OmniaScience

Journal of Technology and Science Education

JOTSE, 2024 – 14(4): 965-989 – Online ISSN: 2013-6374 – Print ISSN: 2014-5349

https://doi.org/10.3926/jotse.2275

QUALITY AND SECURITY AS KEY FACTORS IN THE DEVELOPMENT OF COMPUTER AUDITS IN HIGHER EDUCATION INSTITUTIONS

Daisy Imbaquingo[1,2*], Javier Díaz[1*], José Jácome[2]

[1]Universidad Nacional de La Plata (Argentina)

[2]Universidad Técnica del Norte (Ecuador)

**Corresponding author: daisy.imbaquingoe@info.unlp.edu.ar*
javierd@info.unlp.edu.ar, jgjacome@utn.edu.ec

Received June 2023
Accepted March 2024

Abstract

Higher Education Institutions (HEIs) need a specialized computer audit method to minimize quality and security risks and facilitate institutional evaluation and accreditation. This study aimed to develop a Computer Audit Method for HEIs (MAIIES) providing methodological support for the computer audit process. The MAIIES method includes planning, execution, communication of results, validation, and follow-up of the audit exercise with 47 activities. The validation phase resulted in an evaluation instrument with 42 variables for quality and 18 for security, forming a multivariate model measuring quality and security dimensions. The model comprises factors such as human, technical, contextual, confidentiality, integrity, and availability. The MAIIES method provides a comprehensive audit framework, facilitating compliance with quality and security standards and identifying areas of improvement. It offers a strategic approach for minimizing quality and security risks in HEIs through a comprehensive computer audit process, enabling institutional evaluation and accreditation by ensuring compliance with quality and security standards and identifying areas of improvement.

Keywords – Computer audit, Institutions of higher education, Quality, Security, Factors, Metrics.

To cite this article:

Imbaquingo, D., Díaz, J., & Jácome, J. (2024). Quality and security as key factors in the development of computer audits in higher education institutions. *Journal of Technology and Science Education,* 14(4), 965-989. https://doi.org/10.3926/jotse.2275

---

1. Introduction

The great demand for the use of Information and Communication Technologies (ICT) in various institutions of any environment has involved irregular behaviors occurring daily, which require monitoring and control processes such as audits to minimize risks now of using equipment, facilities, hardware, and software, in addition to seeking the best alternatives in terms of investment and proper use of technology.

Starting from this, it can be understood that organizations are increasingly dependent on information; therefore, protecting sensitive and valuable information becomes a strategic capacity that guarantees business sustainability, profitability, and the global value of a company (Hohan, Olaru & Pirnea, 2015). In

this context, guaranteeing the good use of each of these services allows the sustainable progress of the organization, maintaining a competitive advantage, protecting the reputation, ensuring compliance, and applying laws and regulations (O'Hanley & Tiller, 2013).

An audit can be defined as accumulating and evaluating evidence of specific, quantifiable information carried out by independent and competent persons to determine and report the degree of correspondence between quantifiable information and established standards (Campos-Pacurucu, Narváez-Zurita, Eràzo-Álvarez & Ordoñez-Parra, 2019; Rodríguez-Labrada, Cano-Inclán & Cuesta-Rodríguez, 2018). In turn, computer audits allow the diagnosis and evaluation of the computer environment (hardware, software, databases, networks, facilities, etc.), in which those responsible for the computer area, administrators, accountants, general auditors, and coordinators of processes are executed in the organization. Their participation occurs in different phases of the process: planning, execution (information gathering), analysis of results, and finding useful evidence in preparing the final report (Arcentales-Fernández & Caycedo-Casas, 2017).

Over the years, the Computer Audit has gone from being a support activity in the financial area to being the protagonist in Information Technology (IT) processes; it is a fundamental activity in the growth of any organization that handles critical information and implements technological infrastructure and information systems, thus guaranteeing security, internal operational control, efficiency, effectiveness, continuity of operations, and risk management, which support decision-making and continuous improvement (Imbaquingo, Pedro, Diaz, Saltos & Arciniega, 2021). However, there is no standard and proven methodology for the audit of Higher Education Institutions (HEIs), and no guidelines allow comparison of the results obtained (Soy-i-Aumatell, 2003). Concerning Ecuadorian (HEIs), the topic has not been of interest so far, so the computer audit procedures they use have not been standardized.

