Robinson-cardenas Abanto

TEM Journa - EN - IEE - original.pdf

Universidad Peruana Union

Detalles del documento

Identificador de la entrega
trn:oid:::29566:588105176

Fecha de entrega
8 may 2026, 2:45 p.m. GMT-5

Fecha de descarga
8 may 2026, 2:48 p.m. GMT-5

Nombre del archivo
TEM Journa - EN - IEE - original.pdf

Tamaño del archivo
654.3 KB

11 páginas

6401 palabras

38.707 caracteres

8% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Grupos de coincidencias

18 Sin cita o referencia 8%
Coincidencias sin una citación ni comillas en el texto

2 Faltan citas 0%
Coincidencias que siguen siendo muy similar al material fuente

0 Falta referencia 0%
Las coincidencias tienen comillas, pero no una citación correcta en el texto

0 Con comillas y referencia 0%
Coincidencias de citación en el texto, pero sin comillas

Fuentes principales

7% Fuentes de Internet
4% Publicaciones
2% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Grupos de coincidencias

18 Sin cita o referencia 8%
Coincidencias sin una citación ni comillas en el texto

2 Faltan citas 0%
Coincidencias que siguen siendo muy similar al material fuente

0 Falta referencia 0%
Las coincidencias tienen comillas, pero no una citación correcta en el texto

0 Con comillas y referencia 0%
Coincidencias de citación en el texto, pero sin comillas

Fuentes principales

7% Fuentes de Internet
4% Publicaciones
2% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Internet	db.csstgc.com.cn 3%
2	Internet	doi.org 1%
3	Internet	etd.uum.edu.my <1%
4	Trabajos entregados	USIL-D.A. ADM. EN TURISMO (N.GUILLEN) on 2025-12-02 <1%
5	Publicación	Jose Neyra-Cruz, Jaime Haro-Enríquez, Alfredo Daza, Fernando Asin, Nemias Sabo... <1%
6	Internet	espace.etsmtl.ca <1%
7	Publicación	"Computer Science – CACIC 2017", Springer Science and Business Media LLC, 2018 <1%
8	Internet	www.wcse.org <1%
9	Publicación	"Applied Technologies", Springer Science and Business Media LLC, 2020 <1%

Quality assessment in E-Learning platform security: A model based on ISO/IEC 25000 standards

Nemias Saboya[1] , Jose Cardenas [1], Robinson Espinal [1], Jesus Abanto[1], Jose Bustamante [1]

[1] *Facultad de Ingenieria y arquitectura, Universidad Peruana Unión, Lima, Perú*

***Abstract* –The accelerated growth of e-learning exposed weaknesses in the security of digital educational platforms. In this context, a software security quality assessment model for e-learning was developed, validated, and applied. The model is based on the international standards ISO/IEC 25010, 25023, and 25040, and considers five key security aspects: confidentiality, integrity, non-repudiation, responsibility, and authenticity. For its construction, a structured catalog of metrics and an acceptance scale were developed, facilitating the objective measurement of each aspect. The instrument was validated using the Delphi method, with the participation of software evaluation experts, who confirmed the model's coherence and relevance. Subsequently, it was applied in three e-learning platforms, in collaboration with internal and external evaluators, which enabled verification of its ability to differentiate the implementation of security measures across systems. The results showed that confidentiality reached acceptable values, exceeding 70% on average, while authenticity was the most critical aspect, with values below 40% on all platforms. The attributes of integrity, responsibility, and non-repudiation were rated as only minimally acceptable, indicating limited coverage of control. In summary, the proposed model constitutes a rigorous and replicable tool to support strategic decisions, thereby contributing to the protection of sensitive information for students and teachers.**

***Keywords* – E-learning, Security, ISO/IEC 25010, ISO/IEC 25023, ISO/IEC 25040**

1. Introduction

The COVID-19 crisis, which began in late 2019, disrupted everyday life, the economy, and social interactions worldwide [1]. As part of efforts to stop the spread of the virus, most governments chose to temporarily suspend educational institutions, prioritizing the health of students, teachers, and staff [2]. In this context, there was an acceleration in the adoption of new digital technologies in the educational field, and e-learning reached maturity as the main means of teaching [3]. Educational entities adopted e-learning platforms such as Blackboard, Moodle, and Google Classroom, in addition to support platforms such as Zoom and Microsoft Teams [4], [5]. These platforms have become essential for online education, facilitating not only distance learning but also the introduction of new pedagogical methodologies. However, vulnerabilities have been discovered in e-learning platforms, highlighting the urgent need to implement mitigation strategies to face digital risks [6], [7].

E-learning platforms must be evaluated in aspects such as functionality, efficiency, usability, and security [8], [9]. To carry out this evaluation, the ISO/IEC 25000 family of standards provides a robust framework, enabling the objective measurement of these characteristics, particularly safety, through standardized metrics [10]. Its correct application

[1] DOI: xxxxxx
https://doi.org/10.18421/TEMxx-xx

Corresponding author: Nemias Saboya,
Facultad de Ingeniería y Arquitectura Universidad Peruana Unión, Lima, Perú
Email: saboya@upeu.edu.pe
Received: -----.
Revised: -----.
Accepted: -----.
Published: -----.

contributes to protecting sensitive information, reducing risks of cyberattacks, and strengthening the reputation of educational institutions [11], [12].

In the context of the rapid growth of e-learning, significant security challenges have emerged. Many educational institutions still lack a clear and standardized model for assessing the quality of security on e-learning platforms. Although international standards such as ISO/IEC 25010, ISO/IEC 25023, and ISO/IEC 25040 [13], [14] offer frameworks for assessing software quality, their specific implementation in the context of platform security remains quite limited [15].

The lack of an adequate framework for security assessment has led to vulnerabilities and gaps, putting the protection of sensitive information and the continuity of educational processes at serious risk. Therefore, it is essential to develop a security quality assessment model specifically adapted for e-learning platforms, based on the relevant ISO/IEC international standard [16], [17]. However, it is essential to note that software quality models, such as ISO/IEC 25010, McCall, Boehm, and Dromey, are more general and do not specifically address the security vulnerabilities typical of online educational environments [18].

