Applying Gamification to Promote Privacy and Information Security Awareness in the Public Sector

ABSTRACT

Context: Traditional awareness programs on privacy and information security in the public sector are often perceived as unengaging and ineffective in promoting lasting behavioral change. Human error remains a key vulnerability, and there is growing interest in more engaging approaches such as gamification. **Objective**: This study investigates whether gamification can enhance privacy and information security awareness among public servants, and identifies the organizational factors that influence its perceived feasibility. **Method**: We conducted a quantitative survey with 518 Brazilian public servants working in Information and Communications Technology (ICT), using descriptive statistics to analyze perceptions of traditional and gamified approaches, engagement elements, and institutional readiness. **Results**: Respondents rated traditional methods as moderately effective but lacking in engagement. Gamification was perceived as more motivating and effective for knowledge retention and behavioral change. Key adoption barriers included organizational culture and lack of understanding, while leadership support and digital familiarity were seen as enablers. **Conclusion**: Gamification is viewed as a promising and feasible strategy for improving awareness training in the public sector. However, its successful adoption depends on overcoming cultural resistance and ensuring institutional support. The findings provide empirical evidence to guide future implementations and inform the design of training policies.

CCS CONCEPTS

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

KEYWORDS

Information Security Awareness, Privacy, Gamification, Public Service, Human Factors in Cybersecurity

1 INTRODUCTION

The protection of personal data and the implementation of Information Security (IS) practices have become central concerns for both private and public organizations. The approval of comprehensive data protection regulations—such as the European General Data Protection Regulation (GDPR) [34] and Brazil's General Data Protection Law (LGPD)[27]—has increased pressure on institutions to implement privacy-preserving mechanisms by design. However, despite these legal mandates, empirical studies show that many organizations and professionals still lack the technical knowledge and cultural readiness to fully comply with such frameworks.

Peixoto et al. [35] found that Brazilian software developers struggled to interpret and implement privacy requirements appropriately, often confusing them with security controls. Similarly, de Jesus et al. [12] applied a risk assessment method in a small startup and identified significant vulnerabilities due to a lack of specialized personnel and limited understanding of both security and privacy principles. These studies reinforce a broader concern: without proper awareness and capacity-building, regulatory frameworks alone are insufficient to ensure meaningful data protection.

This scenario is particularly critical in the public sector, where institutional exposure to security risks is high and the consequences of mismanaging personal data can be severe. In recent years, the rise in cyberattacks and data breaches has become a global concern. According to the Threat Landscape Report published by the European Union Agency for Cybersecurity (ENISA) [14], there was a significant increase in such incidents between the second half of 2023 and the first half of 2024, with public sector organizations among the most targeted, accounting for 19% of reported cases [18]. This trend is also evident in Brazil. In 2024, the Brazilian Government's Center for Prevention, Treatment, and Response to Cyber Incidents (CTIR.Gov)[1] reported 14,654 occurrences, including 9,490 incidents and 5,164 vulnerabilities. Notably, 7,471 of these incidents were related to data breaches, highlighting the exposure of the public sector to cybersecurity risks.

One of the main contributing factors to security incidents is human error [18–20]. Unsafe or uninformed behaviors—such as clicking on malicious links, reusing passwords, or neglecting protection protocols—often facilitate cyberattacks [4]. In this context, awareness programs focused on privacy and information security play an important role in mitigating these risks [40].

Traditionally, these programs adopt conventional approaches such as lectures, manuals, and formal training sessions [13, 33, 42]. However, such methods have proven to be less effective in promoting lasting engagement or meaningful behavioral change [15, 41]. Low interactivity, monotony, and limited applicability to daily routines are often cited as barriers to their effectiveness [22]. This highlights the need to explore innovative strategies that overcome these shortcomings.

In this context, gamification emerges as a promising alternative. By incorporating elements such as challenges, rewards, and competition, this approach has shown potential to increase engagement and knowledge retention in privacy and information security training [4, 22, 30].

Despite evidence of its benefits in corporate environments, the adoption of gamification in the public sector remains incipient [22]. There are few documented initiatives and a lack of empirical research evaluating its impact in institutional public settings. This gap highlights the need to explore how gamification can be tailored to the unique characteristics of the public sector, providing more effective solutions for cybersecurity awareness.

To address this gap, this study investigates the research question **RQ.1. Can gamification contribute to privacy and information security awareness in the public sector?**. We combine an exploratory review of prior work with a quantitative survey of 518 Brazilian ICT civil servants to answer this question. The survey

[1] https://www.gov.br/ctir/pt-br

aimed to understand their perceptions regarding the use of gamification in awareness programs focused on privacy and information security.

The findings indicate that despite limited prior exposure to gamification in the workplace, public servants expressed strong confidence in its potential for awareness training. Participants who had experienced gamified activities—either inside or outside their institutions—consistently rated them highly in terms of motivation, engagement, and learning. These results suggest that gamification is not only perceived as a viable alternative to traditional methods but also as a more effective strategy for fostering knowledge retention and driving behavioral change in information security and privacy contexts.

2 BACKGROUND AND RELATED WORK

2.1 Cybersecurity and the Human Factor

Cybersecurity encompasses the protection of cyberspace, information and communication technologies (ICT), and the users involved, safeguarding both tangible and intangible assets against digital threats. Fatokun et al. [15] described it as a multidimensional discipline that covers not only technological infrastructures but also human behaviors. Bouzegza et al. [5] further expand the scope, encompassing areas such as network and application security, phishing, social engineering, data breaches, malware, and privacy.

Cybersecurity threats originate from both internal and external sources, ranging from sophisticated attacks (e.g., ransomware, Advanced Persistent Threats) to simple incidents such as the loss of a mobile device or accidental data disclosure. Despite heavy investments in technical defenses like firewalls and intrusion detection systems, human behavior continues to be a major vulnerability [14, 18–20]. Human-related incidents—whether intentional or accidental—stem from lack of awareness, carelessness, or manipulation [4], limiting the effectiveness of technical controls.

This issue is particularly critical in the public sector. Government institutions manage vast amounts of sensitive data, making them prime targets for malicious actors [10]. Protecting such assets is not only essential for institutional continuity but also a legal and ethical obligation under frameworks like Brazil's General Data Protection Law (LGPD) [27]. In this context, promoting user awareness becomes a strategic requirement to uphold data confidentiality, integrity, and availability [22, 40].

Several frameworks address this challenge through best practices and guidelines, including CyBOK [37], CIS Controls [9], and NIST standards [3]. However, Khando et al. [22] caution that these frameworks must be adapted to each organizational context, especially in the public sector. Public institutions still face major challenges implementing effective awareness programs. Bureaucratic resistance, limited budgets, and lack of continuous training hinder progress [2]. In light of these structural barriers, technical and regulatory measures alone are insufficient [4, 33]. Strengthening the human factor remains key to reducing vulnerabilities [2].

2.2 Privacy and Information Security Awareness

Privacy and information security awareness refers to structured initiatives aimed at educating individuals about risks, responsibilities, and best practices [38]. According to Merritt et al. [29], these programs empower users to recognize secure behaviors and respond to threats. Pahlavanpour and Gao [33] emphasize that effective awareness improves risk perception, supports secure decision-making, and promotes safe system usage.