HEIs must integrate their processes to ensure their correct action and sustainability projections (García & González, 2020) to transform and improve the social environment. In this context, three substantive functions are specified that are executed by the action of knowledge: teaching, research, and linking or extension (Ley Orgánica de Educación Superior [LOES], 2018). Starting from the substantive functions and considering that information systems management is developed in Higher Education Institutions (HEIs) in both the strategic and operational parts, the modules or systems play a leading role as main axes of management, thus becoming an essential requirement (García & González, 2020; Rodríguez-Labrada et al., 2018). The problem is evident as far as information is concerned, for which reason audits are used, which include the process of collecting and evaluating evidence to establish criteria on whether the Information System (IS) may or may not protect existing assets and information technology to maintain data integrity (Rodríguez-Labrada et al., 2018). However, only 12% of HEIs in Ecuador carry out computer audits periodically because their importance is unknown or they lack specialized departments in the area (Cadena, Córdova, Enríquez & Padilla, 2019).

Without a modern and focused method for HEIs, each audit team imposes its procedures and personal criteria, generating quality and security problems in audit information. Furthermore, the quality of audits and information security has been the subject of interest in academic, professional, and legal debates because of a series of corporate collapses and the low levels of results obtained in the execution of previous audits (Sulaiman, Mat-Yasin & Muhamad, 2018), thus generating a lack of definition of the control environment, inadequate definition of technological risks, lack of information, and adequate supervision of internal control. Therefore, it is necessary to develop a new method that can influence the optimal administration of HEIs.

The quality of computerized audit results is difficult to define, and to date, no one has been universally recognized (Sulaiman et al., 2018). However, the most supported concept states that it is the measurement of the success of the performance of the audit exercise (Havelka & Merhout, 2013), focused on the review and validation of the results obtained in the control exercise, which is applied to analyze whether the audit products meet the criteria of relevance, opportunity, and sufficiency; add value to the business; or provide

objective, verified, and independent information for decision-making in the areas, processes, and activities related to the audited object (Imbaquingo, San Pedro, Díaz, Arciniega, Saltos & Ortega, 2022).

When discussing information security, the objective is to protect data through human and technical measures and procedures to guarantee an institution's business sustainability, profitability, and value (Hohan et al., 2015). Therefore, for this investigation, the quality and security of the information within the audit exercise are considered an essential part of the method, identifying audit quality metrics associated with the human, technical, and environmental factors, and security metrics focused on the pillars of integrity, confidentiality, and availability.

The main contribution of this investigative work is the design of a computer audit method for Higher Education Institutions (MAIIES), which ensures the quality and security of the results based on computer audit techniques, good practices, and international reference frameworks. To meet this objective, three research questions have been raised: ¿What are the factors that impact audit quality? ¿What are the metrics to evaluate quality and security in computer audits? What are the activities to develop a computer audit process?

The rest of the paper is organized as follows. Section 2 reviews related work, and Section 3 describes the research materials and methods. Section 4 describes the MAIIES method, highlighting the statistical analysis for the definition of the method validation metrics in terms of quality and safety. Sections 5 and 6 discuss and conclude the study, respectively.

1.1. Related Work

1.1.1. IT Audit

Audits are tools to support decision-making and continuous improvement because they are designed to help and should not create any problems (Cienfuegos, Gómez & Millas, 2021). Therefore, HEIs need a method that adapts to their needs and is easy to follow and understand. However, the existing computer audit methodologies or standards are oriented to the productive sector, so they do not fully adapt to the educational environment and reality of HEIs (Gkrimpizi, Peristeras & Magnisalis, 2023)

Aliyu, Maglaras, He, Yevseyeva, Boiten, Cook et al. (2020) highlight that (HEIs) possess vast amounts of sensitive information and knowledge, making them prime targets for cyber threats targeting their research data, financial records, and IT resources. This reality underscores the ongoing struggle to balance open access to this information with the need to secure it against such threats, especially given the vulnerabilities in HEI IT infrastructures. To address this, the authors suggest a structured evaluation framework aimed at assessing the cybersecurity maturity levels of HEIs.