Several studies have investigated the importance of software security, and researchers [19] emphasize the need to incorporate security from the early stages of development, utilizing the international standard ISO/IEC 25010. For its part [12], demonstrates that the application of these standards in e-learning platforms improves security, although they face challenges in terms of integrity. Other researchers, such as [20], have addressed the gap between academic teachings and industrial demands on security, proposing a maturity approach that integrates security from the design phase. [21] They analyzed the security of personal data storage in Learning Management Systems, identifying significant vulnerabilities and proposing solutions to enhance data confidentiality and security. On the other hand [22], focused on the use of emerging technologies to improve student authenticity in online assessments, addressing aspects of authentication security and preventing account sharing.

Globally, the education industry has been an ideal target for cybercriminals. According to a report by SOCRadar, in 2024, several e-learning platforms experienced a significant increase in cyberattacks, including ransomware attacks, data breaches, and phishing attacks, which affected educational institutions worldwide, including schools and universities [23]. An IBM report revealed that universities and schools have been targeted by 25% more ransomware attacks compared to the previous year, highlighting the growing threat to educational platforms [24].

In Peru, although there are no exact figures on cyberattacks specifically targeting e-learning platforms, a significant increase in cyber incidents has been observed nationwide. In 2024, Peru experienced more than 45.5 billion cyberattacks, including ransomware, phishing, and automated attacks [25]. During the APEC 2024 Summit in Lima, more than half a million cyberattacks were mitigated, demonstrating the growing threat posed by large-scale international events [26].

E-learning platforms such as Google, Moodle, and Blackboard have been breached due to different security flaws, which demonstrates the weakness of teacher and student data:

- Blackboard: In 2019, Bill Demirkapi discovered critical security errors that enabled unauthorized access to sensitive information from more than 5 million records, affecting over 5,000 schools [27].
- Moodle: A vulnerability has been identified in the Moodle Shibboleth authentication module, allowing for remote code execution and potentially compromising millions of accounts. These incidents highlight the severity of security breaches on educational platforms, which can facilitate the manipulation of grades and unauthorized access to exams [28].
- Google: In 2024, Google reached a court settlement in the U.S. after being charged with collecting biometric data from schoolchildren using G Suite for Education without parental consent. The case highlighted critical child privacy risks in digital educational environments, with respect to data protection regulations, especially in children under 13 years of age [29].

This study contributes to the development and validation of a security quality assessment model for e-learning platforms, guided by quality standards such as ISO/IEC 25010, ISO/IEC 25040, and ISO/IEC 25023. This model quantifies the security quality on e-learning platforms and identifies specific vulnerabilities using metrics based on ISO standards.

2. Methodology

This study is based on the principles of applied research, as proposed [30], which presents an evaluation model focused on understanding the various approaches related to software quality. To facilitate the understanding and use of the proposed model, a diagram was designed in accordance with the recommendations of the international standards ISO/IEC 25000. Figure 1 outlines the various phases that comprise the research.

For this, a quantitative approach is used, following the guidelines of [31], which is distinguished by an orderly and validated process, supported by reliable tools for data collection. Through numerical

analysis and statistical techniques, the study ensures the accuracy of the results and their applicability in various scenarios, supporting the effectiveness of the model with data evaluated by experts, as noted by [32].

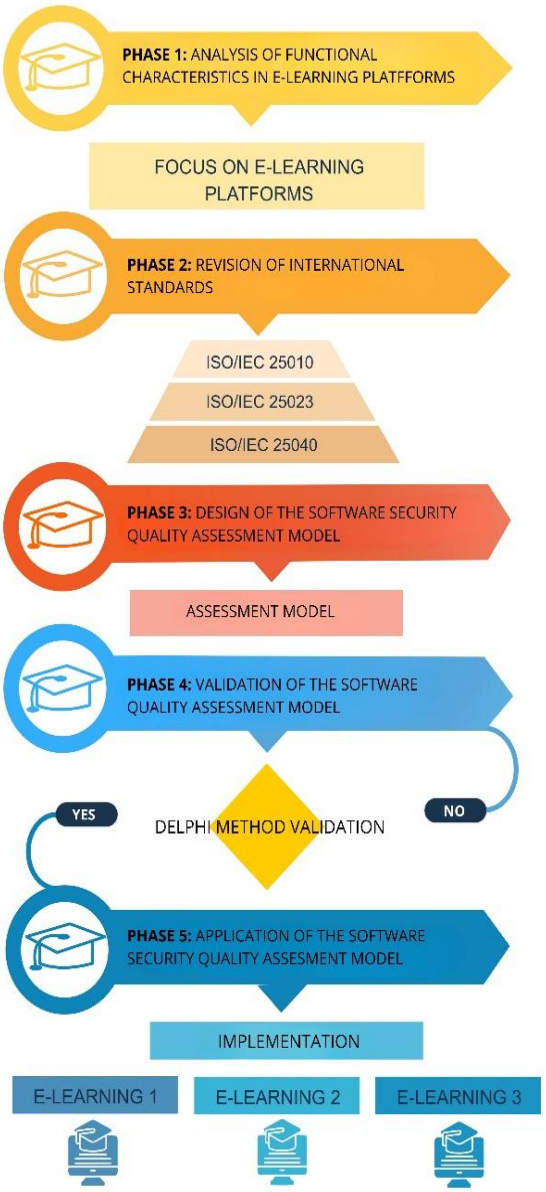

Figure 1. Phases of the investigation of the proposed evaluation model

The methodological development of the model is structured in five phases, which are described below in a summarized way.

2.2. Phase 1: Analysis of functional characteristics in e-learning platforms

In this phase, a literature review was conducted on various e-learning platforms and their functional characteristics, with a particular focus on aspects related to quality and safety. From this analysis, the most common functionalities were identified and grouped into three levels of criticality: high, medium, and low, according to the frequency with which they were reported in the studies [1], [6], [11], [12], [33]. Table I shows this classification, where it can be seen that functions such as authentication, content management, course administration, evaluation management, and forums are the most critical. At the same time, password recovery, chat, and videoconferencing are considered to have medium criticality, while virtual reality, along with the user profile, is considered to have less impact.