Khando et al. [22] highlighted that these programs should go beyond technical instruction, helping employees internalize institutional policies and understand the consequences of improper data handling. However, conventional training approaches—videos, presentations, posters, newsletters, and quizzes—have shown limited effectiveness [13, 33, 42]. Bitrián et al. [4] point out that such methods are often seen as interruptions, resulting in disengagement. Khando et al. [22] and Pahlavanpour and Gao [33] argued that these strategies often neglect social, cultural, and individual factors, and fail to accommodate diverse learner needs. Capatina et al. [8] further suggest that such methods lead to passive learning and poor knowledge retention. These problems are exacerbated in the public sector [2]. Budget constraints, rigid structures, and uninspiring mandatory training create additional barriers. Therefore, new approaches are needed to build an effective culture of privacy and security [40]. One promising solution is gamification.

2.3 Gamification: An Innovative Approach

Gamification refers to the strategic use of game design elements in non-game contexts to foster intrinsic motivation, engagement, and learning [23, 28, 30]. Decusatis [13] described it as a user-centered methodology capable of driving behavioral change through immersive experiences. Game elements such as points, levels, badges, leaderboards, immersive narratives, avatars, and real-time feedback are employed to structure meaningful learning activities [8, 28].

Though widely used in education, healthcare, and corporate training, gamification is still underutilized in privacy and security awareness [17]. Recent studies, however, show that gamified approaches can effectively overcome the limitations of traditional methods [15, 23, 33]. Unlike passive strategies, gamification enables learners to experience complex concepts—such as phishing, ransomware, or social engineering—through simulations [15, 23, 28]. These experiences improve retention and skill acquisition [17], and allow personalization to suit users' roles, learning pace, and expertise [8].

Gamification also provides a safe, low-risk environment for experimentation and learning from mistakes [17, 42]. This is particularly valuable in cybersecurity, which demands practical problem-solving skills [23]. Nevertheless, implementation challenges exist. Developing and maintaining gamified systems can be costly [28]. Sustaining user engagement over time is difficult [33], and diverse user profiles require adaptable designs [15]. Institutional support is essential [22], as is careful design to avoid negative impacts on performance [1].

Despite these barriers, the transformative potential of gamification remains substantial. Its integration with emerging technologies—such as artificial intelligence [33] and immersive environments like the metaverse [1]—further expands its relevance in the future of cybersecurity training.

Recent efforts have also explored how gamification can enhance knowledge sharing in software development teams. Gonçalves et

al. [16] conducted a rapid review and identified key game elements (e.g., points, badges, leaderboards) and motivational strategies (e.g., Self-Determination Theory, Goal-Setting Theory) applied to support collaboration, documentation, and knowledge transfer in software projects. Although gamification shows promise in this domain, the authors emphasize the lack of standardization and long-term evaluation, calling for more rigorous empirical studies tailored to organizational culture and team dynamics. Their findings highlight that gamification can be a powerful mechanism not only for training but also for fostering continuous learning and engagement in knowledge-intensive environments.

2.4 Motivation and Self-Determination Theory

Motivation plays an important role in awareness program success, especially in complex areas like privacy and cybersecurity. Gamification is a powerful strategy to boost engagement by using game design in non-game contexts [33]. In the public sector—where security policies are often perceived as bureaucratic—gamification can make learning more engaging and relevant. Motivation is typically divided into two types: intrinsic (driven by enjoyment or interest) and extrinsic (driven by rewards or avoiding punishment) [23, 41].

The Self-Determination Theory (SDT), proposed by Deci and Ryan [39], is widely used to understand motivation [25]. SDT posits that individuals have three basic psychological needs: competence (feeling capable), autonomy (having control over choices), and relatedness (feeling connected to others) [8]. Satisfying these needs enhances intrinsic motivation and promotes deeper engagement. Gamification can support these needs. Real-time feedback and progressive challenges strengthen competence [7, 25, 32]. Giving learners choices promotes autonomy [21]. Social elements like collaboration and competition foster relatedness [8].

Integrating SDT into gamified experiences moves awareness programs beyond simple information delivery. By aligning with users' psychological needs, gamification fosters sustained motivation and behavior change [26]. When strategically applied, gamification becomes more than just a fun layer—it acts as a catalyst for deeper commitment among public servants to protect data and institutional systems.

While existing literature has explored gamification's theoretical potential in corporate and educational environments, few empirical studies have examined its application in public sector cybersecurity training. Our research addresses this gap by combining a literature review with a large-scale survey of 518 Brazilian public servants to empirically assess perceptions, feasibility, and organizational readiness for gamified awareness programs in privacy and information security.

3 STUDY SETTINGS

This study investigates the use of gamification as a strategy to improve privacy and information security awareness in the public sector. Specifically, it aims to assess public servants' familiarity with gamified training methods, their perceived effectiveness compared to traditional awareness approaches, and the challenges and opportunities for implementing such strategies in government institutions. We adopted a quantitative approach, conducting a cross-sectional survey following the guidelines proposed by Kitchenham and Pfleeger [24].

The target population consisted of Brazilian public servants, and the survey aimed to capture their perceptions regarding the application of gamification in privacy and information security awareness programs. To address **RQ.1. Can gamification contribute to privacy and information security awareness in the public sector?**, we defined two supporting sub-questions:

- **RQ1.1:** How do public servants perceive the effectiveness of gamification compared to traditional awareness methods?
  Motivation: *This question aims to compare traditional methods with gamified approaches for promoting engagement, knowledge retention, and behavioral change.*
- **RQ1.2:** How do public servants perceive the feasibility of using gamification in the public sector?
  Motivation: *This question aims to understand the perceptions of public servants on using gamified approaches in their institutions. Positive perceptions among these individuals can indicate the likelihood of successful adoption and integration of gamified initiatives within their institutions.*
- **RQ1.3:** What are the key factors that influence public servants' perception of the feasibility of implementing gamified awareness programs within their institutions?
  Motivation: *This question investigates factors related to organizational culture, leadership support, engagement elements, institutional priorities, and potential obstacles to adoption.*

3.1 Sampling and Data Collection

A non-probabilistic, convenience sampling method was used. The survey was disseminated through online groups of public servants, using platforms such as WhatsApp, Microsoft Teams, and Outlook. Participation was voluntary and contingent upon acceptance of the Informed Consent Form (ICF), which guaranteed anonymity and confidentiality. Invitations were distributed directly and indirectly, emphasizing the voluntary nature and the value of participants' contributions.

All authors of the paper were involved in designing and validating survey questions. The survey comprised 24 closed-ended questions structured into five thematic sections, as shown in Table 1. Except for Q1 and Q24, all other questions are included in a thematic section. Q1 pertains to the Consent to Participate in the Research. It includes conditions, stipulations, and contact information, as well as a way to verify the respondent's profile. Furthermore, Q24 was designed to ensure the quality of the responses. The survey used 5-point Likert scales for evaluation items and multiple-choice questions (single or multiple selection) for participant profiling. The complete instrument, including the questions and all response options, is publicly available in the Zenodo repository.