Among the most used methodologies in IT audits in HEIs are ITAF, ISO, ISSAI, and ITIL (Otero, 2018) which have been applied within HEIs as a component analysis method to improve the quality and effectiveness of the audit (Siyaya, Epizitone, Jali & Olugbara, 2021), to control operations and verify that the inherent risks are managed correctly (Taşkın & Sandıkkaya, 2023), all of which satisfy the high demands and competition in the market produced by these institutions. Another aspect is the application of an audit to analyze the accessibility of its institutional websites (Kurt, 2017; Sanchez-Puchol, Pastor-Collado & Borrell, 2017), as well as to review the security of information within the IT service department (Ghazvini, Shukur & Hood, 2018) and the assurance of the quality of computer services (Widjajanto, Agustini-Santoso & Riiati, 2018). Furthermore, techniques useful for evaluating higher education were also applied in this study (Bates, 2018). Finally, these methodologies (Carpenter & McGregor, 2020) can be applied to knowledge areas and professional education reforms by offering a constructivist explanation of risk audit technologies (Saputra & Ismandra, 2023).

1.1.2. Quality of Audits

A quality audit can be defined as a comprehensive assessment process that examines the competence and independence of auditors, the effectiveness of audit testing procedures, and the reliability and relevance

of the evidence gathered (Francis, 2023). Audit quality is a multidimensional concept influenced by inputs, processes, and the regulatory ecosystem, highlighting the complexity and layered nature of ensuring high-quality audits (Francis, 2011).

It is complex because, unlike any other field of study, it is difficult to define. To date, there is no universally recognized concept, but it is related to standards applicable to auditing. The closest definition measures the success of process completion (Havelka & Merhout, 2013; Holm & Zaman, 2012). In the guide proposed by (Contact Committee of the Heads of the SAIs of the European Union, 2004), it is established that the quality of the audit starts with the process of identifying and managing the activities that will comply with the objectives and quality indicators established by the regulation and control entities, who ensure that the problems in the quality of the audits are directly related to how the process was designed. For Francis (2004), the definition of quality is related to all audit failures: the higher the failure rate, the lower the audit quality. It is worth mentioning that the idea of quality differs among those involved in the audit and must accommodate the needs of each organization, person, area, or process (Detzen & Gold, 2021). The framework proposed by the International Audit and Assurance Standards Board states that quality is compliant with standards, controls, and the ethics used during the process (International Auditing and Assurance Standards Board, 2014).

Previous studies on audit quality have identified three factors that directly affect the quality of audit results: human, technical, and contextual or environmental. Each factor has a group of metrics that evaluates and measures the quality of an audit exercise (Imbaquingo et al., 2021, 2022)

1.1.3. Information Security

Information security, also known as cybersecurity or IT security, involves protecting electronic data from various risks, including unauthorized access, use, disclosure, interception, and data loss (Salazar & Silvestre, 2017). This encompasses the safeguarding of both business and individual users' confidential information. The core objectives of IT and information security are defined by three critical aspects: confidentiality, ensuring that information is accessible only to those authorized to have access; integrity, guaranteeing the accuracy and completeness of data; and availability, ensuring that authorized users have access to the information and its associated assets when needed (Taherdoost, 2022).

The significance of information security and cybersecurity management is increasing given the necessity to safeguard data, while the incidence of cyberattacks has escalated, as reported by global cybersecurity entities. Furthermore, awareness regarding the implementation of defensive strategies has significantly expanded (Antunes, Maximiano, Gomes & Pinto, 2021). The COVID-19 pandemic has further exacerbated cybersecurity challenges globally, due to the shift towards remote work, prompting an expedited digital transformation (Ahmad, 2020).

Although at the HEIs level, there are studies to guide the audit process and audit proposals for the evaluation of information security by applying methodologies such as COBIT, ISO, ITIL, and others (Haufe, Colomo-Palacios, Dzombeta, Brandis & Stantchev, 2022) none of them contemplate the specific services and processes that are developed within HEIs, to control and guarantee the security of technological assets against different threats and incidents, or to determine opportunities for improvement.

However, several studies discuss information security focused on security pillars: availability (Ahmed & Pathan, 2020; Kure, Islam & Razzaque, 2018) integrity (Eom, Hong, An, Park & Kim, 2019; Gunes, Kayisoglu & Bolat, 2021), and confidentiality (McLeod & Dolezel, 2022; Wagner & Eckhoff, 2019), which allow obtaining various metrics for each pillar to assess information security, including security policies, asset control, encryption, staff training, access control, monitoring plans, incident management, and compliance audits.

