formulation and coordination of the Digital Government Strategy (EGD). DEPSI, under the Secretariat of Digital Government (SGD), is responsible for the Privacy and Information Security Program (PPSI), which aims at data privacy, compliance, and institutional resilience. **Problem**: The culture of privacy and information security in the Federal Public Administration faces development challenges. Despite the PPSI, there is a lack of awareness initiatives, training, a clear strategy, best practices, and performance indicators. **Proposed Solution**: The proposal aims to develop a training journey for Practitioners working in roles related to privacy and information security, with the goal of identifying and promoting the best practices, skills, and competencies required for these roles. **IS Theory**: This study aligns with Organizational Information Processing Theory, providing mechanisms to help organizations adapt to regulatory uncertainties in privacy and security. **Method**: We employed a mixed approach, combining document analysis, a literature review, and a survey. Guidelines and standards were analyzed to map competencies and responsibilities, while the survey gathered practitioners' perceptions of the proposed training journey. **Summary of Results**: We identified the key profiles and their corresponding responsibilities, and proposed a personalized training journey. Survey results indicated that the journey meets Practitioners' expectations, being well-evaluated in terms of criteria and assigned weights. **Contributions and Impact in IS**: This work contributes by presenting a proposal for a Training Journey to assess the knowledge of Federal Public Administration employees and guide them on the best paths for professional development.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**; **Privacy protections**.

Keywords

Privacy, Information Security, Competencies, Criteria, Training Journey

1 Introduction

Privacy has become a significant concern for governments and technology companies worldwide. As the provision of digital services expands, various aspects of users' lives are transformed into data collected and processed by countless information systems. Organizations that handle personal data are increasingly pressured by their users, employees, and various stakeholders to build systems that respect individuals' right to privacy [1]. These demands are accompanied by a new wave of privacy legislation. Over the past decade, countries across all major regions of the world have enacted data protection laws, bringing the total number of countries with such regulations to 157 by mid-March 2022 [14].

Privacy and information security managers are often responsible for designing, managing, testing, and implementing a range of technical and organizational controls necessary to ensure regulatory compliance. Therefore, it is essential that they not only fully understand the significance of privacy and security issues but also possess knowledge of existing privacy laws and standards [4]. However, the interpretation of legal documents tends to be vague, making it challenging to translate these legal requirements into concrete engineering practices [12].

The Brazilian General Data Protection Law, known as LGPD (Law 13.709/2018), came into effect in August 2020. It consists of ten chapters and 65 articles addressing control measures, compliance evidence, rights, and obligations related to the processing of personal data [8]. According to Article 3, the law applies to any data processing operation aimed at offering or providing goods or services or processing data of individuals located within Brazilian territory [7].

Failure to comply with the law can result in severe penalties, subjecting violators to the following administrative sanctions imposed by the National Data Protection Authority (ANPD), as outlined in Article 52: warnings; simple fines (2% of the revenue from the last financial year, capped at fifty million reals per violation); daily fines; publication of the violation; blocking and/or deletion of the personal data involved; partial suspension of database operations; suspension of data processing activities; and complete prohibition of business activities related to data processing [7].

Many of the proposed approaches to mitigate or clarify the specifications of legal requirements are inadequate for addressing legal ambiguities, which are common in laws and regulations [23]. These approaches often fail to quickly rewrite legal texts and require interpretation to resolve any ambiguities that may arise in the existing legislation or regulations [22]. Managers and practitioners in the ICT field bring different, and sometimes conflicting, perspectives to the interpretation of legal texts, and in some cases, they may not fully grasp all the principles of the LGPD [5, 32]. Therefore, they need models to support compliance with the LGPD [2].

Privacy Engineering addresses the gap between legislation, research, and practice, emerging as a field focused on the design, implementation, adaptation, and evaluation of theories, methods, techniques, and tools to systematically capture and address privacy issues in the development of sociotechnical systems [15]. According to Stallings [35], privacy engineering encompasses the technical

capabilities and management processes necessary to implement, deploy, and operate privacy resources and controls in functioning systems. Examples of privacy resources include privacy notices, consent management platforms, transparency tools (such as privacy dashboards), data portability mechanisms, and data deletion mechanisms (the right to be forgotten).

Many studies have addressed privacy from the perspective of software practitioners, particularly through interview-based research that allows for an in-depth understanding of practitioners' opinions and industry practices [4, 5, 10, 29, 30]. These studies often emphasize practitioners' perceptions of privacy and personal factors. Other research focuses on the privacy perspectives of specific roles, such as application developers [3, 11, 20]. However, there are still significant gaps in the research, such as the lack of studies emphasizing the importance of privacy and information security culture, as well as the adoption of concrete training practices for practitioners dealing with privacy laws in the industry.

In this context, the aim of this research is to explore this gap by investigating how organizational culture influences the understanding and practice of privacy and information security. This study stands out for its originality in integrating cultural and practical aspects, proposing a model that not only analyzes norms, guidelines, best practices, and legislation but also recommends strategies for training practitioners working in the field of privacy and information security.

The relevance of this work lies in the increasing importance of privacy legislation and the necessity of ensuring that practitioners in the field possess the knowledge and skills required to implement effective data protection and information security practices. By addressing these issues, the research not only contributes to the existing literature but also provides practical insights that can be applied in the training of practitioners and the enhancement of privacy and information security policies in Brazilian organizations.

2 Background and Related Work

Privacy is a process of boundary regulation, where individuals adjust their accessibility along a spectrum of openness and closeness depending on the context [18]. User privacy can be understood as the right to decide when, how, and for what purpose their personal information is shared with others or organizations [18]. However, as Nissenbaum points out [27], privacy cannot be defined in absolute terms because it holds different meanings for each individual, and privacy expectations are strongly tied to the context in which it is applied. Furthermore, defining an appropriate profile for a data privacy practitioner also depends on the context and the applicable legislation.

The General Data Protection Law (LGPD) [7] outlines specific roles for practitioners working in the field of data privacy, namely: Controller, Processor, and Data Protection Officer (DPO). Mello and Miramontes [24] presented the legal definitions, duties, and responsibilities of the Controller, Processor, and Data Protection Officer, along with an introduction to the National Data Protection Authority (ANPD), which serves as the regulatory and interpretive body of the LGPD.

Evandro et al. [9] explored the application of the General Data Protection Law in Brazil and how companies are adapting to ensure compliance with the law's guidelines. The authors proposed a framework to support Information and Communication Technology (ICT) practitioners in implementing LGPD principles within organizations. They also conducted a survey with Brazilian ICT practitioners regarding their organizations' compliance with the LGPD, revealing weaknesses in data privacy management and information security methodologies across various companies.