3.2 Pilot Study

We conducted a pilot study with four public servants to assess the clarity and relevance of the questions. Based on their feedback, we revised some wording and adjusted response options. The average completion time was approximately 10 minutes and was included

ID	Question	Type
Q1	*Informed Consent*	*Binary*
1. Participant Profile (Demographics)		
Q2	Which level of public administration do you currently work for?	Multiple Choice
Q3	What is the approximate size of your public institution?	Multiple Choice
Q4	How long have you been working in the public sector?	Multiple Choice
Q5	What is your current area of work in the public sector?	Multiple Choice
Q6	What is your age range?	Multiple Choice
Q7	What is your highest level of education?	Multiple Choice
2. Knowledge and Training (Demographics)		
Q8	How would you rate your familiarity with digital technologies?	Likert Scale
Q9	How would you rate your knowledge of information security?	Likert Scale
Q10	How would you rate your knowledge of privacy and data protection?	Likert Scale
Q11	Have you participated in awareness campaigns on Information Security and Privacy in your organization?	Likert Scale
3. Traditional Methods and Gamification Experience (RQ 1.1)		
Q12	How do you rate traditional awareness methods used in your institution (e.g., videos, emails)?	Likert Scale
Q13	Have you ever participated in activities with gamification elements (e.g., points, rankings, challenges)?	Multiple Choice
Q14	How do you evaluate your experience with gamified activities? (engagement, motivation, learning)	Likert Scale
Q15	After participating in gamified activities, I noticed improvement in my knowledge.	Likert Scale
4. Perceptions on Gamification in Public Sector(RQ 1.2)		
Q16	Do you believe gamification can contribute to training in the following aspects?	Likert Scale
Q17	I believe gamification can reduce human errors in information security.	Likert Scale
Q18	Do you consider it feasible to apply gamification in your organization's training?	Likert Scale
5. Barriers, Preferences, and Leadership (RQ 1.3)		
Q19	Which elements do you consider most effective to enhance engagement in educational activities?	Multiple Choice
Q20	In your opinion, what factors hinder gamification adoption in the public sector?	Multiple Choice
Q21	How does your organization prioritize privacy and information security?	Likert Scale
Q22	Institutional leadership support is important for successful gamified training.	Likert Scale
Q23	Does your top management support innovation in training?	Likert Scale
Q24	*Please enter the current year to confirm that you are not a bot.*	*Open Question*

Table 1: Survey Questions

in the instructions of the final version. Pilot responses were not included in the final analysis. The final survey was distributed via Google Forms and remained open from May 29 to June 20, 2025. A total of 524 responses were collected. However, six participants did not provide informed consent and withdrew during the process, resulting in 518 valid responses being retained for analysis.

3.3 Data Analysis

We conducted a comprehensive descriptive analysis to examine public servants' perceptions and attitudes toward gamification in cybersecurity awareness programs. We treated multiple-choice questions as nominal variables and Likert-scale questions as ordinal variables. All Likert-scale questions used a 5-point scale.

For demographic variables (Q2 to Q7), we computed absolute (n) and relative (%) frequencies. Since these variables do not follow a metric scale, descriptive statistics based on counts and percentages were used to avoid misleading interpretations based on averages. For 5-point Likert scale items (see Table 1), we reported the mean to reflect overall trends, the median to identify the central value and detect potential asymmetries, and the standard deviation to assess variability. Lower standard deviation values indicate greater agreement among participants. In cases where additional detail was relevant—such as identifying opinion polarization—we also presented the full percentage distribution for each response category. This dual presentation was particularly useful for evaluating traditional methods (Q12) and organizational prioritization of privacy and security (Q21).

For items measuring agreement or experience (Q11, Q15–Q18, Q22, Q23), we presented the percentage of responses across all scale points. This approach enabled us to visualize the exact proportions of neutral respondents and those who agreed and disagreed. Questions Q19 and Q20 allowed multiple selections. Each option was treated as a separate binary variable, and the percentage of respondents selecting each item was calculated. This enabled us to rank the options based on perceived importance.

4 RESULTS

4.1 Participants Profile

We received 518 responses to our survey questionnaire, all of which were from Brazil. Among the participants, most of them indicated that they work in the federal public administration (Q2), while four reported working in some state-level institutions, two in municipal administrations, and another three in agencies under the Federal District Government, as presented in Table 2.

Regarding the size of their institutions (Q3), 445 public servants reported working in organizations with more than 5,000 employees. An additional 24 participants stated that their agencies employ between 1,001 and 5,000 staff members, eight work in institutions with 201 to 1,000 employees, and seven respondents are part of agencies with up to 200 employees. A small number of participants (34) reported not knowing the size of their organization. These distributions are detailed in Table 2.

As for time in public service (Q4), the majority of respondents—398 participants (76.8%)—have more than 15 years of service tenure, while 83 (16%) reported between 7 and 14 years of service. Ten participants (1.9%) have between 4 and 6 years of service, and only 27 respondents (5.3%) have worked in the public sector for up to 3 years. These numbers indicate a respondent pool with long careers in public service. The most common areas of professional activity (Q5) include Information and Communication Technology (ICT) (49%), Systems Audit (14.9%), and Customer Support (13.9%).

In terms of age distribution (Q6), most participants are concentrated in the age ranges of 45–54 years (33.6%) and 55–59 years (24.7%). Finally, regarding education level (Q7), 271 respondents (52.3%) reported holding a postgraduate specialization degree, 168 (32.4%) have a bachelor's degree, 69 (13.3%) hold a master's degree, and 7 participants (1.4%) reported having a doctorate. These results also indicate a high level of educational attainment among the respondents.

Variable	Frequency	%
Administrative Level (Q2)		
Federal	509	98.3%
State	4	0.8%
Federal District	3	0.6%
Municipal	2	0.3%
Institution Size (Q3)		
More than 5,000 employees	445	85.9%
1,001–5,000 employees	24	4.6%
201–1,000 employees	8	1.5%
Up to 200 employees	7	1.4%
Not sure / Did not answer	34	6.6%
Time in the Public Service (Q4)		
Less than 1 year	3	0.6%
1–3 years	23	4.7%
4–6 years	10	1.9%
7–14 years	83	16%
More than 15 years	398	76.8%
Area of Work (Q5)		
ICT	254	49%
Systems Audit	77	14.9%
Customer Support	72	13.9%
Other areas (Information Security, Privacy, and etc.)	115	22.2%
Age Range (Q6)		
Under 25 years	2	0.4%
25–34 years	25	4.8%
35–44 years	100	19.3%
45–54 years	174	33.6%
55–59 years	128	24.7%
60 years and over	89	17.2%
Education Level (Q7)		
High School	3	0.6%
Bachelor's Degree	168	32.4%
Specialization	271	52.3%
Master's Degree	69	13.3%
PhD Degree	7	1.4%

Table 2: Sociodemographic Profile of Participants (n=518)

4.2 Knowledge and Training

We also asked the respondents about previous knowledge and familiarity that could affect the interpretation of our research questions. Table 3 summarizes aspects and the answers we got.

Regarding **technology familiarity (Q8)**, 224 public servants reported having a good level of familiarity with digital technologies, 196 indicated a moderate level, and 82 participants stated they were highly familiar. Only 16 respondents reported having low digital familiarity. As shown in Table 3, the mean score was 3.72 and the median was 4 ("Good") on a 5-point Likert scale. The low standard deviation (SD = 0.76) indicates a high degree of consistency in responses, suggesting that most participants feel comfortable using digital technologies. This is a relevant finding, as it points to a participant profile that is likely to be receptive to innovative technological solutions, such as gamification.