Table 1. Functional Feature Criticality Rating

Criticality level	*Functional characteristics*	*Studies*
High	Authentication Content management Course management Evaluation management	[1], [6], [11], [12], [13]
Medium	Forums Password recovery Chat Video conference	[1], [6], [12], [33]
Low	Virtual reality Profile	[11]

2.1. Phase 2: Revision of International Standards

In this phase, the foundation is laid for developing a reliable assessment model. To this end, an exhaustive analysis of international software quality standards and frameworks was conducted, with a particular focus on the security of e-learning platforms. Table 2 presents a comparison of different quality models, highlighting their key characteristics and citing relevant studies. This comparison enabled the clarification of how each model integrates safety, continuous improvement, ease of maintenance, and its market acceptance.

Table 2. Comparison of software quality models

Characteristics	*McCall*	*ISO 25010*	*Boehm*	*Dromey*	*ISO 9126*
Safety as a key attribute	[34]	[35]		[36]	[37]
Oriented to continuous improvement		[38]	[37]	[37]	
Maintainability evaluation		[39]			
Widespread use in industry	[40], [41]	[8]			

In Table 3, several international standards related to safety metrics were compared. This comparison was key to understanding how each standard addresses fundamental aspects such as the confidentiality, integrity, and availability of

information. This analysis facilitated the identification of the most appropriate standards to evaluate e-learning platforms, ensuring that the threats and vulnerabilities inherent to these environments were effectively covered.

Table 3. Comparison of international standards on safety metrics

Characteristics	***ISO 25023***	***Owasp metrics***	***ISO 15408***	***ISO 27005***
Confidentiality, integrity, availability	[42], [43]		[44]	[45]
International Standards	[42]		[46]	[46]
Quantitative metrics	[42]	[43]		
Applicability in IT				[45]

On the other hand, Table 4 presents a detailed analysis of the characteristics of the evaluation models. These processes were especially valuable for e-learning platforms because they offer a clear and accessible description of each stage, serving as a practical guide for technical teams and educational administrators. In this way, it was sought to ensure that the systems continuously maintained the quality standards necessary for the correct functioning of the e-learning platforms.

Table 4. Comparison of software evaluation models

Characteristics	***ISO 25040***	***ISO 15939***	***ISO 33063***	***ISO 29119***
Continuous Evaluation	[46]	[47]		[48]
International Standardization	[49]		[50]	
Focus on global software quality.	[46]			[51]
Clear definition of stages	[52]	[47]	[50]	
Process Oriented	[49]			

2.3. Phase 3: Design of the software security quality assessment model

In this phase, an evaluation model was designed to measure the level of security on e-learning platforms, based on the information collected in Phases 1 and 2. The design focused on five fundamental aspects defined by ISO/IEC 25010 [53]: Confidentiality, Integrity, Non-Repudiation, Responsibility, and Authenticity.

For the evaluation of these aspects, ISO/IEC 25040 [49] was chosen, which guarantees a structured evaluation process that includes process inputs and outputs, limitations, and resources, thus ensuring that the evaluation model is technical and reliable.

On the other hand, the 10 external security metrics defined in ISO/IEC 25023 [42], taking into account the characteristics or functionalities of the e-learning platforms described in Table 6. Based on the metrics, an instrument was developed to serve as the basis and evaluation tool for the e-learning platforms. This instrument is structured around the 5 security aspects and the 10 corresponding metrics. The confidentiality aspect consists of 21 items, Integrity of 18 items, Non-Repudiation of 9 items, Responsibility of 13 items, and Authenticity of 36 items; each item has three alternatives (Yes, No, and Not Applicable). According to the results, the formula for the metric is applied and averaged for each aspect evaluated. For the final result, the value of the aspect is multiplied by a certain weight (Confidentiality = 0.4, Integrity =0.15, Non-Repudiation =0.05, Responsibility = 0.10 and Authenticity = 0.30), and finally, the results are added and verified on what scale it is according to Table V, where an acceptance scale is defined considering the scores obtained by the evaluated platform: "Unacceptable", "Minimally Acceptable", "Target Range", and "Exceeds the Requirements" said scales are presented in Table 5

Table 5. Acceptance scale for safety assessment

Acceptance level	***Measurement Scale***
Unacceptable (I)	0 <= X < 40
Minimally Acceptable (MA)	40 <= X < 60
Target range (RO)	60 <= X < 90
Exceeds requirements (ER)	90 <= X < 100

The final design of the model articulates aspects, metrics, and scale in an evaluation process structured in five stages, as presented in Figure 2. Stage 1 (Establish) identifies the most relevant security aspects that will be used to evaluate the e-learning platform. Stage 2 (Specify) involves selecting and weighting the most appropriate metrics to evaluate the aspects identified in Stage 1, with reference to the ISO/IEC 25023 standard. Stage 3 (Design) customizes the evaluation instrument according to the specific characteristics of the e-learning platform's context. Stage 4 (Execute) corresponds to the application of the instrument in practice, where the evaluation process is developed in a structured and controlled manner, in accordance with the provisions of ISO/IEC 25040. Finally, in Stage 5 (Conclude), the results obtained are processed and analyzed, generating a report that determines the level of general acceptance of the evaluated platform and each safety aspect defined in Table 6.