Rocha et al. [33] investigated the challenges faced by software practitioners in Brazil when implementing the principles of the General Data Protection Law. The authors identified the main difficulties that hinder developers from applying privacy requirements and ensuring compliance with the LGPD in software applications. They proposed a reference guide to support ICT practitioners in implementing the law's principles.

Iwaya et al. [17] explored the perspectives, mindsets, and privacy practices used by software practitioners, as well as organizational aspects related to data privacy. The authors conducted interviews with 30 software practitioners from nine countries, qualitatively analyzing the responses through thematic analysis to develop a privacy engineering framework. They identified three interconnected themes: 1) Practitioners' personal privacy mindset and posture, categorized into knowledge, attitudes, and behaviors; 2) Organizational privacy aspects, including decision-making power and examples of privacy climate; and 3) Privacy engineering practices, focusing on procedures and controls used in the industry. The authors emphasized the positive impact of privacy laws, such as the GDPR, on practitioners' behavior and organizational culture. Moreover, organizational culture strongly influences privacy practices. The results suggest that fostering a conducive environment for privacy engineering depends on aligning the privacy values of practitioners with those of their organizations, with support from leadership and top management. Organizations should also promote education and training on privacy methods and tools.

Peixoto et al. [30] investigated developers' level of knowledge and understanding of privacy, focusing on personal, behavioral, and external environmental factors that influence their decision-making regarding privacy requirements. The authors conducted semi-structured interviews with thirteen practitioners from six companies and identified nine personal factors, five behavioral factors, and seven external environmental factors that shape developers' decisions about privacy. Among the key factors identified were the lack of knowledge about privacy laws, the lack of understanding of information privacy concepts, and the inability to distinguish between privacy and security concepts.

According to related studies, several challenges still remain regarding the implementation of the LGPD, as well as in the training of practitioners working in this area. Most studies indicate that practitioners lack knowledge about both privacy and privacy laws. Moreover, there are organizational weaknesses in developing and applying data privacy management and information security methodologies in Brazilian organizations, particularly within federal public administration agencies. These weaknesses, combined with the lack of practical guidance from academia and industry concerning the roles defined by the LGPD, highlight the need for a methodology to support the individual and organizational training

of practitioners working in data privacy and information security, particularly Controllers, Processors, Data Protection Officers, and Information Security Managers.

3 Study Settings

This study aims to create a training journey model for practitioners working in the field of data privacy and information security. To achieve our objective, we conducted a literature review to identify the criteria, sub-criteria, competencies, and qualifications that these practitioners need to acquire in order to fulfill their roles. Additionally, we developed a quantitative evaluation model to assess whether a practitioners is qualified to perform this role based on the identified criteria. Therefore, this research has an applied nature as it seeks to solve specific problems, namely, the creation of a training journey for practitioners working in data privacy and information security. Specifically, we will present the proposed training journey for the role of the Data Protection Officer (DPO).

This research also has an exploratory nature [13], as we conducted a literature review, a case study with privacy practitioners, and applied a survey to gather their perceptions regarding the proposed model. Therefore, this research employs both qualitative and quantitative approaches. The qualitative approach enabled the classification of the criteria, sub-criteria, competencies, and qualifications needed to perform the role's functions, while the quantitative approach was used for the statistical analysis of the survey data [21]. Figure 1 presents the methodology adopted to conduct this research.

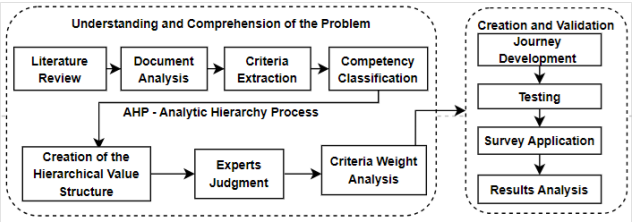


Figure 1: Methodology adopted to conduct this research

In the Literature Review phase (Figure 1), a literature review was conducted to identify documents containing information related to the qualifications and competencies required for privacy practitioners. The analyzed documents included standards, guidelines, laws, regulations, government official documents, and judgments.

In the Document Analysis phase (Figure 1), the documents were thoroughly reviewed by two researchers to identify procedures, qualifications, best practices, competencies, skills, and internal policies related to the roles of practitioners working in privacy and information security. During the Criteria Extraction and Sub-criteria (Figure 1) for the training journey phase, a detailed review and analysis of standards, laws, regulations, guides, decrees, official government documents, and judgments were conducted. These documents provided the necessary parameters to define the curriculum content, skills, and competencies required for practitioners to assume their roles. The criteria were used to guide the training journey, covering technical, legal, and operational aspects, along with sub-criteria that detailed the specific competencies required for each role.

The Competency Classification phase (Figure 1) concludes the problem diagnosis, that is, the understanding and comprehension of the issue. As a result of this phase, the criteria and sub-criteria were classified. Additionally, the skills and competencies were labeled according to the complexity level of the skills/qualifications, being categorized as: Beginner, Basic, Intermediate, Advanced, and Expert. In the Creation of the Hierarchical Value Structure phase (Figure 1), we began the block for applying the Analytic Hierarchy Process (AHP). The problem was transformed into a hierarchical structure containing the criteria and their respective sub-criteria. The skills and competencies/qualifications were transformed into sub-criteria. This structure is one of the prerequisites for applying AHP [34].

After the creation of the Hierarchical Value Structure based on standards, laws, guidelines, regulations, decrees, official documents, and judgments, experts with expertise in data protection and legal compliance were invited to assign weights and priorities to each criterion and sub-criterion (Experts Judgment, Figure 1). With the support of AHP, the experts compared the criteria and sub-criteria pairwise, evaluating the relative importance of each in relation to the others, considering aspects such as legal compliance, technical capability, governance, and accountability in handling personal data [34].

To perform the pairwise comparison, the experts used Saaty's scale [34]. This phase (Criteria Weight Analysis, Figure 1) is important because it is through the experts' judgment that AHP calculates the weights of the criteria and sub-criteria, which will later be assessed in the proposed training journey. Based on this judgment, it was possible to determine the relevance of each criterion for proposing the training journey. After calculating the weights using AHP, a consistency index analysis was conducted. This index measures how consistent the experts' judgment was, concluding the AHP application phase [34].

In the Journey Development phase (Figure 1), we began the Model Creation and Validation block. After analyzing the weights of the criteria, we proposed the training journey. The criteria and sub-criteria, along with their respective weights, became indicators. Thus, as the employee completes the training and progresses through their journey, the criteria and sub-criteria will be met, and their respective weights will accumulate, generating a final index. The passing grade for each criterion and sub-criterion is 60% for the practitioner to be approved.

In the Testing phase (Figure 1), we conducted a simulation of the proposed training journey with federal public administration employees who work as data protection officers, data controllers, and information security managers. Through this case study, we validated the proposed training journey model to verify whether the AHP weights and the proposed model were able to transform the qualitative information provided by the participants into quantitative values (percentage of knowledge level).