Variable	Mean	Median	SD
Technology Familiarity (Q8)	3.72	4	0.76
Information Security Knowledge (Q9)	3.28	3	0.89
Data Privacy Knowledge (Q10)	3.21	3	0.90

Table 3: Digital Familiarity and Knowledge in Privacy and Information Security

Regarding **knowledge of information security and privacy (Q9)**, the majority of participants (204) reported having a good level of knowledge, while 161 indicated an intermediate level of knowledge. Additionally, 30 respondents rated their knowledge as advanced. A total of 120 participants reported having only a basic understanding. It is noteworthy that all participants reported having at least some level of knowledge on the topic; in other words, no one selected the "no knowledge" option. These results suggest that, on average, participants perceive themselves as having a moderate to good understanding of information security and privacy.

We can observe in Table 3, a relatively low standard deviation, which indicates that responses are moderately concentrated around the mean, reinforcing the idea that the sample has a consistent baseline of knowledge in this domain. This finding is important, as it suggests that public servants may be well-positioned to benefit from more advanced or innovative training approaches, such as gamification.

Finally, regarding **knowledge of privacy and personal data protection (Q10)**, most participants (198) rated their knowledge as good, while 161 indicated an intermediate level. Additionally, 24 respondents reported having advanced knowledge. A total of

131 participants stated they had only a basic understanding, and 4 participants indicated they had no knowledge at all of the topic.

The mean score 3.21 and the SD 0.90 (Table 3) indicate that, on average, participants reported an intermediate level of knowledge in privacy and data protection, with a slightly more dispersed distribution compared to information security (Q9).

This pattern suggests that, despite a moderate overall score, these topics—particularly in relation to the LGPD [27]—remain areas in which public servants identify a need for additional training and clarification. This finding aligns with prior studies [6, 31, 35, 36] that highlight insufficient preparedness among professionals regarding data protection regulations. Therefore, the development of targeted awareness initiatives, potentially supported by gamification strategies, is important to strengthen institutional compliance and foster a privacy-conscious culture in the public sector.

We also asked the participants if they had participated in awareness campaigns on Information Security and Privacy. A total of 56.7% of participants agreed or strongly agreed that they had participated in awareness campaigns on Information Security and Privacy within their organization (Q11). Meanwhile, 17.4% neither agreed nor disagreed, and 25.9% reported not having participated in such campaigns in their workplace. The results presented in this section indicate that our sample is suitable to answer our proposed research questions.

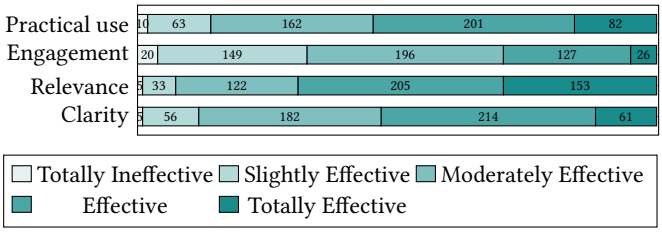
4.3 RQ1.1. Perceptions of Effectiveness in Awareness Programs using Traditional and Gamified approaches

4.3.1 Perception of Traditional Methods. We first asked the respondents to evaluate how traditional privacy and information security awareness strategies—such as videos, emails, and presentations—are implemented in their institutions (Q12). This evaluation was based on four dimensions: clarity of information, relevance to daily work, level of engagement generated, and practical applicability.

The results revealed varying levels of perceived effectiveness across these dimensions. The dimension Information Clarity received an average rating of 3.52 and a median of 4 on a 5-point Likert scale, indicating that most respondents considered the communication to be between "moderately effective" and "effective". The moderate standard deviation (SD = 0.87) suggests a fair degree of consensus among participants, as shown in Figure 1.

The highest-rated dimension was Work Relevance, with a mean of 3.90 and a median of 4, reflecting that civil servants generally acknowledge the usefulness of the content for their day-to-day activities. Despite a slightly higher standard deviation (SD = 0.93), the overall perception remains strongly positive. In contrast, Generated Engagement emerged as the most critical issue. With an average rating of 2.98 and a median of 3, the results indicate that traditional methods are perceived as lacking in terms of participant motivation. The relatively high dispersion (SD = 0.94) further reinforces the need to explore more engaging approaches—such as gamification—to enhance participation.

Lastly, about the practical application of the acquired knowledge, the respondents showed relatively favorable results, with a mean of 3.54 and a median of 4, suggesting that many respondents were able to apply what they learned to their professional context. However, the standard deviation (SD = 0.96) reveals that this outcome is not uniformly experienced across the sample. Figure 1 presents a visual summary of these findings, combining the stacked distribution of responses for each evaluation dimension with descriptive statistics (mean, median, and standard deviation).



Dimension	Mean	Median	SD
Information clarity	3.52	4	0.87
Work relevance	3.90	4	0.93
Generated engagement	2.98	3	0.94
Practical application	3.54	4	0.96

Figure 1: Evaluation of traditional awareness methods in information security and privacy.

4.3.2 Perceptions of Gamification. To compare traditional and gamified approaches, we also designed questions that focused on participants' experiences and perceptions of the gamified method. We began by providing a definition and then inquired whether the participants had been exposed to activities that included gamification elements (Q13).

The majority of participants (50.4%) reported that they had never been exposed to activities involving gamification elements (Q13), such as points, rankings, or challenges. 32.2% (172 respondents) indicated prior exposure to gamification outside the workplace—through applications, learning platforms, games, and similar contexts. Only 16.4% (85 participants) of respondents stated that they had experienced gamified activities within their professional environment, as shown in Figure 2. These results highlight that, although gamification elements are present in other domains, their use in the public sector workplace remains limited and largely unexplored. It is worth noting that the 257 respondents who reported prior experience with gamification rated traditional awareness methods (Q12) more positively across all four evaluated dimensions.

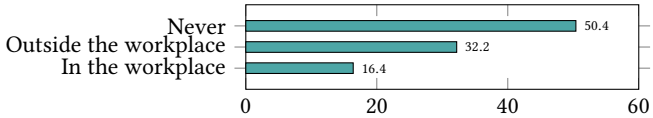


Figure 2: Exposure to gamification elements (Q13).

To explore the applicability of gamification in privacy and information security awareness efforts, we asked participants to evaluate their previous experience with gamified activities (Q14)—regardless

of whether that experience occurred within or outside the workplace. Respondents were asked to assess this experience across three dimensions: engagement, motivation, and learning.

As shown in Table 4, the results were consistently positive. The dimension of motivation received the highest average rating (mean = 3.96, median = 4, SD = 0.94), suggesting that gamified experiences are perceived as highly motivating. Engagement followed closely with a mean of 3.93 and SD = 0.90, while learning was also positively rated (mean = 3.89, SD = 0.93). In all three dimensions, the median score was 4, indicating that most participants considered their gamified experiences to be good or excellent. These findings highlight the potential of gamification to promote more engaging and effective awareness strategies in the public sector.

Dimension	Mean	Median	SD
Engagement	3.93	4	0.90
Motivation	3.96	4	0.94
Learning	3.89	4	0.93

Table 4: Evaluation of Gamified Experience (Q14)

After participating in gamified activities (Q15), 177 respondents (51.4% agreed and 17.5% strongly agreed) reported an improvement in their knowledge as a result of the gamification experience. Additionally, 18.7% neither agreed nor disagreed, while only 12.4% expressed disagreement—6.2% disagreed and 6.2% strongly disagreed. These results suggest a strong perceived association between gamified activities and knowledge acquisition, reinforcing the potential of gamification to support effective learning in awareness programs.