2. Materials and Methods

The methodology for the development of the MAIIES is based on the Framework of Technology, Organization, and Environment (TOE), which proposes the adoption of new technologies in organizations considering three aspects: technological, organizational, and environmental or environment (Palos-Sanchez, Reyes-Menendez & Saura, 2019). This is consistent with the bibliographic review and with the aspects to be considered in an audit process. Within the technological context, all the technical and technological tools used in the audit phases (Contact Committee of the Heads of the SAIs of the European Union, 2004; Normas Internacionales de Ética para Contadores [IESBA], 2021) are considered; in the organizational context, those involved in the audit process and the structure of HEIs (Harris & Williams, 2020; Knechel, Krishnan, Pevzner, Shefchik & Velury, 2013); and in the context or environment, everything related to the regulatory environment, organizational structure, and current regulations to audit (Esparza, Diaz, Egas, Sinchiguano & Misacango, 2020; Havelka & Merhout, 2013).

The methodology begins with a literature review to obtain a deep understanding of IT audit methodologies, the reference frameworks used by IT auditors, and their phases and activities. Figure 1 shows the flow to literature review.

Figure 1. Flow to literature review

Next, metrics that allow the evaluation of the quality and security of the results in computer audit processes carried out in HEIs and end with a statistical analysis to identify and define quality and security evaluation instruments in computer audits.

The reference frameworks chosen for the study were ISO 19011:2018, ISSAI 5300, ITAF, and IIA s. They are based on compliance with certain parameters, such as validity and compliance with the general structure of a computer audit, frequent use, and implementation in auditing processes. Within each referential framework, there are unique procedures for developing an audit process. However, the union of two or more frameworks or methodologies is necessary for an audit to be considered complete and successful. Consequently, for the creation of MAIIES, the activities of each framework were identified as the basis for the proposed method.

Several authors agree that an audit is structured in three phases: audit planning, audit execution, and results communication (Harris & Williams, 2020). However, for the development of the MAIIES, validation and follow-up phases were added, thus ensuring a complete method with feedback that included an evaluation based on quality indicators, security, and post-audit compliance. In addition, follow-up is considered to encourage appropriate responses to the findings identified in the audit and lay the foundation for future audit work (Contact Committee of the Heads of the SAIs of the European Union, 2004).

In previous studies, the factors and metrics of quality and security of the results in computer audit processes were identified through a literature review, in which the human, technical, and contextual factors stand out, and 94 metrics were grouped into each factor (Imbaquingo et al., 2021), along with a statistical analysis in which it was determined if the metrics were grouped correctly in the identified factors, allowing a reduction of dimensions based on their results (Imbaquingo et al., 2022). However, with the 64-resulting metrics, the analysis focuses on computer audit processes implemented in Ecuadorian HEIs using data processing techniques such as Mahalanobis distances, Confirmatory Factorial Analysis, and the Kruskal-Wallis test.

Mahalanobis Distances. These distances allow measurement of the number of standard deviations where the observations are located. Geometrically, Euclidean distance is the shortest distance between two

points; however, it does not consider the correlation between highly correlated variables. The Mahalanobis distance differs from the Euclidean distance in that it considers correlations between variables [61, 62]. Each Mahalanobis distance is a scale-invariant metric that obtains the distance between a point generated by an $x \in \mathbb{R}^p$, p-variant probability distribution $fx(.)$, and the mean $\mu = E(X)$ of the distribution. We assume that distribution $fx(.)$ has second-order finite moments and the covariance matrix can be defined as $\sum = E(X - \mu)$. Equation 1 defines the Mahalanobis distances are defined as:

$$D(\boldsymbol{X}, \mu) = \sqrt{(\boldsymbol{X} - \mu)^T \Sigma^{-1} (\boldsymbol{X} - \mu)} \tag{1}$$