Table 6. Security metrics based on ISO/IEC 25023

Key aspects	***Metrics***	***Description***	***Formula***
Confidentiality	1. Access control	What proportion of sensitive data is protected from unauthorized access?	X = 1 - (A / B) A = Number of sensitive data that can be accessed without authorization B = Number of data requiring access control
	2. Data encryption	How well is the encryption/decryption of data elements implemented as specified in the requirements?	X= A / B A= Number of data encrypted/decrypted correctly B= Number of data requiring encryption/decryption
	3. Cryptographic algorithms	What proportion of cryptographic algorithms have been well evaluated?	X = 1 - A/B A= Number of broken or unacceptably risky cryptographic algorithms in use B= Number of cryptographic algorithms used
Integrity	4. Data integrity	To what extent has corruption or modification of data due to unauthorized access been prevented?	X = 1 - A/B A= Number of data items that have been effectively corrupted by unauthorized access B= Number of data elements for which corruption or modification must be prevented
	5. Internal data corruption prevention	To what extent has corruption or modification of data due to unauthorized access been prevented?	X= A /B A= Number of data corruption prevention methods actually implemented B= Number of data corruption prevention methods available and recommended
Non-Repudiation	6. Using a digital signature	What is the proportion of events requiring non-repudiation processed using digital signatures?	X=A/B A= Number of events that ensure non-repudiation using a digital signature B= Number of accesses to the system and the data registered in the system log
Responsibility	7. Integrity of the user audit trail	How complete is the audit trail regarding user access to the system or data?	X = A/B A= Number of accesses registered in all records (logs) B= Number of accesses to the system or to the data actually verified
	8. System Record Retention	How long is the system log retained in percentage stable storage?	X=A/B A= Duration for which the system log is effectively kept in stable storage B= Retention period specified to keep the system log in stable storage
Authenticity	9. Sufficiency of the authentication mechanism	How well does the system authenticate a subject's identity?	X=A/B A= Number of authentication mechanisms provided (for example, user ID/password or IC card) B= Number of authentication mechanisms specified
	10. Compliance with authentication rules	What is the proportion of the required authentication rule that is set?	X=A/B A= Number of authentication rules implemented B= Number of authentication rules specified

2.4. Phase 4: Validation of the software quality assessment model

During the fourth phase, the instrument for model validation was developed; this instrument consists of five dimensions: alignment with e-learning platforms and ISO standards, with two items; methodology and metrics, with three items; objectivity, with four items; effectiveness, with two items; and ease of use, with three items. The Delphi method was then used to validate the model. This method involves assembling a panel of experts to reach a consensus on a specific problem or issue. For this purpose, experts in cybersecurity, quality, and software evaluation were selected to make a value judgment using the aforementioned validation instrument. Iterative feedback was conducted with the experts until a consensus was reached, and the model was subsequently validated, as illustrated in Figure 3, which outlines the model validation process.

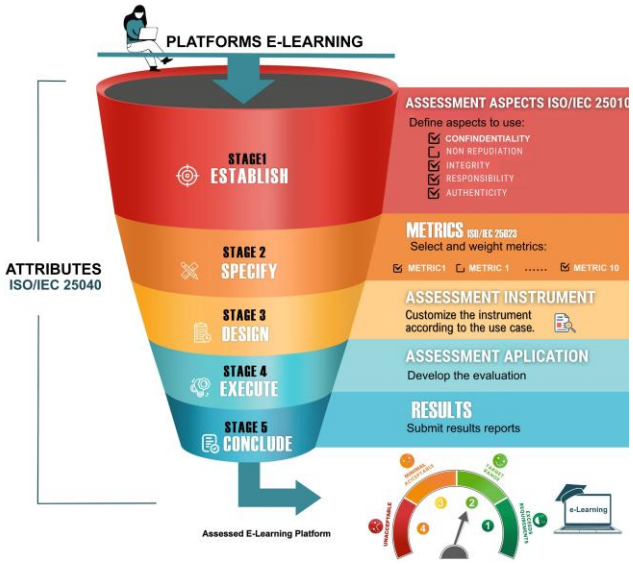

Figure 2. Final design of the safety assessment model

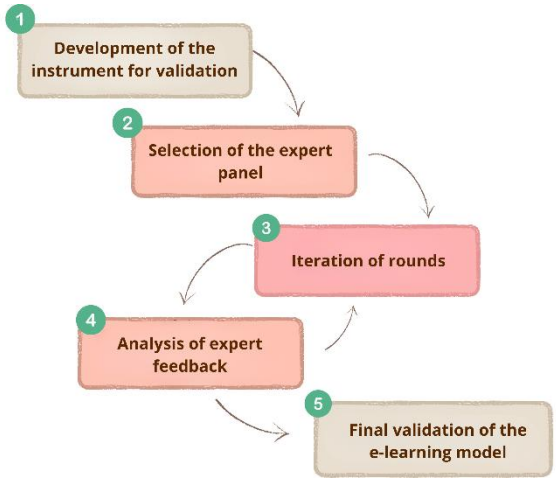

Figure 3. Validation process of the proposed model (Delphi method)

2.5. Phase 5: Application of the software security quality assessment model

Finally, in Phase 5, the security quality assessment model was implemented in three different e-learning platforms. To do this, firstly, a detailed plan was developed that defined the platforms, modules and tools to be evaluated, as well as the quality methods and metrics to be applied, then the evaluators carried out the measurements, three evaluations were obtained for each platform, of which one result was by an internal technical evaluator of the development team, an internal evaluator with an auditor profile and an external safety expert evaluator. Subsequently, the acquirer reviewed the results to make decisions about the adoption or improvement of the platforms, generating a report with final recommendations based on the evaluated quality attributes.

3. Results

The security quality assessment model was applied to educational platforms of three different institutions: Platform A, Platform B and Platform C, in each of these platforms three evaluators were assigned who used the instrument developed and validated in the study, the roles of these evaluators were: "Internal Auditor (AI)", "External Evaluator (EE)" and "Technical Leader (LT)".

Figure 4 shows the consolidated results of the three e-learning platforms in the five security aspects evaluated. In Platform A, the results show uneven performance in the five security aspects evaluated. Confidentiality reaches the "Target Range" with values greater than 60% in the three evaluations (LT: 77%, AI: 87%, and EE: 68%), indicating that there are adequate mechanisms in place to protect the sensitive information of users. However, authenticity reflects a clear weakness, with very low scores (LT: 38%, AI: 25%, and EE: 22%), indicating an "Unacceptable" level and posing serious risks to the validation of users' identities. Regarding integrity, the results are heterogeneous: while the technical leader reports 71%, the other evaluators indicate very low levels (EE: 38% and AI: 13%), which suggests a lack of consistency in the controls implemented. The responsibility is divided 50% between the internal auditor and external evaluator, classified as "Minimally Acceptable," and the technical leader at 75%, which reflects limitations in the traceability of actions within the system. Finally, the evaluation of the Non-Repudiation aspect is not contemplated because the objective of the e-learning platform does not require such functionality.