RQ1.1 Summary: While traditional methods are seen as moderately effective—especially in terms of clarity and relevance—they fall short in generating engagement. On the other hand, when asked about gamification, most of the respondents rated engagement, motivation, and learning as good or excellent. These findings highlight the potential of gamification to promote more engaging and effective awareness strategies in the public sector.

4.4 RQ1.2. Application of Gamification in the Public Sector

Through questions 16 to 18, we explored participants' perceptions regarding the potential benefits of using gamification in privacy and information security training within government institutions. Specifically, Question 16 asked whether participants believed gamification could support three key aspects of training programs: making sessions more engaging, enhancing knowledge retention, and encouraging behavioral change.

The results, presented in Figure 3, indicate consistently positive perceptions. Regarding the ability of gamification to make trainings more engaging, 80.6% of respondents (n=403) agreed or strongly agreed, while only 5.2% disagreed. Similarly, 79.5% (n=397) believed that gamification could help with knowledge retention, with just 6.3% expressing disagreement. When asked about its potential to promote behavior change, 72.8% (n=363) responded favorably, and 6.2% disagreed.

These findings strongly support the idea that public servants view gamification as a valuable approach to improving training outcomes in privacy and information security. The relatively low percentages of disagreement and neutral responses suggest that gamification is well-positioned to address common weaknesses found in traditional awareness programs. Figure 3 provides a visual summary of responses for each dimension evaluated.

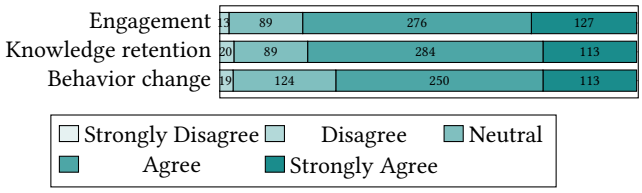


Figure 3: Perceived benefits of gamification in public sector privacy and security training (Q16).

We explored whether participants believe that gamification can help reduce human errors in information security (Q17), considering the context of the public sector. The results reveal a predominantly positive perception: 53.7% of respondents (n = 278) agreed with the statement, and 11.4% (n = 59) strongly agreed. Together, these responses indicate that nearly two-thirds of public servants recognize the potential of gamified approaches to address human-related vulnerabilities in security practices. Meanwhile, 28.2% (n = 146) neither agreed nor disagreed, suggesting a moderate level of uncertainty or lack of exposure to such initiatives. A smaller proportion expressed disagreement, with 4.9% (n = 25) disagreeing and 2% (n = 10) strongly disagreeing.

Finally, we asked participants whether they consider it feasible to apply gamification in training activities within their own organizations (Q18). The responses were even more favorable than those to Q17. A total of 57.5% of participants (n = 298) agreed, and 18.5% (n = 96) strongly agreed, indicating a broad sense of institutional openness and perceived feasibility for implementing gamified awareness strategies. Only 7.7% (n = 40) expressed disagreement (5.7% disagreed and 2% strongly disagreed), while 16.2% (n = 84) reported a neutral stance. These results reinforce the relevance and practical viability of gamification as an innovative training approach in the context of public sector organizations.

RQ1.2 Summary: Overall, participants perceive gamification as a promising approach to enhance awareness, support knowledge retention, and encourage behavioral change in privacy and information security training in the public sector.

4.5 RQ1.3. Factors Influencing the Adoption of Gamification

To better assess the feasibility of implementing gamified awareness programs in the public sector, we examined participants' perceptions of organizational culture, leadership support, and potential

barriers. Questions Q19 to Q23 aimed to identify factors that influence engagement, institutional priorities, and obstacles that could hinder the adoption of gamification. These aspects are important for understanding an organization's readiness and openness to adopting innovative training approaches.

To answer RQ1.3, we asked participants to indicate which elements they considered most effective in enhancing engagement in educational activities (Q19). The most frequently selected item was immediate feedback (57.9%), followed by challenges (49.0%) and symbolic rewards (42.1%). Other elements highlighted by participants included missions or goals (40.2%), narratives or storytelling (37.3%), points (30.9%), and rankings (27.8%).

These results reveal a clear preference for interactive and motivational features that create dynamic learning experiences. The median selection rate across all items was 40.2%, with a standard deviation of 10.34, indicating moderate variability in participant preferences. This suggests that a diverse combination of engagement strategies may be needed to design gamified training programs in the public sector effectively. Figure 4 shows the distribution of responses for each engagement element evaluated.

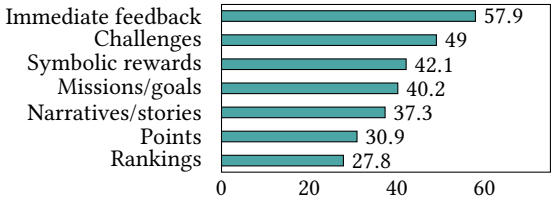


Figure 4: Most effective elements to increase engagement in educational activities (Q19).

4.5.1 Adoption Barriers on the Public Sector. To identify key obstacles to implementing gamified awareness programs in the public sector, participants were asked to identify the factors they believe hinder gamification adoption (Q20). As shown in Figure 5, the most frequently cited barriers were organizational culture (66.4%) and a lack of understanding about what gamification is (63.7%). Resistance from public servants (48.8%) and low leadership support (29.9%) were also notable concerns. Financial constraints (23.4%) and limited technological infrastructure (12.7%) were less commonly reported, but still relevant.

These findings suggest that successful implementation of gamified strategies depends not only on available resources but also on cultural change and increased awareness about the concept of gamification itself.

4.5.2 Privacy and Security Prioritization. Regarding how participants perceive their organization's prioritization of information security and privacy (Q21), the majority reported that it is considered essential (53.9%) or a high priority (31.1%). A smaller portion indicated it was a medium priority (10.4%), while only a few viewed it as a low priority (2.9%) or not a priority at all (1.7%), as shown in Figure 6.

These results suggest that most public institutions formally recognize the strategic importance of privacy and security. However,

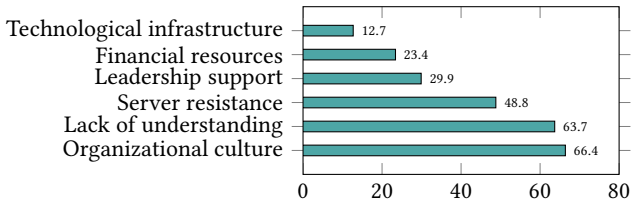


Figure 5: Perceived barriers to the adoption of gamification in the public sector (Q20).

the presence of a small yet relevant group reporting lower prioritization highlights potential disparities in implementation across organizations. On a 5-point Likert scale (where 1 = Not a priority and 5 = Essential), the median response was 5 (Essential) and the standard deviation was approximately 0.84, indicating a strong central tendency toward high prioritization with relatively low variability in responses.

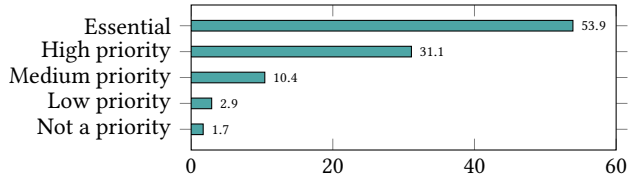


Figure 6: Perceived organizational prioritization of information security and privacy (Q21).