Confirmatory Factorial Analysis. In addition, confirmatory factor analysis (CFA) was carried out to correctly explain the factors that compose the whole structure, confirming its validity and reliability. In this formulation, there is a vector of observed responses Y_i which is predicted by the unobserved latent variables ξ, through the model (see Equation 2):

$$\boldsymbol{Y} = \boldsymbol{\Lambda}\, \xi + \epsilon, \tag{2}$$

Where Y is a vector of dimension $p \times 1$ of observed random variables, ξ is the unobserved latent variables, and Λ is a dimension matrix $p \times k$ with k equal to the number of unobserved latent variables. Also, as Y is constituted by a set of variables ξ that imperfectly explain Y, the model considers the error $\in$. The model is commonly solved by a maximum likelihood (ML) estimation formulation generated by iterative minimization of the fitting function (F_{ML}) of the Equation 3:

$$\begin{aligned} F_{ML} = {} & ln|\boldsymbol{\Lambda\Omega\Lambda'} + \boldsymbol{I} - diag(\boldsymbol{\Lambda\Omega\Lambda'})| \\ & + tr\left(R(\boldsymbol{\Lambda\Omega\Lambda'} + \boldsymbol{I} - -diag(\boldsymbol{\Lambda\Omega\Lambda'})^{-1})\right) - \ln(R) - p, \end{aligned} \tag{3}$$

Where ΛΩΛ' is the variance-covariance matrix involved in the proposed factor analysis model, and R is the observed variance-covariance matrix. In this way, the model parameters are estimated by minimizing the distance between the variance-covariance implied in the model and the observed one (Rosseel, 2012; Yang-Wallentin, Joreskog & Luo, 2010).

Kruskal-Wallis Test. With the results obtained through the data treatment and the validation of the construct by the CFA, it is guaranteed that a data sample is valid, does not present alterations due to the influence of outliers, and is made up only of a set of variables that correctly explain the factors that are of interest in the investigation. Since these data come from non-ordinal variables, a non-parametric technique must be used to compare the groups determined by categorical variables. The Kruskal-Wallis test is a non-parametric alternative to one-way ANOVA. It is assumed that the observations in each sample group are from a sample with the same distribution. Therefore, for this test, the null hypothesis was established based on the Equation 4:

$$H_0: \eta_1 = \eta_2 = \cdots = \eta_k, \tag{4}$$

Where η_i is the median of the ith group defined by the categorical variable in the sample. In this case, the null hypothesis is equivalent to: "H_0 *: the samples come from identical populations*". We define n that represents the total number of observations $n = \sum_{i=1}^{k} n_i$, where n_i represents the sample size of each group i = 1,2, …, k and k represents the number of groups to be compared. Ranks were obtained for each observation in ascending or descending order of magnitude when ties existed. In this way, $R(X_{ij})$ represents the rank assigned to the j-th observation of the i-th group, X_{ij} and R_i represent the sum of ranks assigned to the i-th group, $R_i \sum_{i=1}^{ni} R(X_{ij})$ for i = 1,2, …, k. In this way, the static test T is defined on the Equation 5:

$$T = \frac{1}{S^2}\left(\sum_{i=1}^{k}\frac{R_i^2}{n_i} - \frac{n(n+2)^2}{4}\right), \tag{5}$$

where:

$$S^2 = \frac{1}{n-1}\left(\sum_{allrank} R(X_{ij})^2 - \frac{n(n-1)^2}{2}\right), \tag{6}$$

If there are no ties, S^2 it is simplified to the expression $n(n + 1)/12$ and the statistical test is reduced to Equation 7:

$$T = \frac{12}{n(n+1)}\sum_{i=1}^{k}\frac{R_i^2}{n_i} - 3(n+1). \tag{7}$$

Under the null hypothesis, H_0 and the previously defined assumption, T it is distributed asymptotically to the chi-square distribution with k – 1 degrees of freedom $T \sim \chi^2_{k-1}$ (Lehmann, 2006; Nwobi & Akanno, 2021).

Dunn-Šidák Test. Finally, as a post hoc test for Kruskal-Wallis, we applied the Dunn–Šidák test for the comparison between more than two samples in a paired way, constituting in this way an alternative, where in case of reaching the level of significance at a general level, Dunn's test is capable of contrasting each possible pair and identifying which pairs of groups present significant differences (Dunn, 1958). Moreover, Dunn's test can provide even smaller confidence intervals than Tukey's test. For a given FWER (wise error rate (FWER) error metric α, the Dunn–Šidák test defined as $\mu_i - \mu_j$ can be calculated using the Equation 8 and 9:

$$\mu_i - \mu_j = \bar{y}_i - \bar{y}_j \pm t_{\alpha',\nu}\sqrt{s^2\left(\frac{1}{n_i} + \frac{1}{n_j}\right)}, \tag{8}$$

where

$$\alpha' = \frac{1}{2}\left(1 - (1-\alpha)^{\frac{1}{c}}\right), \tag{9}$$

$\bar{y}_i$ and $\bar{y}_j$ are the means of the samples considered, c is is the number of possible comparisons in the family, and the quantile $t_{\alpha',\nu}$ is obtained from Student's probability distribution t for a given parameter of degrees of freedom ν. Finally, the confidence intervals for each possible Dunn-Šidák test (see Equation 10) were obtained as follows:

$$\sum_{i=1}^{k} c_i \bar{y}_i \pm t_{\alpha',\nu}\sqrt{s^2\sum_{i=1}^{k}\frac{c_i^2}{n_i}}, \tag{10}$$

3. Results

The MAIIES proposal is structured in five phases: planning, execution, communication of results, validation, and follow-up. Each phase encompasses a set of activities, and for the complete method, 47 are accounted for. These activities were verified using the Delphi Method, a technique that allows gathering information based on the opinions of experts in a specific area to obtain a consolidation of a given topic (Reguant & Torrado, 2016). Figure 2 shows the general scheme of the proposed method.

For the validation phase, a statistical analysis of the metrics obtained for the quality and security of information in computer audit processes implemented in HEIs was conducted. The database consists of 54 computer audit observations performed in 54 HEIs in Ecuador. The variables used to construct the audit evaluation model are proposed in (Imbaquingo et al., 2021, 2022; Stoel, Havelka & Merhout, 2012). Thus, the evaluation instrument was made up of 81 variables, of which eight were categorical, including the name of the institution, the area where it is located, the level of studies it offers, compliance with the performance of audits, the perception of the importance of performing audits, whether previous audits have been performed, the type of audit previously performed and the type of audit. The 81 variables were evaluated on a ten-level ordinal scale, where each of the variables proposed in (Imbaquingo et al., 2022) was scored to measure the quality dimension composed of human, technical and contextual factors. The information security dimension is based on confidentiality, integrity and availability based on the ISO 27000 standard. The variables distribution for each factor is presented in Tables 1 and 2.