In Platform B, the results indicate progress in certain security aspects, although significant weaknesses persist. Confidentiality obtains relatively stable values (LT: 64%, AI: 70%, and EE: 70%),

placing it within a "Target Range", which indicates a good level of protection. In terms of authenticity, the three evaluators agree on a low score (38%), ranking it in the "Unacceptable" level. This finding reveals a significant lack in identity validation and represents a critical risk to the platform's reliability. Integrity presents a mixed evaluation: while the Internal Auditor achieves 64%, the other evaluators record lower results (LT: 50% and EE: 48%), falling within the "Minimally Acceptable" range. This reflects that data consistency controls are not fully secured. Responsibility is the strongest point of Platform B, with maximum values (AI: 100% and EE: 100%), although the Technical Leader only scores 50%. Overall, this aspect can be considered acceptable, as it highlights the presence of traceability mechanisms, although there are differences in the evaluators' perceptions. Finally, non-repudiation receives a critical rating (0% in EE and AI, and 44% in LT), which places this aspect at the "unacceptable" level, revealing the lack of controls that ensure transaction verification and the impossibility for a user to deny their participation in them.

In Platform C, the results indicate acceptable performance in certain security aspects, although critical gaps persist that impact the overall confidence in the system. Confidentiality shows consistent values (LT: 65%, AI: 75% and EE: 76%), reaching the "Target Range" and evidencing an optimal level of information protection. As for authenticity, the three evaluators agree on very low scores (LT: 31%, AI: 22%, and EE: 22%), indicating a clearly "Unacceptable" level. This weakness is the most critical point of the platform, since it puts the veracity of the users' identity at risk. Integrity obtains mixed results: while the Internal Auditor registers 38% "Unacceptable", the Technical Leader achieves 71% and the External Evaluator 33%, the latter falls within the "Unacceptable" range. This variability reflects the lack of uniformity in the mechanisms that ensure data consistency and integrity. In the case of responsibility, the three evaluators assign 50%, placing this aspect at the "Minimally Acceptable" level. Although there is traceability in the actions, there is no evidence of solid control that allows for detailed monitoring of the operations. Finally, non-repudiation presents a heterogeneous situation: the Technical Leader and the Internal Auditor report low values (67% and 44%, respectively), while the External Evaluator reports a higher value of 33%. This places this aspect between the "Unacceptable" and the "Minimally Acceptable", which casts doubt on the system's ability to guarantee the validation of transactions and the non-denial of responsibilities.

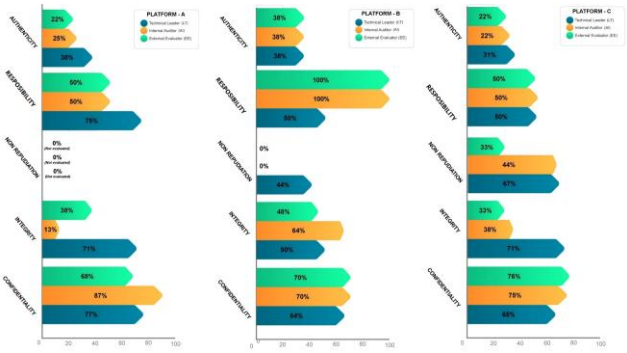

Figure 4. Result of the assessment of the security quality of e-learning platforms

Finally, the results were consolidated in Figure 5 considering the five key security aspects by the three platforms; all platforms are within the "Minimally Acceptable" scale, although the confidentiality aspect reaches the expected level in all platforms, the general picture is worrying, since the authenticity aspect is the weakest link, since their evaluations score an "Unacceptable" level in the three platforms analyzed, which raises serious doubts about the identity of the users and the veracity of the data. Other aspects, such as integrity, responsibility, and non-repudiation, also exhibit deficiencies, leaving information systems in a "Minimally Acceptable" state. These findings underscore the need to strengthen access controls, authentication policies, and security standards on e-learning platforms.

All platforms have weaknesses reported by the three evaluators of each of them, however, some vulnerabilities are shown in Table VII as the main ones because they appear in all the evaluations, this reveals that they need rules to strengthen their authentication mechanism and implement clear conforming security policies while it is recommended to invest in updating technologies for authentication and encryption, to guarantee compliance with the aspects of authenticity, confidentiality and integrity defined in ISO/IEC 25010.

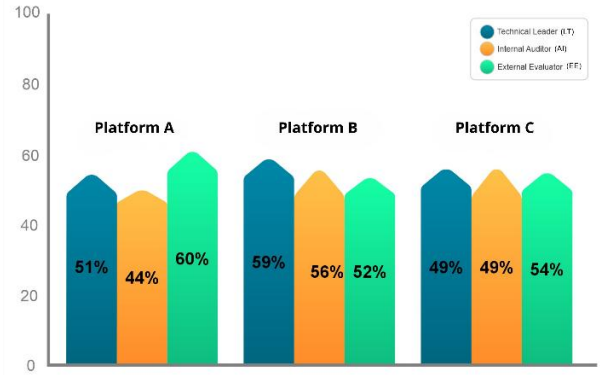

Figure 5. Consolidated results of the three e-learning platforms

Table 7. Principal vulnerabilities detected in the evaluated platforms

Aspect	*Criteria Evaluated*	*Identified vulnerability*
Authenticity	Compliance with authentication rules	Temporary passwords with no defined validity period
		Non-generic error messages in the login (can filter information)
		No mandatory password change after a defined period
		No MFA or reauthentication for critical functions
	Sufficiency of the authentication mechanism	No integration with a single-use authentication (OTP) application
		No integration with multiple authentication applications
		No limit on failed attempts with authentication apps
		No limit on attempts for password recovery
		Failure to prevent the use of personal information as a password
Confidentiality	Access control	Unauthorized access to credentials
	Data encryption	Certificates, diplomas, and qualifications without encryption
	Cryptographic algorithms	Use of MD5 for hashing (vulnerable to collisions)

4. Discussion

The results obtained validate the proposed evaluation model as an effective tool for diagnosing the level of security on e-learning platforms. Unlike the approach proposed in [12], which focuses exclusively on usability and user experience, the model developed in this study explicitly addresses software security quality, incorporating five critical aspects defined by the ISO/IEC 25010 standard. This enables a more technical and structured evaluation, considering key elements such as authenticity, non-repudiation, and responsibility, which are essential in environments where sensitive student and teacher data are managed.