4.5.3 Leadership and Gamified Training. Participants were asked whether they believe that institutional leadership support is important for the success of gamified training programs (Q22). The vast majority responded positively: 233 participants strongly agreed and 223 agreed, representing 88% of all responses. Only 53 participants (10.2%) remained neutral, and very few disagreed (six strongly disagreed and three disagreed).

These results underscore the strong consensus on the critical role leadership support plays in facilitating the implementation and effectiveness of gamification strategies in public sector training. Figure 7 illustrates this distribution.

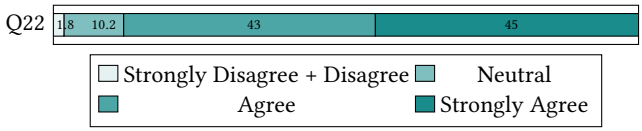


Figure 7: Perceptions of leadership support importance for gamified training success (Q22).

4.5.4 Institutional Support for Training Innovations. To assess institutional support for training innovations, we asked participants whether top management in their organizations supports innovation in training programs (Q23). The responses revealed a generally positive outlook: a combined 65.1% of respondents indicated that leadership supports innovation either frequently or always (217

and 108 participants, respectively). Meanwhile, 30.7% stated that such support occurs only occasionally (153 selected sometimes), and a small portion reported rare (28) or nonexistent support (12).

This distribution indicates a trend toward favorable institutional environments for implementing gamified awareness programs, though some variability in leadership engagement remains. Figure 8 illustrates the full distribution of responses.

Figure 8: Perceived top management support for training innovation (Q23).

RQ1.3 Summary: Participants identified several factors that influence the feasibility of adopting gamified awareness programs in the public sector. Immediate feedback, challenges, and symbolic rewards were seen as the most effective elements to enhance engagement. However, barriers such as organizational culture, lack of understanding of gamification, and resistance from staff were frequently cited. Most respondents perceived privacy and security as high or essential priorities in their institutions, and a large majority agreed that leadership support plays a crucial role in the success of gamified training. These results highlight that while there is a favorable environment for innovation, successful implementation depends on overcoming cultural and structural challenges.

5 DISCUSSION

The data analysis revealed four main findings. First, traditional training methods in information security and privacy—although perceived as clear and relevant—fail to effectively engage participants (Finding 1, derived from Q12). Second, there is a broadly positive perception of gamification's potential to make training more motivating, improve knowledge retention, and foster behavioral change, even among those with little or no prior experience with this approach (Finding 2, derived from Q14, Q15, and Q16). Third, for public servants, the most effective gamification elements are those that promote a sense of competence and autonomy, such as immediate feedback and progressive challenges, rather than purely competitive features (Finding 3, derived from Q19). Finally, the main obstacles to adopting gamification in the public sector are not financial or technological, but rather cultural and cognitive—such as organizational culture and a lack of understanding of what gamification entails (Finding 4, derived from Q20).

The data analyzed in this study confirm a common criticism found in the literature: traditional training methods often fail to engage participants (Q12). The dimension of "Generated Engagement" received the lowest rating among the four evaluation criteria for conventional training, reflecting a perception that ranges from neutrality to ineffectiveness. This finding is particularly noteworthy when compared to the more favorable ratings for "Clarity of Information" and "Relevance to Work." The data suggest that the issue may not be with the content itself, which is viewed as relatively clear and relevant, but rather with the manner in which the content is delivered. This interpretation is supported by the works of Bitrián et al. [4] and Khando et al. [22], which characterize traditional training as overly focused on compliance. This approach promotes passive learning and leaves employees feeling disengaged. Therefore, the results presented herein provide quantitative evidence, particularly within the context of the Brazilian public sector, that expository and non-interactive training models fail to capture attention and motivate professionals. This indicates a significant engagement deficit that must be addressed.

On the other hand, the perception of gamification's potential is extremely positive (Q16). Most employees believe that adding playful elements to training can make it more engaging, enhance knowledge retention, and encourage behavioral change. This positive perception is particularly strong among those who have experienced gamification (Q13), as they tend to rate these experiences highly in terms of motivation. This finding aligns with recent literature that links gamification to increased participation, motivation, and retention. For instance, Nair et al. [30] found that motivation scores in the gamified module averaged 3.92, which is 11% higher than the traditional module's average of 3.53. Despite the high receptivity to gamification, reported prior experience with it is low. This discrepancy may reflect a latent demand for more engaging training methods, an intuitive sense of gamification's benefits even in the absence of direct experience, or possibly a tendency for respondents to answer in a socially desirable manner. Nonetheless, this situation presents a strategic opportunity for the adoption of gamified approaches in training.

Respondents indicated a preference for techniques that emphasize competence over those centered on competition (Q19). This finding aligns with Self-Determination Theory [39], which highlights competence and autonomy as essential drivers of intrinsic motivation. In the context of public service, this preference may be related to the collaborative nature of public work and the emphasis on collective service over individual achievements. For those responsible for experts in gamified environment design, this finding suggests that engaging this audience requires a focus on creating meaningful learning experiences that include progressive challenges and feedback cycles, rather than primarily concentrating on competitive elements.

Despite the strong optimism expressed by participants who believe in gamification's potential to reduce human errors (Q17) and consider it viable in their organizations (Q18), it is essential to balance these expectations with evidence from the literature. Gwenhure et al. [17] highlighted the lack of studies demonstrating the long-term effectiveness of gamification and the sustainability of behavioral change. For instance, Wu et al. [43] found that while gamification significantly improves knowledge acquisition in specific areas of information security, it does not have a substantial impact on participants' attitudes, compliance intentions, or their willingness to engage in continuous learning. In other words, the transfer of acquired knowledge into lasting attitudinal and behavioral change is not automatic. Therefore, the optimistic perception among employees should be regarded as a powerful catalyst for

change, but it must be accompanied by strategic implementation, continuous evaluation, and the use of behavioral impact metrics.

Finally, regarding organizational factors, the most important research finding is the identification of "Organizational Culture" as the main barrier to adopting gamification (Q20). This factor, along with "Lack of Understanding of Gamification," was classified as more important than some more traditionally recognized obstacles, such as "Financial Constraints" and "Limited Technological Infrastructure." This finding aligns with existing literature on innovation in the public sector, which often points to organizational and cultural barriers as the most prevalent and challenging hurdles to overcome [11]. Therefore, before selecting software or platforms for gamification, organizations should prioritize effective communication, provide conceptual training, and create an environment that encourages experimentation.

Addressing these cultural and cognitive barriers is therefore a prerequisite for the sustainable and effective implementation of gamified awareness programs in the public sector, enabling organizations to fully leverage their potential for improving privacy and information security training.

6 THREATS TO VALIDITY

Internal Validity: The cross-sectional design of the study does not allow for the establishment of definitive causal relationships between variables. While the findings indicate associations, longitudinal studies are needed to confirm whether positive perceptions of gamification lead to effective learning outcomes and lasting behavioral changes. **External Validity:** This study was conducted within the context of the Brazilian public administration. Therefore, its findings may not be directly generalizable to other countries without appropriate consideration of cultural and institutional differences. Moreover, the sample predominantly comprised federal civil servants, which limits the applicability of the results to state and municipal levels—where organizational culture, technological infrastructure, and training practices may differ significantly. Variations across agencies, job functions, and hierarchical levels may also influence perceptions of gamification. The use of convenience sampling may have led to an overrepresentation of participants with greater interest or familiarity with technology, potentially resulting in more favorable evaluations. Additionally, collecting data exclusively through online forms may have excluded individuals with lower digital proficiency, introducing a possible selection bias.