In the Survey Application phase (Figure 1), we conducted a survey during a postgraduate course session for employees of federal public administration agencies (part of the Privacy and Information Security training program), with the goal of gathering the perceptions of practitioners working in privacy and information security regarding the proposed Training Journey model. The survey

consisted of 7 closed-ended questions and 1 open-ended question, totaling 8 questions. All questions and their respective answer options are available at Zenodo. A total of 22 practitioners participating in the training course responded to the survey. Finally, in the Results Analysis (Figure 1), we analyzed the survey responses both quantitatively and qualitatively and refined the model based on the suggested improvements.

4 Results

In the literature review conducted, 48 documents containing guidelines on Information Security and Privacy skills and competencies, provided by the government, were identified. Of these, 18 documents are related to privacy and the profiles described by the General Data Protection Law (LGPD), while 30 documents pertain to Information Security and their respective profiles according to regulations. Figure 2 shows the respective percentages of the types of documents analyzed/cataloged. Of the identified documents, 59.5% are guides and guidelines, while 11.9% are international technical standards.

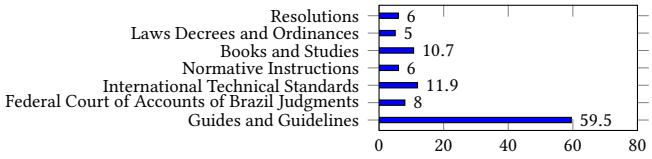


Figure 2: Distribution of Guidance Sources (%)

It is worth highlighting that some documents were particularly important in the extraction of criteria, competencies, skills/qualifications, and responsibilities. Among them are the regulations and guides from the National Data Protection Authority (ANPD), the LGPD, and the Privacy and Information Security Program (PPSI). Table 1 presents the amount of data extracted from 18 documents for the proposed training journey for the Data Protection Officer. Based

Table 1: Information Extracted from the Documents

Topic	Quantity	Sources
Responsibilities	95	LGPD, PPSI, ANPD
Skills	29	PPSI
Principles	9	LGPD

on the information extracted from the documents presented in Table 1, we held several meetings with the managers of the Secretariat of Digital Government (SGD) to define the criteria to be used in creating the Data Protection Officer's Training Journey. After several analyses by the three researchers and the managers, a consensus was reached, and the following criteria were established: Professional Training, Academic Education, Language Certification, Professional Certification, Competencies, and Skills.

The Professional Training criterion was chosen due to the specific competencies found in the documents (Table 1). These documents require the practitioner to have experience in the field and knowledge to handle the technical terms inherent to the Data Protection Officer's profile. As a result, Years of Experience and Time in Role became subcriteria under Professional Training. The Academic Education criterion was chosen because the practitioner is required to hold a bachelor's degree or a postgraduate qualification in the relevant field. Therefore, Bachelor's Degree and Postgraduate Degree were established as subcriteria under Academic Education.

Regarding the Language Proficiency criterion, it was chosen due to the number of articles, ISOs [16], technical standards, and the GDPR [28] being written in other languages. As for the Professional Certification criterion, it was selected because it serves as a strong reference in the job market, and there are already certification organizations that offer exams focused on the LGPD and Data Protection. The Competencies criterion had each of its skills grouped according to their themes and were classified into six subcriteria: Knowledge in Information Technology, Privacy By Design, Privacy Strategy, Legislations, Guidance Documents and Risk Management and Compliance. Each of the competencies in these subcriteria was labeled according to its complexity and difficulty, which will serve as a guide for the future Data Protection Officer to know where to start their journey or even complement their professional development. The labels are: Beginner, Basic, Intermediate, Advanced, and Expert. The following Tables 2, 3, 4, 5, 6, 7 partially presents the competencies related to the six subcriteria mentioned earlier, the complete table with all skills is available at https://zenodo.org/records/15008980. Regarding the Knowledge in Information Technology skills, Table 2 presents the 7 competencies and qualifications related to the theme.

Table 2: Knowledge in Information Technology

Level	Skills
Beginner	Basics of IT and Information Systems [25]
	Concepts of Privacy and Security in IT
	Data Storage Basics
Basic	Access Management and Authentication
	Basic Knowledge of Cloud Data Storage
Intermediate	Systems Monitoring and Auditing
	Data Loss Prevention

Regarding the Privacy By Design sub-criterion, we identified 12 competencies required for the Data Protection Officer, as shown partially in Table 3.

Table 3: Privacy By Design

Level	Skills
Beginner	Privacy Principles
	Notions of Compliance with Privacy Regulations
Basic	Basic Implementation of Privacy by Default
	Integration of Privacy by Design in Simple Projects
	Documentation and Compliance Evidence
Intermediate	Privacy Impact Assessment with a focus on Privacy by Design
	Data Management and Minimization
Advanced	Development of System Architectures with Privacy by Design
	Privacy-Focused Threat Modeling

In the sub-criterion Privacy Strategies, we identified 35 skills, as shown partially in Table 4.

In the documents regarding laws and data privacy legislation, we identified 35 skills, as shown partially in Table 5.

Through an analysis of Guidance Documents created by National Data Protection Authority (ANPD) and Secretariat of Digital

Table 4: Privacy Strategies

Level	Skills
Beginner	Basic Concepts of Privacy
	Notions of Privacy and Data Protection
Basic	Consent Management
	Data Mapping and Personal Data Inventory
Intermediate	Anonymization and Pseudonymization
	Data Lifecycle Management
	Privacy Governance Models
Advanced	Privacy Education and Culture in the Organization
	Privacy Incident Resolution
Expert	Privacy Tool Evaluation Criteria [26]
	Corporate Social Responsibility and Transparency

Table 5: Legislations

Level	Skills
Beginner	LGPD Basic Notions [7]
	Principles of the Access to Information Law [6]
Basic	Compliance with LGPD and its Obligations [7]
	Confidential and Personal Information [7]
Intermediate	Data Retention and Deletion Policy [7]
	Incident Notification Obligations [7]
Advanced	ISO 29100 – Information Privacy Framework [16]
	ISO 27701 – Information Privacy Management [19]
Expert	Knowledge about the General Data Protection Regulation (GDPR) [28]

Government (SGD), we were able to identify 27 skills related to the respective documents, as shown partially in Table 6.

Table 6: Guidance Documents

Level	Skills
Beginner	Knowledge of General Privacy and Security Structuring Requirements
Basic	Knowledge about the PPSI Framework Maturity Indicators
	Knowledge of the PPSI Framework Cybersecurity Controls
Intermediate	Knowledge about the Privacy by Design and Default Guide
Advanced	Knowledge about Data Protection and Electoral Legislation in Practice

In the sub-criterion Privacy Strategies, we identified 18 skills, as shown partially in Table 7.