For its part, the proposal presented in [18] is based on a set of general quality indicators applicable to learning management systems. However, this approach lacks a structure based on specific technical standards such as ISO/IEC 25023 and does not include a validated catalog of metrics directly applicable to software security analysis. In contrast, the present study incorporates normative metrics integrated into an instrument designed and validated through expert judgment.

In addition, the differentiated results between the evaluated platforms demonstrate the model's discriminatory capacity, clearly identifying particular strengths and weaknesses. For example, the observed differences in confidentiality and authenticity between platforms B and C reflect substantial variations in the implementation of access controls, encryption, and authentication mechanisms. These distinctions enable technology decision-makers to make informed decisions to mitigate risks and improve institutional data protection.

Finally, although the model demonstrated solid results in its validation and initial application, the reduced sample size is recognized as a limitation. Therefore, its application is recommended on a greater number of platforms and in diverse institutional contexts to strengthen its external validity and expand its practical applicability in the digital educational field.

5. Conclusion

This study presented a software security quality assessment model for e-learning platforms, based on ISO/IEC 25010, 25023, and 25040 standards. The model was developed in five phases and integrates five security aspects, a structured catalog of technical metrics, and an acceptance scale validated through expert judgment.

The application of the model across three educational platforms enabled the identification of significant differences in compliance with safety criteria. The results showed that the instrument can accurately discriminate between platforms with different levels of technical maturity in key aspects such as confidentiality, authenticity, and responsibility.

Unlike previous proposals [12], [18], the model presented is based on international standards and offers a quantitative structure that facilitates the reproducible evaluation of digital educational systems. This makes it a valuable tool for both audit processes and the continuous improvement of technological platforms in academic environments.

As future work, it is proposed to extend the application of the model to a larger sample of platforms, as well as to explore its integration in hybrid or mobile environments, where security remains a significant challenge. It is also recommended to evaluate the model's adaptability to other software domains beyond the educational field.

References

[1]. Alkabaa, A. S. (2022). Effectiveness of using E-learning systems during COVID-19 in Saudi Arabia: Experiences and perceptions analysis of engineering students. *Education and Information Technologies*, *27*(8), 10625–10645. Doi: 10.1007/s10639-022-11054-z

[2]. Kaur, J., & Kumar, P. (2022). Teachers' perception of online teaching and its effects on learning outcome during Covid-19: an India based mixed method study. *Journal of E-Learning and Knowledge Society*, *18*(2), 11–21. Doi: 10.20368/1971-8829/1135450

[3]. Saloom, R. H., Elameer, A. S., & Jalal, A. S. (2018). A new style of an academic institutions in Iraq: E-University. *Proceedings of the 1st Annual International Conference on Information and Sciences (AiCIS 2018)*, 187–192. Doi: 10.1109/AiCIS.2018.00044

[4]. Turnbull, D., Chugh, R., & Luck, J. (2021). Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge? *Education and Information Technologies*, *26*(5), 6401–6419. Doi: 10.1007/s10639-021-10633-w

[5]. Chatti, H., & Hadoussa, S. (2021). Factors Affecting the Adoption of E-Learning Technology by Students during the COVID-19 Quarantine Period: The Application of the UTAUT Model. *Engineering, Technology & Applied Science Research*, *11*(2), 6993–7000. Doi: 10.48084/etasr.3985

[6]. Akacha, S. A. L., & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability*, *15*(19), 14132. Doi: 10.3390/su151914132

[7]. Rathgeb, C., Poppelmann, K., & Busch, C. (2021). Face morphing attacks: A threat to eLearning? *Proceedings of the IEEE Global Engineering Education Conference (EDUCON 2021)*, 1149–1154. Doi: 10.1109/EDUCON46332.2021.9454128

[8]. Thamilarasan, Y., Raja Ikram, R. R., Osman, M., Salahuddin, L., Wan Bujeri, W. Y., & Kanchymalay, K. (2023). Enhanced System Usability Scale using the Software Quality Standard Approach. *Engineering, Technology and Applied Science Research*, *13*(5), 11779–11784. Doi: 10.48084/etasr.5971

[9]. Awangditama, B. R., Mardhatillah, L., & Rochimah, S. (2023). Quality Conformity Analysis Functional and Usability in Academic Information Systems Using ISO/IEC 25010. Proceedings of the 14th International Conference on Information and Communication Technology and System (ICTS 2023), 24–28. Doi: 10.1109/ICTS58770.2023.10330881

[10]. Schaffernak, H., Moesl, B., Url, P., Victoria Koglbauer, I., & Vorraber, W. (2025). Towards sustainable software quality in use: a review of measures. Next Research, 2(3), 100680. Doi: 10.1016/j.nexres.2025.100680

[11]. Manglapuz, S. J. R., & Lacatan, L. L. (2019). Academic management android application for student performance analytics: A comprehensive evaluation using ISO 25010:2011. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 5085–5089. Doi: 10.35940/ijitee.L2735.1081219

[12]. Sekarini, D., Alfiani, F. S., & Rochimah, S. (2020). Security Characteristic Evaluation of New Students Admission Information System Based on ISO/IEC 25010 Quality Standard. *Proceedings of the 12th International Conference on Information Technology and Electrical Engineering (ICITEE 2020)*, 120–124. Doi: 10.1109/ICITEE49829.2020.9271756