Construct Validity: The reliance on self-reported data introduces potential biases, as the study measures participants' perceptions, beliefs, and attitudes instead of objective behavioral changes. Even if respondents believe in the effectiveness of gamification, their perceptions may not accurately reflect practical outcomes.

7 CONCLUSIONS

This study investigated the potential of gamification to improve awareness programs related to privacy and information security in the Brazilian public sector, as well as the factors that influence the perceived feasibility of this approach. The findings suggest that gamification is not only a viable tool but also a strategic and highly promising method for strengthening awareness initiatives in this domain.

Several pieces of evidence support this conclusion. Traditional methods are often perceived as having low engagement levels, whereas gamification is viewed very positively, particularly in terms of motivation, engagement, and learning. Moreover, participants expressed confidence in gamification's ability to influence practical security outcomes and considered its implementation within organizations feasible. It is important to note, however, that the findings reflect beliefs, attitudes, and intentions rather than direct evidence of long-term behavioral change.

From a practical perspective, the study highlights a strong demand among employees for more engaging and modern training formats, which have the potential to enhance both participation and motivation. From a theoretical perspective, the study provides empirical evidence of the persistent "engagement deficit" associated with traditional training methods in the public sector, an area largely overlooked in prior research. It also reveals that cultural and cognitive barriers—such as organizational resistance and lack of conceptual understanding—pose greater challenges to adoption than financial or technological constraints. This reinforces a sociotechnical perspective on change management in governmental settings.

From a methodological perspective, this study contributes by developing and applying a survey instrument that can be adapted and reused by other researchers to assess perceptions of gamification across different public sector levels or in diverse national contexts. This adaptability supports cross-contextual comparisons and contributes to a broader knowledge base. Furthermore, the study provides reference data for future longitudinal investigations, which could use these findings as a baseline for measuring changes in perceptions and the long-term impact of gamification. Future research could also explore the development of a gamified version of the survey instrument itself. By transforming the data collection process into an interactive and playful experience, researchers would not only demonstrate the practical application of gamification principles but also enhance participant engagement and improve data quality.

Finally, the results offer significant guidance for training policies related to privacy and information security in the public sector. The identified receptiveness suggests that employees are likely to respond positively to investments in gamified approaches. However, successful implementation in government contexts requires careful consideration of regulatory aspects to ensure equity and inclusion, thereby preventing the exclusion of employees with lower technological familiarity or different learning preferences.

In summary, the findings highlight gamification's potential to transform educational practices in the public sector, provided it is implemented as part of a comprehensive change management strategy. This study thus offers a foundation for managerial action and serves as a basis for further academic research, emphasizing the importance of interdisciplinary approaches that combine technology, education, and public administration.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available in Zenodo at https://zenodo.org/records/15794815.

REFERENCES

[1] Jamal N. Al-Karaki, Awni Itradat, and Selam Mekonen. 2023. Immersive Cybersecurity Teaching/Training Using Gamification on the Metaverse: A Hands-On Case Study. In *IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, DASC/PiCom/CBDCom/CyberSciTech 2023, Abu Dhabi, United Arab Emirates, November 14-17, 2023*. IEEE, https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361297, 101–108. https://doi.org/10.1109/DASC/PICOM/CBDCOM/CY59711.2023.10361297

[2] Maria Lourdes Bacud and Sten Mäses. 2021. Game-based learning for cybersecurity awareness training programmes in the public sector. In *ECEL 2021 20th European Conference on e-Learning*. Academic Conferences International limited, 10.34190/EEL.21.044, 50.

[3] M. P. Barrett. 2018. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.* Technical Report NIST.CSWP.04162018. NIST Cybersecurity Framework. https://doi.org/10.6028/NIST.CSWP.04162018

[4] Paula Bitrián, Isabel Buil, Sara Catalán, and Dominik Merli. 2024. Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours. *Journal of Business Research* 179 (2024), 114685.

[5] Firdaous Bouzegza. 2023. Enhancing cybersecurity awareness through educational games: design of an adaptive visual novel game. *Université de Montréal* 1 (2023), 1–19.

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

[7] Yang Cao, Shaoying Gong, Yan-Qing Wang, Q. Zheng, and Zhen Wang. 2022. How to provide competitors in educational gamification: The roles of competitor level and autonomous choice. *Comput. Hum. Behav.* 138 (2022), 107477. https://doi.org/10.1016/j.chb.2022.107477

[8] Alexandru Capatina, David Juarez-Varon, Adrian Micu, and Angela Eliza Micu. 2024. Leveling up in corporate training: Unveiling the power of gamification to enhance knowledge retention, knowledge sharing, and job performance. *Journal of Innovation & Knowledge* 9, 3 (2024), 100530.

[9] Center for Internet Security. 2021. *Critical Security Controls Version 8.* Center for Internet Security. https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf

[10] Oleksandr Chumak, Serhii Holovkin, Oleksandr Piroh, Tetiana Pushkar, and Oleg Diegtiar. 2024. Information protection and cyber security in the public and financial sectors. *Edelweiss Applied Science and Technology* 8, 5 (2024), 1164–1174. https://doi.org/10.55214/25768484.v8i5.1819

[11] Emre Cinar, Paul Trott, and Christopher Simms. 2019. A systematic review of barriers to public sector innovation process. *Public management review* 21, 2 (2019), 264–290.

[12] Ewerton David Brito de Jesus, Jéssyka Vilela, and Carla Silva. 2024. Requisitos de Segurança e Privacidade em Startups: Um Estudo Empírico em uma Aplicação de Governança de Dados. In *Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024*, Márcia Lucena, Maria Lencastre, and Luciana C. Ballejos (Eds.). Even3, Brasil, https://doi.org/10.29327/1407529.27-13, 1–14. https://doi.org/10.29327/1407529.27-13

[13] Casimer M. DeCusatis, Erin Alvarico, and Omar Dirahoui. 2022. Gamification of cybersecurity training. In *Proceedings of the 1st International Workshop on Gamification of Software Development, Verification, and Validation, Gamify 2022, Singapore, 17 November 2022*, Riccardo Coppola, Luca Ardito, Mirna Muñoz, and Maurizio Leotta (Eds.). ACM, https://doi.org/10.1145/3548771.3561409, 10–13. https://doi.org/10.1145/3548771.3561409

[14] European Union Agency for Cybersecurity (ENISA). 2024. *ENISA Threat Landscape 2024.* Technical Report. ENISA, Heraklion. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[15] Faith Fatokun, Zalizah Awang, Suraya Hamid, Johnson O Fatokun, and Azah Norman. 2024. Cybersecurity knowledge deterioration and the role of gamification intervention. *Journal of Advanced Research in Applied Sciences and Engineering Technology* 43, 1 (2024), 66–94.

[16] Rodrigo Feitosa Gonçalves, Carlos Eduardo Barbosa, Matheus Argôlo, and Jano Moreira de Souza. 2025. Gamification applied to knowledge sharing in software development: A rapid review. *Information and Software Technology* 187 (2025), 107829. https://doi.org/10.1016/j.infsof.2025.107829

[17] Anderson Kevin Gwenhure and Flourensia Sapty Rahayu. 2024. Gamification of cybersecurity awareness for non-it professionals: A systematic literature review. *International Journal of Serious Games* 11, 1 (2024), 83–99.