Table 7: Risk Management and Compliance

Level	Skills
Beginner	Privacy Incident Management
	Compliance Fundamentals
Basic	Privacy Risk Management
	Privacy Leadership
Intermediate	Risk-Based Decision Making
	Execution of Operational Risk Analysis
	Implementation of LGPD Compliance Programs
Advanced	Integrating Privacy with Business Strategy
	Continuous Risk and Compliance Monitoring
Expert	Data Governance and Corporate Privacy Strategy
	Relationship with Regulators

Based on the criteria and sub-criteria identified in the analyzed documents, we constructed a value hierarchy structure to apply the AHP. This structure represents the criteria (Experience, Academic Background, Language Proficiency, Professional Certification, Competencies) and sub-criteria (Work Experience, Job Experience, Undergraduate, Postgraduate, Beginner, Intermediate, Advanced, Expert, IT Knowledge, Privacy by Design, Privacy Strategies, Legislations, Guidance Documents, Risk Management and Compliance). These criteria and sub-criteria were adopted to propose the Data Protection Officer training journey based on the judgments made by privacy experts, as shown in Figure 3.

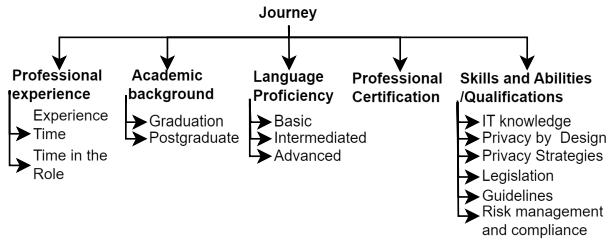


Figure 3: Hierarchical Structure of Criteria and Sub-criteria

Once the construction of the final hierarchical value structure was completed, we proceeded to evaluate the criteria and sub-criteria using pairwise comparison [34]. The results of the comparison of the criteria and sub-criteria are presented in Table 8. The consistency index of this comparison was 8%, which is below the 10% recommended by the AHP method. After the evaluation/assessment of the criteria by the experts, the corresponding weights were assigned to each of them, as shown in Figure 4.

Table 8: Evaluation of the Criteria and Sub-criteria for the Proposed Training Journey

Sub-criteria for Competencies and Skills / Qualifications					
Criteria	**Academic Background**	**Professional Background**	**Language Proficiency**	**Professional Certification**	**Competencies and Skills / Qualifications**
Academic Background	x	⇑ 5	⇐ 3	⇑ 7	⇑ 7
Professional Background	x	x	5	⇑ 3	⇑ 5
Language Proficiency	x	x	x	⇑ 7	⇑ 9
Professional Certification	x	x	x	x	⇑ 3
Competencies and Skills / Qualifications	x	x	x	x	x

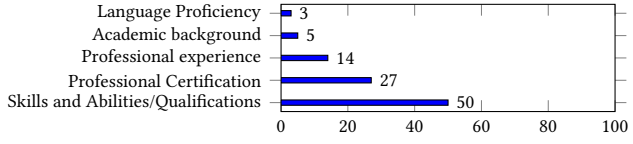


Figure 4: Weights of the criteria after the experts' assessment

Regarding the Professional Experience/Education criterion, the sub-criterion Experience Time (75) was judged by the experts as moderately more important than Time in the Role (25), meaning that the former holds a value three times more important on the quantitative scale. The consistency index for this judgment was 0%,

below the 10% recommended by the AHP method. The Language Proficiency criterion was also evaluated by the privacy experts. Table 9 shows the classification assigned to this criterion. The consistency index for this judgment was 2%, below the 10% recommended by the AHP method.

Table 9: Evaluation of the Language Proficiency Criterion by the Experts

Language Proficiency Criterion			
Certification	**Basic**	**Intermediate**	**Advanced**
Basic	X	⇑ 2	⇑ 3
Intermediate	X	X	1
Advanced	X	X	X

In the Academic Background criterion, the experts rated the Bachelor's degree (66) sub-criterion as moderately more important than the Postgraduate degree (33) sub-criterion, which corresponds to a score of 2. The consistency index of this judgment was 0%, well below the 10% recommended by the AHP method.

The judgment of the weights assigned by privacy experts to the subcriteria of Competencies and Skills/Qualifications is presented in Table 10. The consistency ratio of this judgment was 3%, which is below the 10% threshold recommended by the AHP method.

Table 10: Evaluation of the Language Proficiency Criterion by Experts

Competencies and Qualifications Criterion						
Subcriteria	**Knowledge in IT**	**Privacy Strategies**	**Privacy by Design**	**Legislations**	**Guidance Documents**	**Risk Management and Compliance**
Knowledge in IT	x	⇑ 5	⇑ 5	⇑ 7	⇑ 5	⇑ 5
Privacy Strategies	x	x	1	⇑ 3	⇑ 4	⇑ 3
Privacy by Design	x	x	x	⇑ 3	⇑ 6	⇑ 2
Legislations	x	x	x	x	1	⇐ 6
Guidance Documents	x	x	x	x	x	⇐ 5
Risk Management and Compliance	x	x	x	x	x	x

The Figure 5 presents the global weights of the subcriteria used in the proposed model to calculate the training journey of the Data Protection Officer. After defining all the weights for the criteria and

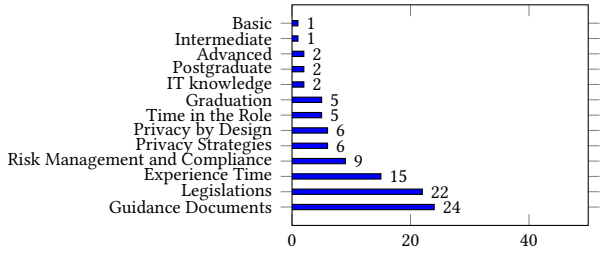


Figure 5: Global Distribution of Subcriteria Weights

subcriteria, we inserted the values into the proposed model. Figure 6 (a) presents the proposed model. It is worth noting that the fields highlighted in red represent the weights of the criteria, the fields highlighted in orange represent the weights of the subcriteria, the fields highlighted in blue represent the score of the practitioner who conducted the assessment, and the fields highlighted in green represent the actual score of the item provided by the practitioner. If the privacy practitioner has a score higher than the weight of a criterion or sub-criterion, the model will only consider the maximum value of the criterion.