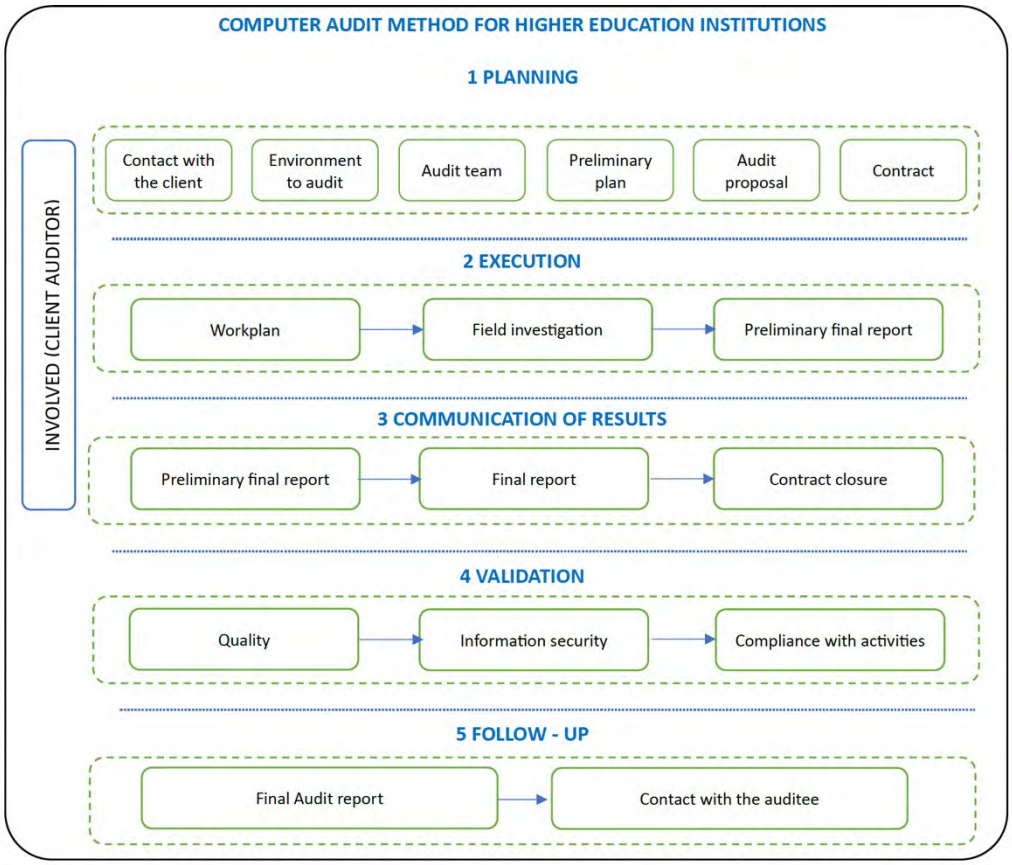

Figure 2. MAIIES scheme

Variable	Factor
	Human factor
*p*1	The audit team sought to involve the client throughout the audit process
*p*2	The audit team obtained the client's agreement about the activities carried out
*p*4	The staff performing the audit had the necessary competencies to perform their work
*p*5	The auditor had soft skills (characteristics and personal competencies that demonstrate how the auditor works with others)
*p*6	The staff who performed the audit provided effective suggestions to the Institution
*p*7	The auditor was open-minded when receiving new ideas
*p*8	The auditor was sure of himself and his work
*p*9	The audit team retained its independence in appearance and action

Variable	Factor
	Human factor
*p*10	The audit team focused on the facts
*p*11	The audit team received support to achieve the goals
*p*12	The audit team demonstrated effort in conducting the audit
*p*13	The auditor was concerned about their training and continuous updating
*p*14	The auditor had national and international certifications in auditing and computer auditing
*p*15	Audit team members demonstrated knowledge of information security and data processing
*p*16	Differences with the client were dealt with in a timely, professional, and objective manner
*p*17	The audit team was available to meet the client's requests
*p*18	Those involved in the audit had frequent communication
*p*19	The auditor engaged experts to support the audit process to obtain results and recommendations for the client
*p*20	The auditor followed policies and procedures that regulate its ethical and professional compliance
	Technical Factor
*p*21	The audit team used templates and forms to document
*p*22	The audit findings and conclusions were an accurate reflection of the actual facts of the audited process
*p*23	The audit results were supported and documented with the evidence collected during the audit.
*p*24	The members of the audit team and those responsible for the institution ensured at all times the information
*p*25	The client positively received the findings, conclusions, and recommendations
*p*26	Resources for the audit were allocated according to the importance and complexity of the audit
*p*27	The system, process, or object audited was significant to the organization
*p*28	In the scope, all the elements necessary to audit successfully were addressed.
*p*29	The execution of the audit complied with the elements agreed upon in the scope
*p*30	The results were delivered at the right and established time
*p*31	The risk assessment model was understandable
*p*32	The audit plan took into account the risks related to the client
*p*33	The audit process was carried out with accuracy and precision
*p*34	The audit report was clear and concise with its results
*p*35	The scope, findings, and recommendations have been understandable to anyone who used the audit report.
*p*36	The audit was executed under the policies, standards, manuals, guidelines, and practices of computer auditing
*p*37	Checklists were complete, approved, and documented
*p*38	An expert reviewed the fieldwork
*p*39	The client or managers of the audited organization provided support for the collection of information
*p*40	Information and results from previous audits were available for review
*p*41	The objectives and scope of the audit were adequately specified
*p*42	The activities and tools for the audit were clearly described
*p*43	Audit team members had a clear and consistent understanding of the audit plan
*p*44	The audit budget and schedule were properly established
*p*45	The requirements of personnel and equipment assigned for the audit were evaluated
*p*46	The audit plan was prepared, reviewed, and approved by the supervisors, managers of the organization, and members of the audit team
*p*47	The audit team used an IT audit methodology to plan, manage and perform the audit
*p*48	The audit team used technological tools and new methodologies to carry out their work
	Context Factor
*p*49	Through his reports, the auditor promoted an organizational culture based on good computer security practices
*p*50	The audit team had strict quality control procedures

Variable	Factor
	Human factor
*p*51	The audit team leader was committed to the quality control system
*p*52	The rules and regulations issued by control bodies were reflected in the audit plan
*p*53	The audit team knew the relevant information of laws and regulations that can have a significant impact on the audit objectives
*p*54	Disciplinary measures were applied in case of non-compliance with the audit plan or current legal regulations
*p*55	The audit cost was established in accordance with the complexity and the activities carried out.