[13]. Aziz, M. N., Sapta, I. M., & Rochimah, S. (2018). Security Characteristic Evaluation Based on ISO/IEC 25023 Quality Model, Case Study: Laboratory Management Information System. *Proceedings of the Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS 2018)*, 332–336. Doi: 10.1109/EECCIS.2018.8692982

[14]. Yenny Milagritos Sifuentes Díaz, & José Luis Peralta Luján. (2022). Modelo de medición y evaluación de calidad del software basado en la norma ISO/IEC 25000 para medir la usabilidad en productos de software académicos universitarios. *Tecnohumanismo*, *2(1)*, 181–204 Doi: 10.53673/th.v2i4.125

[15]. Purbaratri, W., Hartomo, K. D., Hendry, & Tambotoh, J. J. C. (2023). The New Smart Government Software Quality Framework Uses Modifications to ISO/IEC 25010. *Proceedings of the 8th International Conference on Informatics and Computing (ICIC 2023)*, 1-6 Doi: 10.1109/ICIC60109.2023.10382109

[16]. Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information (Switzerland), 13(4). Doi: 10.3390/info13040192

[17]. Ivanova, M., Trifonova, I., & Bogdanova, G. (2022). Privacy Preservation in eLearning: Exploration and Analysis. *Proceedings of the 20th International Conference on Information Technology Based Higher Education and Training (ITHET 2022)*, 1-8 Doi: 10.1109/ITHET56107.2022.10031904

[18]. Peters, E., & Aggrey, G. K. (2020). An ISO 25010 based quality model for ERP systems. Advances in Science, Technology and Engineering Systems, 5(2), 578–583. Doi: 10.25046/aj050272

[19]. Haoues, M., Sellami, A., Ben-Abdallah, H., & Demirors, O. (2019). Evaluating Software Security Change Requests: A COSMIC-Based Quantification Approach. *Proceedings of the 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2019)*, 268–275. Doi: 10.1109/SEAA.2019.00049

[20]. Al-Matouq, H., Mahmood, S., Alshayeb, M., & Niazi, M. (2020). A Maturity Model for Secure Software Design: A Multivocal Study. IEEE Access, 8, 215758–215776. Doi: 10.1109/ACCESS.2020.3040220

[21]. Amo, D., Alier, M., García-Pĕalvo, F. J., Fonseca, D., & Casany, M. J. (2019). GDPR security and confidentiality compliance in LMS' a problem analysis and engineering solution proposal. Proceedings of the ACM International Conference Proceeding Series, 253–259. Doi: 10.1145/3362789.3362823

[22]. Herrera-Cubides, J. F., Gaona-García, P. A., & Salcedo-Salgado, G. A. (2019). Towards the construction of a user unique authentication mechanism on LMS platforms through model-driven engineering(MDE). Scientific Programming, 2019. Doi: 10.1155/2019/9313571

[23]. SoCRadar. (2024). *Education Industry Biggest Attacks in 2024*. SoCRadar. Retrieved from: https://socradar.io/biggest-education-industry-attacks-in-2024/ [accessed: 01 October 2024]

[24]. IBM. (2024). *Reducing ransomware recovery costs in education.* Jennifer Gregory. Retrieved from: https://www.ibm.com/think/insights/reducing-ransomware-recovery-costs-in-education [accessed: 01 October 2024]

[25]. Infobae. (2025). *Perú registró 45 mil millones de ciberataques en 2024: así puedes proteger tu pyme sin ser experto en tecnología.* Infobae. Retrieved from : https://www.infobae.com/peru/2025/05/22/peru-registro-45-mil-millones-de-ciberataques-en-2024-asi-puedes-proteger-tu-pyme-sin-ser-experto-en-tecnologia/ [accessed: 03 October 2024]

[26]. APEC Peru 2024. (2024). *APEC Peru 2024 successfully fended off more than half a million cyberattacks*. APEC Perú. Retrieved from: https://www.apecperu.pe/2024/en/2024/11/22/apec-peru-2024-successfully-fended-off-more-than-half-a-million-cyberattacks/ [accessed: 03 October 2024]

[27]. Greenberg, A. (2019). *Teen hacker exposes vulnerabilities in Blackboard.* Wired. Retrieved from: https://www.wired.com/story/teen-hacker-school-software-blackboard-follett [accessed: 09 October 2024]

[28]. Paganini, P. (2020). *Moodle account takeover threats. In Security Affairs.* Affairs. Retrieved from: https://securityaffairs.com/116560/hacking/moodle-account-takeover-threats.html [accessed: 09 October 2024]

[29]. Kimery, A. (2024). *Google settles over kids' biometric data collection in schools.* Biometric Update. Retrieved from: https://www.biometricupdate.com/202408/google-settles-over-kids-biometric-data-collection-in-schools [accessed: 10 October 2024]

[30]. Silva Vernier, L., Dartora, J., Herbert, J., Cazella, S. C., & Centenaro Levandowski, D. (2021). *Model for quality analysis of neonatal hearing screening software: theory applied. International* Journal of Medical Informatics, 150, 104435.

[31]. Hernández Sampieri, R., Fernández Collado, C., & María del Pilar Baptista Lucio, M. (2014) *Metodologia de la investigacion sexta edicion.* mcgraw-hill & interamericana.

[32]. Aponte Figueroa, G., Cardozo Montilla, M. A., & Melo, R. M. (2012). *metodo delphi: aplicaciones y posibilidades en la gestion prospectiva de la investigacion y desarrollo.* Revista Venezolana de Análisis de Coyuntura, XVIII(1), 41-52

[33]. Djeki, E., Degila, J., Bondiombouy, C., & Alhassan, M. H. (2022). *Preventive Measures for Digital Learning Spaces' Security Issues.* 2022 IEEE TEMSCON EUROPE 2022, 48–55. Doi: TEMSCONEUROPE54743.2022.9801945.

[34]. Budi, S., Gata, W., Noor, M., Pangabean, S., & Rahayu, C. S. (2022). *News Portal Website Measurement Analysis Using ISO/IEC 25010 And McCall Methods.* Journal of Applied Engineering and Technological Science (JAETS), 4(1), 273–285. Doi: 10.37385/jaets.v4i1.1094.