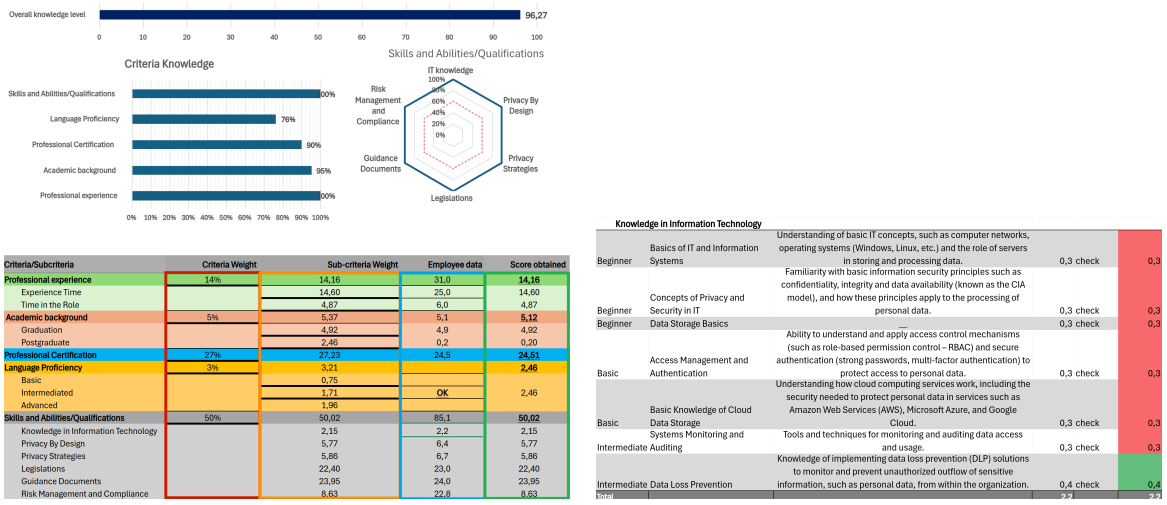
Figure 6 (b) shows the calculation of the score for the Competencies and Skills/Qualifications criterion, based on the levels and competencies presented in Tables 2, 3, 4, and 5. As the practitioner performs the assessment of their competencies, a radar chart is generated, highlighting the areas where the Data Protection Officer needs to improve their knowledge and skills (Figure 6). The required competencies for the privacy practitioner have specific weights, and the competencies that the Data Protection Officer reports not possessing during the assessment will be marked with a dark red color, as shown in Figure 6. The color scale was defined according to the weight assigned to each competency.

The dashboard shown in Figure (a) 6 also includes two additional bar charts. The top bar chart displays the calculated percentage of the overall score for the entire assessment (diagnostic) completed by the Data Protection Officer (DPO). The score is calculated by summing the scores of all the subcriteria. The bar chart in the lower-left corner, containing five bars, shows the score for each criterion. For the Data Protection Officer to be considered qualified to take on the responsibilities of the position, they must have a score of 60% or lower for each criterion and sub-criterion in the proposed training journey.

It is important to note that the values presented in Figure 6 is a simulation involving a data privacy practitioner who wishes to take on the role of Data Protection Officer in a federal public administration agency. In this evaluation, it became evident that the practitioner needs to obtain certain professional certifications to assume this role. In the Competencies and Skills/Qualifications criterion, the practitioner achieved the necessary score to be approved and take on the Data Protection Officer role. However, the subcriteria Privacy by Design and Privacy Strategies fell below the desired 60% threshold. This result indicates that the practitioner needs to improve their knowledge in key areas to perform this function effectively. A full simulation of the data protection officer assessment/diagnosis, along with the values for criteria such as competencies and skills/qualifications, is available at Zenodo.

4.1 Survey Results

During the class on Privacy Management and Personal Data Protection, we presented the proposed model of the Training Journey to the students. We explained the entire process of constructing the proposal, from the analysis of documents to the definition of weights using AHP. The presentation was delivered by the three authors of this paper, and course participants asked questions about the development of the work, as well as the expectations of the federal public administration regarding the mandatory training journey for all agency members. After the presentation and addressing any possible doubts, we conducted a simulation of the proposal with the students, gathering their skills and competencies to assess their knowledge level regarding the abilities needed to perform the role of Data Protection Officer or Information Security Manager. Following the simulations and necessary adjustments to



Criteria/Subcriteria	Criteria Weight	Sub-criteria Weight	Employee data	Score obtained
Professional experience	14%	14,16	31,0	14,16
Experience Time		14,60	25,0	14,60
Time in the Role		4,87	6,0	4,87
Academic background	5%	5,37	5,1	5,12
Graduation		4,92	4,9	4,92
Postgraduate		2,46	0,2	0,20
Professional Certification	27%	27,23	24,5	24,51
Language Proficiency	3%	3,21		2,46
Basic		0,75		
Intermediated		1,71	OK	2,46
Advanced		1,96		
Skills and Abilities/Qualifications	50%	50,02	85,1	50,02
Knowledge in Information Technology		2,15	2,2	2,15
Privacy By Design		5,77	6,4	5,77
Privacy Strategies		5,86	6,7	5,86
Legislations		22,40	23,0	22,40
Guidance Documents		23,95	24,0	23,95
Risk Management and Compliance		8,63	22,8	8,63

(a)

Knowledge in Information Technology				
Beginner	Basics of IT and Information Systems	Understanding of basic IT concepts, such as computer networks, operating systems (Windows, Linux, etc.) and the role of servers in storing and processing data.	0,3 check	0,3
Beginner	Concepts of Privacy and Security in IT	Familiarity with basic information security principles such as confidentiality, integrity and data availability (known as the CIA model), and how these principles apply to the processing of personal data.	0,3 check	0,3
Beginner	Data Storage Basics		0,3 check	0,3
Basic	Access Management and Authentication	Ability to understand and apply access control mechanisms (such as role-based permission control – RBAC) and secure authentication (strong passwords, multi-factor authentication) to protect access to personal data.	0,3 check	0,3
Basic	Basic Knowledge of Cloud Data Storage	Understanding how cloud computing services work, including the security needed to protect personal data in services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.	0,3 check	0,3
Intermediate	Systems Monitoring and Auditing	Tools and techniques for monitoring and auditing data access and usage.	0,3 check	0,3
Intermediate	Data Loss Prevention	Knowledge of implementing data loss prevention (DLP) solutions to monitor and prevent unauthorized outflow of sensitive information, such as personal data, from within the organization.	0,4 check	0,4
Total			2,7	2,7

(b)

Figure 6: Figure (a) shows the simulation of the DPO Assessment/Diagnosis, while (b) shows values of the Criteria: Competencies and Skills/Qualifications.

the criteria and subcriteria, as well as their respective weights, we conducted a survey to gather their perceptions of the proposed model. Table 11 presents the participants' profiles. The survey was completed by 22 practitioners, all of whom work in federal public administration agencies. All responses from the survey are available at at Zenodo.