[18] C. David Hylender, Philippe Langlois, Alex Pinto, and Suzanne Widup. 2024. 2024 data breach investigations report. *Verizon RISK Team, 17th edition, Available: https://www.verizon.com/business/resources/T3e/reports/2024-dbir-data-breach-investigations-report.pdf* 1 (2024), 1–100.

[19] IBM. 2024. *Threat Intelligence Index 2024.* Technical Report. IBM, [S. l.]. https://www.ibm.com/downloads/documents/br-pt/10a99803d4afd208

[20] Patrick Joyce. 2024. Voice of the CISO Report: Global Insights into CISO Challenges, Expectations and Priorities. *PROOFPOINT, Available: https://nationalcioreview.com/wp-content/uploads/2024/06/pfpt-us-wp-voice-of-the-CISO-report.pdf* 1 (2024), 1–22.

[21] Adele HT Kam and Irfan N Umar. 2024. Fostering autonomous motivation: a deeper evaluation of gamified learning. *Journal of Computing in Higher Education* 36, 2 (2024), 368–388.

[22] Khando Khando, Shang Gao, Sirajul M Islam, and Ali Salman. 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security* 106 (2021), 102267.

[23] Joo Baek Kim, Chen Zhong, Hong Liu, et al. 2025. The Impact of Gamification on Cybersecurity Learning: Multi-Study Analysis. *Communications of the Association for Information Systems* 56, 1 (2025), 6.

[24] Barbara A. Kitchenham and Shari Lawrence Pfleeger. 2008. Personal Opinion Surveys. In *Guide to Advanced Empirical Software Engineering*, Forrest Shull, Janice Singer, and Dag I. K. Sjøberg (Eds.). Springer, https://doi.org/10.1007/978-1-84800-044-5_3, 63–92. https://doi.org/10.1007/978-1-84800-044-5_3

[25] Jeanine Krath, Linda Schürmann, and Harald FO Von Korflesch. 2021. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Computers in human behavior* 125 (2021), 106963.

[26] Han Li, Xin Robert Luo, Paul Benjamin Lowry, and Jie Zhang. 2025. Understanding the postadoption use of gamified learning systems against the conflicting role of the game layer. *Information & Management* 62, 4 (2025), 104133.

[27] Pereira Neto Macedo. 2018. Brazilian General Data Protection Law (LGPD). *National Congress, accessed in October 18, 2019* 1 (2018), 1–31. https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

[28] Richard Matovu, Joshua C. Nwokeji, Terry S. Holmes, and Md Tajmilur Rahman. 2022. Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges. In *IEEE Frontiers in Education Conference, FIE 2022, Uppsala, Sweden, October 8-11, 2022*. IEEE, https://doi.org/10.1109/FIE56618.2022.9962519, 1–9. https://doi.org/10.1109/FIE56618.2022.9962519

[29] Marian Merritt, Susan Hansche, Brenda Ellis, Kevin Sanchez-Cherry, Julie Snyder, and Donald Walden. 2023. *Building a Cybersecurity and Privacy Learning Program.* Technical Report. National Institute of Standards and Technology.

[30] Sridevi Nair and Jain Mathew. 2023. Levelling up organisational learning through gamification: Based on evidence from public sector organisations in India. *South Asian Journal of Human Resources Management* 10, 1 (2023), 64–84.

[31] Christiano Neitzke, João Mendes, Luis Rivero, Mário Meireles Teixeira, and Davi Viana. 2023. Enhancing LGPD Compliance: Evaluating a Checklist for LGPD Quality Attributes within a Government Office. In *Proceedings of the XXII Brazilian Symposium on Software Quality, SBQS 2023, Brasilia, Brazil, November 7-10, 2023*, Edna Dias Canedo, Daniel de Paula Porto, Fábio Lúcio Lopes de Mendonça, Rafael Timóteo de Sousa Júnior, Monalessa Perini Barcellos, Ismayle de Sousa Santos, Sheila S. Reinehr, Sérgio Soares, Uirá Kulesza, Érica Ferreira de Souza, Adriano Albuquerque, Carla I. M. Bezerra, Rodrigo Pereira dos Santos, Alessandro F. Garcia, Simone Dornelas Costa, and Adolfo Gustavo Serra Seca Neto (Eds.). ACM, https://doi.org/10.1145/3629479.3629497, 218–227. https://doi.org/10.1145/3629479.3629497

[32] Bang Nguyen-Viet and Bac Nguyen-Viet. 2024. The synergy of immersion and basic psychological needs satisfaction: Exploring gamification's impact on student engagement and learning outcomes. *Acta psychologica* 252 (2024), 104660. https://doi.org/10.1016/j.actpsy.2024.104660

[33] Omid Pahlavanpour and Shang Gao. 2024. A systematic mapping study on gamification within information security awareness programs. *Heliyon* 10, 19 (2024), e38474. https://www.sciencedirect.com/science/article/pii/S2405844024145057

[34] The European Parliament and The Council. 2018. General Data Protection Regulation (GDPR). *Intersoft Consulting* 1 (2018), 1–88. https://gdpr-info.eu

[35] Mariana Peixoto, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo, and Tony Gorschek. 2023. The perspective of Brazilian software developers on data privacy. *Journal of Systems and Software* 195 (2023), 111523. https://www.sciencedirect.com/science/article/pii/S0164121222001996

[36] 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), 1–18. https://doi.org/10.1002/SMR.2755

[37] Awais Rashid, Andrew Martin, Howard Chivers, George Danezis, Steve Schneider, and Emil Lupu. 2021. The Cyber Security Body of Knowledge v1.1.0. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf. University of Bristol, Version 1.1.0.

[38] 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

[39] Richard M Ryan and Edward L Deci. 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist* 55, 1 (2000), 68.

[40] 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

[41] Ricardo Cordeiro Galvão SantAna van Erven, Demétrius de Almeida Jubé, Helen Reis Santos, Sérgio Antônio Andrade de Freitas, and Edna Dias Canedo. 2023. Gamification Project to Receive Continuous Feedback in the Context of the Evolution of Public Service for Lawyers. In *IEEE Frontiers in Education Conference, FIE 2023, College Station, TX, USA, October 18-21, 2023*. IEEE, https://doi.org/10.1109/FIE58773.2023.10343441, 1–8. https://doi.org/10.1109/FIE58773.2023.10343441

[42] Biju Varghese, Rajendran Murthy, and Sean William Hansen. 2024. Game On: Theorizing the Impacts of Gamification on Organizational Cybersecurity Training Efficacy. In *30th Americas Conference on Information Systems: Elevating Life through Digital Social Entrepreneurship, AMCIS 2024, Salt Lake City, UT, USA, August 15-17, 2024*, Michelle Carter, Kelly J. Fadel, Thomas O. Meservy, Deborah J. Armstrong, Amit Deokar, and Matthew L. Jensen (Eds.). Association for Information Systems, https://aisel.aisnet.org/amcis2024/security/security/36, 1–11.

[43] Tienhua Wu, Kuang-You Tien, Wei-Chih Hsu, and Fu-Hsiang Wen. 2021. Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences* 11, 19 (2021), 9266.