[35]. Marroquin, J. P., & Rodriguez, C. R. (2023). Quality Assessment Model Based on ISO/IEC 25010 for E-Learning Platforms in the Cloud and Based on Laravel. *Proceedings - 2023 15th IEEE International Conference on Computational Intelligence and Communication Networks*, CICN 2023, 751–757. Doi: 10.1109/CICN59264.2023.10402281

[36]. Raffoul, E., Domínguez, K., Pérez, M., Mendoza, L. E., & Grimán, A. C. (2008). Quality model for the selection of floss-based issue tracking system. *Proceedings of the IASTED*

International Conference on Software Engineering, SE 2008, 43–49.

[37]. Ortega, M., Pérez, M., & Rojas, T. (2003). *Construction of a Systemic Quality Model for Evaluating a Software Product. Software Quality Journal, 11(3), 219–242. Doi: 10.1023/A:1025166710988*

[38]. Chand, R., Khan, S. U. R., Hussain, S., Wang, W.-L., Tang, M.-H., & Ibrahim, N. (2024). Exploring Software Quality Through Data-Driven Approaches and Knowledge Graphs. *Proceeding of the Good practices and new perspectives in information systems and technologies Lecture Notes in Networks and Systems*, vol 990, 373–382. Doi: 10.1007/978-3-031-60328-0_37

[39]. Aguirre, A. F., Villareal-Freire, Á., Gil, R., & Collazos, C. A. (2017). Extending the concept of user satisfaction in e-learning systems from ISO/IEC 25010. *Proceedings of the Lecture Notes in Computer,* vol 10290, 167–179. Doi: 10.1007/978-3-319-58640-3_13

[40]. Wang, S.-H., Samadhiya, D., & Chen, D. (2011). *Software quality: Role and value of quality models.* International Journal of Advancements in Computing Technology, 3(6), 65–74. Doi: 10.4156/ijact.vol3.issue6.9

[41]. Wolski, M., Walter, B., Kupiński, S., & Chojnacki, J. (2018). *Software quality model for a research-driven organization—An experience report.* Journal of Software: Evolution and Process, 30(5). Doi: 10.1002/smr.1911

[42]. Falco, M., Scott, E., & Robiolo, G. (2020). Overview of an automated framework to measure and track the quality level of a product. *Proceedings of the* 2020 IEEE Congreso Bienal de Argentina, ARGENCON 2020. Doi: 10.1109/ARGENCON49523.2020.9505405

[43]. Sonmez, F. O., & Kilic, B. G. (2021*). Holistic Web Application Security Visualization for Multi-Project and Multi-Phase Dynamic Application Security Test Results.* IEEE Access, 9, 25858–25884. Doi: 10.1109/ACCESS.2021.3057044

[44]. Nakai, H., Tsuda, N., Honda, K., Washizaki, H., & Fukazawa, Y. (2016). Initial Framework for Software Quality Evaluation Based on ISO/IEC 25022 and ISO/IEC 25023. *Proceedings of the 2016 IEEE International Conference on Software Quality, Reliability and Security-Companion, QRS-C 2016, 410–411*. Doi: 10.1109/QRS-C.2016.66

[45]. Taylor, S., Surridge, M., & Pickering, B. (2021). Regulatory Compliance Modelling Using Risk Management Techniques. *Proceedings of the* IEEE World AI IoT Congress, 474–481. *Doi: 10.1109/AIIoT52608.2021.9454188*

[46]. Dhouib, A., Trabelsi, A., Kolski, C., & Neji, M. (2017). *Prioritizing the usability criteria of adaptive user interfaces of information systems based on ISO/IEC 25040 standard*. Ingenierie Des Systemes d'Information, 22(4), 107–128. Doi: 10.3166/ISI.22.4.107-128

[47]. Monla, Z., Assila, A., Beladjine, D., & Zghal, M. (2024). Maturity Measurement Framework for Evaluating BIM-Based AR/VR Systems Adapted from ISO/IEC 15939 Standard. *Proceeding of the Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14721 LNCS, 79–95. Doi: 10.1007/978-3-031-61318-0_7

[48]. Patrício, C., Pinto, R., & Marques, G. (2021). *A Study on Software Testing Standard Using ISO/IEC/IEEE 29119-2: 2013*. Studies in Systems, Decision and Control, 295, 43–62. Doi: 10.1007/978-3-030-47411-9_3

[49]. Calabrese, J., Esponda, S., Pasini, A., & Pesado, P. (2021). *Data Evaluation Model Using GQM Approach.* Communications in Computer and Information Science, 1409 CCIS, 141–154. Doi: 10.1007/978-3-030-75836-3_10

[50]. Carpio, A. F. Del. (2018). *Visualizing composition and behavior of the ISO/IEC 33000 assessment framework through a multi-layer model.* Computer Standards and Interfaces, 60, 3–12. Doi: 10.1016/j.csi.2018.04.008

[51]. Buchalcevova, A. (2021). *Towards higher software quality in very small entities: ISO/IEC 29110 software basic profile mapping to testing standards.* International Journal of Information Technologies and Systems Approach, 14(1), 1–16. Doi: 10.4018/IJITSA.2021010105

[52]. Yuan, Y., Wu, X., Lu, Y., Esaki, K., Azuma, M., & Komiyama, T. (2013). Introduction of Quality Requirement and Evaluation Based on ISO/IEC SQuaRE Series of Standard. *Proceedings of the Communications in Computer and Information Science*, vol 320, 94–101. Doi: 10.1007/978-3-642-35795-4_12

[53]. Rojas, H., Renteria, R., Duran, V. M., Gutiérrez, Y. T., Cabrera, M. J. I., & Aminuddin, A. (2025). *Mapping the Evolution and Future Directions of ISO/IEC 25010: A Bibliometric and Thematic Analysis. Engineering,* Technology & Applied Science Research, 15(5), 27530–27541. Doi: 10.48084/etasr.11772.