We asked the participants how they seek to develop the qualifications necessary to perform the role of Data Protection Officer, Data Controller, Data Processor, or Information Security Manager (Q7). 72.7% of the participants reported that they do so by taking courses offered by the National School of Public Administration (ENAP), the School of Tax Administration of Brazil (ESAF), the Virtual Learning Environment of the Federal Comptroller General's Office (CGU), the Brazilian Legislative Institute (ILB), Alura, and Udemy. 63.6% of them pursue training through seminars and undergraduate and postgraduate courses, respectively. 60% stated that they develop their skills through training programs, 59.1% through lectures, 54.5% through workshops, and 50% of the participants indicated that they engage in reading documents and guidelines.

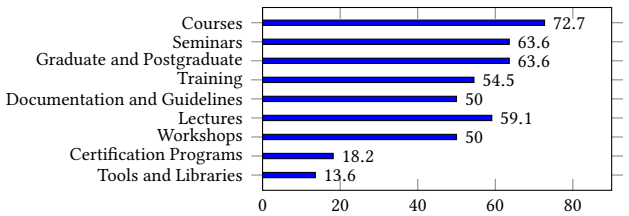


Figure 7: Methods for enhancing competencies and skills/qualifications

Practitioners Localization	%
Distrito Federal	45.5
Espirito Santo	4.5
Goiás	4.5
Minas Gerais	18.2
Rio de Janeiro	18.2
Tocantins	4.5
Role	%
Information Security Analyst	18.2
Information Security Manager	31.8
Data Protection Officer (DPO)	18.2
Manager of the Infrastructure and Information Security Division	4.5
Data Operator	27.3
Years Experience	%
>= 1	27.3
1-5	68.2
6-10	4.5
Education Level	%
Doctorate Degree	4.5
Master's Degree	36.4
Master Student	4.5
Postgraduate	54.5
Data Privacy Expertise	%
The group works (or worked) on privacy	54.5
I have experience working as a DPO, focusing on data privacy and compliance	22.7
I have never had direct or indirect experience with privacy, nor as a Data Protection Officer	22.7

Table 11: Practitioner Profile (n=22)

In Q8, we investigated the practitioners' perception of the methodology proposed for the training journey. During the class, we simulated the training journey for the profiles of the Data Protection

Officer (DPO) and the Information Security Manager. In the survey, we focused on the perception of the DPO profile to gather more targeted insights, and we believe that by validating the proposal for one profile, the training journey can be replicated for any other profile. 60% of the participants agreed or strongly agreed that the proposal is easy and simple to implement in order to assess the competencies, skills, and qualifications of practitioners wishing to act as DPOs (Q8a in Figure 8). 66.6% of the participants agreed or strongly agreed that the proposed methodology for training the DPO meets the needs to professionalize a practitioner aiming to take on this role (Q8b in Figure 8).

80% of the participants agreed or strongly agreed that the criteria and subcriteria used are relevant and effective for assessing the competencies, skills, and qualifications of practitioners intending to work as Data Protection Officers (Q8c in Figure 8). 60% of the participants strongly agreed or agreed that the competencies, skills, and qualifications identified in the literature are sufficient to assess the desired profile for the Data Protection Officers (Q8d in Figure 8). 66.6% of the participants strongly agreed or agreed that the classification of competencies, skills, and qualifications into levels: Beginner, Basic, Intermediate, Advanced, and Expert, along with their respective weights, effectively guide the practitioner in identifying the areas they need to specialize in to become a Data Protection Officers (Q8e in Figure 8).

73.3% of the participants strongly agreed or agreed that the distribution of weights given by privacy experts to the criteria and subcriteria for competencies, skills, and qualifications using AHP was done according to the needs of the desired profile for a Data Protection Officer (Q8f in Figure 8). 66.7% of the participants strongly agreed or agreed that the 60% threshold for the criteria and subcriteria is an acceptable value for assessing the level of knowledge required to perform the role of Data Protection Officer (Q8g in Figure 8). However, only 46.6% of the participants strongly agreed or agreed that the proposed methodology is capable of motivating and engaging the target audience to train and achieve the required score to perform the role of Data Protection Officer (Q8h in Figure 8). On the other hand, 46.7% of the participants strongly agreed or agreed that the proposed methodology for assessing the level of knowledge is fairer compared to other existing evaluation methods, which only take into account the exam score from a course or certification (Q8i in Figure 8).

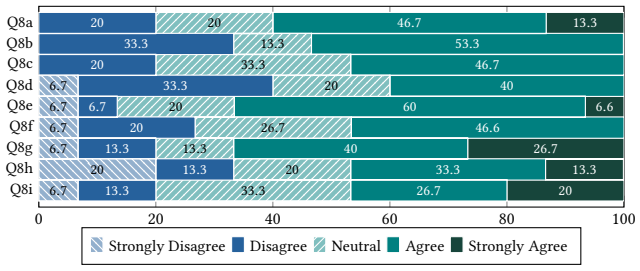


Figure 8: Practitioners' Perceptions

Regarding the open-ended question (Q9), all participants provided satisfactory comments on the proposal, and some suggested improvements or ways to promote it. Respondents #R4 and #R13 stated:

> *"The federal public administration should conduct multidisciplinary workshops to train practitioners, as well as use discussion groups (forums)."*

> *"I understand that the methodology serves as a guide for the Data Protection Officer to understand the necessary knowledge and begin their training journey, considering the levels of beginner, basic, intermediate, and advanced. I believe that the criteria related to the ICT area are set at a higher level than is practically needed. In this regard, I think that the more applicable knowledge would be related to information security, data management, and information security risks at the beginner and basic levels."*

Based on the results obtained from the survey, it is possible to conclude that the proposed training journey meets the expectations of practitioners working in privacy and information security within federal public administration agencies. Furthermore, it is likely that the training will be well-received by them as a tool for diagnosing the necessary competencies, skills, and qualifications required to take on the role of Data Protection Officer in any federal public administration agency.

5 Discussions

The results from the analysis of documents, legislation, guidelines, and standards enabled the creation of a training journey model for practitioners working in privacy and information security, in compliance with the General Data Protection Law (LGPD) and the related normative instructions. The findings highlight the important role that organizational culture plays in the acceptance and implementation of privacy and information security practices. The development of a privacy mindset through continuous training can transform how practitioners and organizations approach compliance with the LGPD and related information security guidelines.

The application of the Analytic Hierarchy Process method proved to be a robust approach for prioritizing criteria and sub-criteria related to the competencies, skills, and qualifications of practitioners working in privacy and information security. Ribeiro and Canedo [31] also used the Analytic Hierarchy Process method to select the best alternatives for implementing security criteria in a Federal public administration agency. The results showed that the Risks to Data Privacy criterion was the highest priority for the implementation of personal data security within the agency, as the main objective of the LGPD is to keep personal data private and accessible only to the data subject. Finally, the results highlight the need for a more proactive approach from organizations to ensure their practitioners are adequately trained to address the challenges of complying with privacy and information security laws, thereby reducing risks and penalties.

6 Threats to Validity

To ensure the reliability of the results, it is important to consider potential threats to the validity of the study. Based on Wohlin's model [36], we discuss the threats to internal, external, construct, and conclusion validity, and present the strategies implemented to mitigate them. **Threats to Internal Validity**: Subjectivity in

Weight Assignment – Although the Analytic Hierarchy Process is a robust decision-making technique, the assignment of weights to criteria can be subjective, depending on the interpretation of the researchers or expert group. This subjectivity may introduce bias, especially when there is no clear consensus on which qualifications are most important. To mitigate this threat, the weights were defined and assessed by multiple experts, and various simulations were conducted, covering different areas of knowledge. **Threats to External Validity**: Outdated Information and Lack of Context – The qualifications were defined based on legal documents, standards, and regulations. However, these sources may not align with current industry or public sector practices and requirements. Additionally, laws and regulations often have long review cycles, which may lead to outdated information. Criteria established in different legislative or regulatory contexts may therefore not reflect the specific needs of the data protection officer role. To mitigate this threat, we recommend that the proposed training journey model be regularly updated to ensure that the competencies and qualifications remain aligned with current demands.

Threats to Construct Validity: Definition and Measurement of Criteria – Construct validity may be threatened by how the concepts of competencies, skills, and qualifications were defined and measured in the model. If these concepts are not clearly operationalized, there may be a discrepancy between what the model intends to measure and what is actually measured. To mitigate this threat, normative documents and literature reviews were used to clearly define the criteria, along with consultations with field experts to validate the definitions. **Threats to Conclusion Validity**: Consistency of Results – Conclusion validity may be compromised if the obtained results are inconsistent or if there is significant variability in the interpretations of the experts. Additionally, the analysis could be susceptible to statistical errors or misinterpretations of the data. To reduce this threat, method triangulation was used, combining simulations, privacy expert analysis, and reviews of standards, which strengthens the robustness of the conclusions drawn. Another factor that may impact conclusion validity is related to the survey conducted with 21 practitioners in the privacy and information security field. Since the number of participants was relatively small, this may limit the generalization of the results to a broader context. Furthermore, the practitioners' perceptions may vary depending on their experiences and organizational profiles, which could influence their responses. To mitigate this threat, the responses were triangulated with other data sources, and the diversity of the participants' areas of expertise was considered in the analysis of the results.

7 Conclusions

The proposed model provides a strong foundation for training data protection officers in federal public administration agencies, ensuring practitioners possess the knowledge needed to support organizations in complying with data privacy laws. To maintain alignment with legislative updates, we recommend regular updates to the proposed model, tailored to each organization's needs, to ensure that data protection officers' skills and competencies remain current. By basing desired qualifications for practitioners on normative criteria, federal public administration can mitigate the risks of regulatory non-compliance while empowering data protection officers to operate effectively in a dynamic environment where continuous training and knowledge updates are essential. Although implementing the proposed model may face some resistance from practitioners or decision-makers, these guidelines can support practitioners in enhancing their competencies and skills by enabling self-assessment of their knowledge against the requirements needed for the role of data protection officer. Additionally, the criteria derived from the literature serve both as tools for regulatory adherence and as a framework for ongoing professional development. This approach helps identify areas for growth, encourages further training, and adapts officers' profiles to organizational changes and data privacy legislation updates.

In tests conducted with practitioners in privacy and security, the model proved efficient and aligned with the necessary skills, as the assigned weights successfully highlighted each professional's strengths and areas for improvement in relation to the requirements for the role of data protection officer. The proposed model provided a detailed overview of mastered competencies and areas needing enhancement, emphasizing its practical applicability in both public and private organizations. Therefore, the model serves as a tool to support practitioners in developing the skills needed to meet legal standards in privacy, data protection, and information security. Furthermore, it contributes to discussions on Information Systems Perspectives and Trends in Government and Education by offering a framework to identify and classify essential data protection and information security competencies. This approach enhances the effectiveness of information management, particularly in areas that handle critical and sensitive government data.

Implementing this model can significantly enhance data quality, information security, and regulatory compliance, fostering a culture of responsibility and ethics in information system use. It promotes innovative and adaptive practices to meet the evolving demands of various sectors, equipping public and private organizations to address current and future information management challenges. Furthermore, this evaluation model for data protection officer qualifications and competencies aligns closely with Brazil's Major Research Challenges in Information Systems for 2016-2026, particularly in privacy and information security. These challenges highlight the need for solutions that ensure data integrity and enable efficient information management amid rapid digital transformation.

Data Availability

The materials produced during the research, including the survey form and the file containing all the survey responses, are available at https://zenodo.org/records/15008980.

Acknowledgments

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.

References

[1] Vinicius Camargo Andrade, Richard D. Ribeiro, Rafael dos Passos Canteri, Sheila S. Reinehr, Cinthia O. de A. Freitas, and Andreia Malucelli. 2024. Privacy in Practice: Exploring Concrete Relationships Between Privacy Patterns and Privacy by Design Principles in Software Engineering. In *27th Iberoamerican Conference on Software Engineering, CIbSE 2024, Curitiba, Brazil, May 6-10, 2024*. Curran Associates, https://doi.org/10.5753/cibse.2024.28453, 271–285. https://doi.org/10.5753/CIBSE.2024.28453

[2] Eric Araújo, Jéssyka Vilela, Carla Silva, and Carina Alves. 2021. Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD aware Business Processes. In *SBSI 2021: XVII Brazilian Symposium on Information Systems, Uberlândia, Brazil, June 7 - 10, 2021*. ACM, https://doi.org/10.1145/3466933.3466982, 46:1–46:9.

[3] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Faith Cranor. 2014. The privacy and security behaviors of smartphone app developers. In *Workshop on Usable Security*. Citeseer, Workshop on Usable Security, Workshop on Usable Security, 1–10.

[4] Edna Dias Canedo, Ian Nery Bandeira, Angélica Toffano Seidel Calazans, Pedro Henrique Teixeira Costa, Emille Catarine Rodrigues Cançado, and Rodrigo Bonifácio. 2023. Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. *Requir. Eng.* 28, 2 (2023), 177–194. https://doi.org/10.1007/S00766-022-00382-8

[5] Edna Dias Canedo, Angélica Toffano Seidel Calazans, Anderson Jefferson Cerqueira, Pedro Henrique Teixeira Costa, and Eloisa Toffano Seidel Masson. 2021. Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil. In *29th IEEE International Requirements Engineering Conference, RE 2021, Notre Dame, IN, USA, September 20-24, 2021*. IEEE, https://doi.org/10.1109/RE51729.2021.00013, 58–69. https://doi.org/10.1109/RE51729.2021.00013

[6] Nartional Congress da República, Presidência. 2011. Brazilian Acess to Information Law (LAI). *Nartional Congress* 1, 1 (2011), 1. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

[7] Nartional Congress da República, Presidência. 2018. Brazilian General Data Protection Law (LGPD). *Nartional Congress, accessed in April 10, 2022* 1, 1 (2018), 1–31. https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

[8] Evandro Thalles Vale de Castro, Geovana R. S. Silva, and Edna Dias Canedo. 2022. Ensuring privacy in the application of the Brazilian general data protection law (LGPD). In *SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, April 25 - 29, 2022*. ACM, https://doi.org/10.1145/3477314.3507023, 1228–1235. https://doi.org/10.1145/3477314.3507023

[9] Evandro Thalles Vale de Castro, Geovana R. S. Silva, and Edna Dias Canedo. 2022. Ensuring privacy in the application of the Brazilian general data protection law (LGPD). In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing* (Virtual Event) *(SAC '22)*. Association for Computing Machinery, New York, NY, USA, 1228–1235. https://doi.org/10.1145/3477314.3507023

[10] Ruy Ovídio Perrelli de Melo, Jéssyka Vilela, and Carla Silva. 2024. Do Entendimento à Aplicação: Requisitos de Privacidade e a Visão dos Usuários sobre a LGPD. In *Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024*. Even3, Brasil, https://doi.org/10.29327/1407529.27-27, 1–8.

[11] Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek. 2023. How Can We Design Privacy-Friendly Apps for Children? Using a Research through Design Process to Understand Developers' Needs and Challenges. *Proc. ACM Hum. Comput. Interact.* 7, CSCW2 (2023), 1–29. https://doi.org/10.1145/3610066

[12] Sâmmara Éllen Renner Ferrão, Geovana Ramos Sousa Silva, Edna Dias Canedo, and Fabiana Freitas Mendes. 2024. Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. *Inf. Softw. Technol.* 168 (2024), 107396. https://doi.org/10.1016/J.INFSOF.2024.107396

[13] Antonio C. Gil. 1991. *Métodos e técnicas de pesquisa social.* Atlas, São Paulo.

[14] Graham Greenleaf. 2022. Now 157 Countries: Twelve Data Privacy Laws in 2021/22. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4137418#paper-references-widget [Online; accessed 10. Oct. 2024].

[15] Seda Gurses and José M. del Álamo. 2016. Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Secur. Priv.* 14, 2 (2016), 40–46. https://doi.org/10.1109/MSP.2016.37

[16] ISO/IEC. 2011. ISO/IEC 29100:2011 Information Technology - Security techniques - Privacy Framework.

[17] Leonardo Horn Iwaya, Muhammad Ali Babar, and Awais Rashid. 2023. Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices. *IEEE Trans. Software Eng.* 49, 9 (2023), 4324–4348. https://doi.org/10.1109/TSE.2023.3290237

[18] Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. 2009. Methods for Designing Privacy Aware Information Systems: A Review. In *PCI 2009, 13th Panhellenic Conference on Informatics, 10-12 September 2009, Corfu, Greece*. IEEE Computer Society, https://doi.org/10.1109/PCI.2009.45, 185–194. https://doi.org/10.1109/PCI.2009.45

[19] Eric Lachaud. 2020. ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. *Eur. Data Prot. L. Rev.* 6 (2020), 194.

[20] Tianshi Li, Yuvraj Agarwal, and Jason I. Hong. 2018. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4 (2018), 178:1–178:35. https://doi.org/10.1145/3287056

[21] Menga Lüdke and Marli D. A. André. 1999. *A Pesquisa em educação: abordagens qualitativas.* EPU, São Paulo.

[22] Aaron K. Massey, Eric Holtgrefe, and Sepideh Ghanavati. 2017. Modeling Regulatory Ambiguities for Requirements Analysis. In *Conceptual Modeling - 36th International Conference, ER 2017, Valencia, Spain, November 6-9, 2017, Proceedings (Lecture Notes in Computer Science, Vol. 10650)*. Springer, https://doi.org/10.1007/978-3-319-69904-2_19, 231–238. https://doi.org/10.1007/978-3-319-69904-2_19

[23] Aaron K. Massey, Richard Rutledge, Annie I. Antón, and Peter P. Swire. 2014. Identifying and classifying ambiguity for regulatory requirements. In *IEEE 22nd International Requirements Engineering Conference, RE 2014, Karlskrona, Sweden, August 25-29, 2014*. IEEE Computer Society, https://doi.org/10.1109/RE.2014.6912250, 83–92. https://doi.org/10.1109/RE.2014.6912250

[24] Ana Paula Mello and Giovanna Coelho Miramontes. 2022. LGPD: agentes De Tratamento, Resposável E ANPD. *Cadernos Jurídicos da Faculdade de Direito de Sorocaba* 3, 1 (mar. 2022), 73–80. https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/88

[25] MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS 2024. *Guia sobre Privacidade desde a Concepção e por Padrão: PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)*. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, Brasília. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf

[26] European Union Agency For Network and Information Security. 2015. *Online privacy tools for the general public: Towards a methodology for the evaluation of PETs-for internet & mobile users*. European Union Agency For Network And Information Security, European Union. https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public

[27] Helen Nissenbaum. 2010. *Privacy in Context - Technology, Policy, and the Integrity of Social Life.* Stanford University Press, http://www.sup.org/book.cgi?id=8862.

[28] European Parliament and Council of European Union. 2016. General Data Protection Regulation (GDPR). , 88 pages. https://gdpr-info.eu/,Last access on 10 April 2022.

[29] Mariana Maia Peixoto, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo, and Tony Gorschek. 2020. On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview. In *Requirements Engineering: Foundation for Software Quality - 26th International Working Conference, REFSQ 2020, Pisa, Italy, March 24-27, 2020, Proceedings [REFSQ 2020 was postponed] (Lecture Notes in Computer Science, Vol. 12045)*. Springer, https://doi.org/10.1007/978-3-030-44429-7_8, 116–123.

[30] 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

[31] Renato Carauta Ribeiro and Edna Dias Canedo. 2020. Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. In *dg.o '20: The 21st Annual International Conference on Digital Government Research, Seoul, Republic of Korea, June 15-19, 2020*. ACM, https://doi.org/10.1145/3396956.3398252, 175–184. https://doi.org/10.1145/3396956.3398252

[32] 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*. ACM, https://doi.org/10.1145/3555776.3577615, 1352–1361. https://doi.org/10.1145/3555776.3577615

[33] 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* (Tallinn, Estonia) *(SAC '23)*. Association for Computing Machinery, New York, NY, USA, 1352–1361. https://doi.org/10.1145/3555776.3577615

[34] T. L. Saaty. 1980. *The Analytic Hierarchy Process.* McGraw-Hill, New York, NY, USA.

[35] William Stallings. 2019. *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices.* Addison-Wesley Professional, Addison-Wesley Professional.

[36] 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