Table 1. Variables and factors proposed for the evaluation of the Quality dimension.

Variable	Factor
	Confidentiality Factor
*p*56	Information security policies are applied within the institution
*p*57	The information security policies and procedures within the institution are updated periodically
*p*58	Information security responsibilities are delegated, documented, and formally delivered to all institution staff, depending on their position.
*p*59	Security policies and actions are applied to sensitive information of the institution
*p*60	Information access policies are updated and applied based on existing user roles
*p*61	An information security accreditation is available for all its computer systems
*p*62	Documented procedures are in place to follow in case of security incidents
*p*63	Information security compliance audits are performed
*p*64	Password management policies apply to end users of the institution
*p*65	Users accessing the network and the actions they perform are identified
	Integrity Factor
*p*66	Access control is applied to the institution's IT infrastructure and services
*p*67	Users, collaborators, and staff are trained and involved in information security issues
*p*68	Vulnerability analysis of the institution's web services is carried out
*p*69	Plans for monitoring and managing the impact of security incidents in the institution are applied
*p*70	Inventory of all IT assets is updated and documented
	Availability Factor
*p*71	Applications are available to protect all your IT solutions from malware
*p*72	Data backups are made
*p*73	The activities developed by the users are monitored

Table 2. Variables and factors proposed for the evaluation of the Information Security dimension

Statistical analysis began by processing the data that constituted the database. Each audit carried out in the HEIs constitutes a multivariate observation; therefore, Mahalanobis Distances were used to detect atypical observations. A cutoff score of 128.5648 was established based on the distribution χ^2 conserved 99.9% of the distribution, where 0.01% of the furthest distances were considered outliers. In this way, by computing the Mahalanobis distances for the entire database, none were detected as atypical, so the final database comprised 54 audit observations from higher education institutions.

The instrument proposed was validated for a group of internal auditors from Ecuador (Imbaquingo et al., 2022). However, the present study was developed in a specialized manner for higher education institutions, so in the first instance ten variables that do not apply to the context of higher education were eliminated. Therefore, a new process of verification of the validity and reliability of the modified instrument was carried out, for which the Confirmatory Factor Analysis (CFA) technique was selected. The analysis began by verifying the assumptions of additivity, normality, linearity, homogeneity, and homoscedasticity. Figure 4 shows the results of the multivariate additivity analysis of the sample using a correlation matrix, which is presented in Figure 3.

Figure 3 shows that none of the pairs of questions reached very high or perfect correlation values close to 1, so the additivity hypothesis was accepted. The correlation values were close to 1; therefore, the additivity hypothesis was accepted. To verify the multivariate assumptions of normality, linearity, homogeneity, and homoscedasticity, the sham regression analysis was used. The results were observed using the histogram, the QQ diagram, and the scatter plot presented in Figure 4.

As can be seen, Figure 4a shows the histogram of the adjusted values from a regression performed using the quantiles of the distribution χ^2 is the response variable, and the ordinal variables of the instrument as predictors. These adjusted values were standardized, and subsequently, a histogram was obtained, whose values described a distribution similar to the normal; therefore, the assumption of normality was accepted. To observe the assumption of linearity, the Q-Q plot was used, which is the diagram obtained by plotting the quantiles of the real sample concerning theoretical quantiles obtained from a random sample of the distribution χ^2 for the same number of degrees of freedom of the sample. As shown in Figure 4b, when plotting the Q-Q plot, the quantiles were distributed similarly to a straight line with a slope of 1, so the assumption of linearity was accepted. Finally, the assumptions of homogeneity and homoscedasticity were observed using the scatter plot shown in Figure 4c, where the standardized residuals were projected based on the residuals obtained in the fit of the regression model. As can be seen, the residuals were arranged similarly in the four quadrants, and there were no pre-established groups or patterns identified; therefore, the assumptions of homogeneity and homoscedasticity were accepted (Guevara, Herrera, García & Quiña, 2020; Jácome, Herrera, Herrera, Caraguay, Basantes & Ortega, 2019).

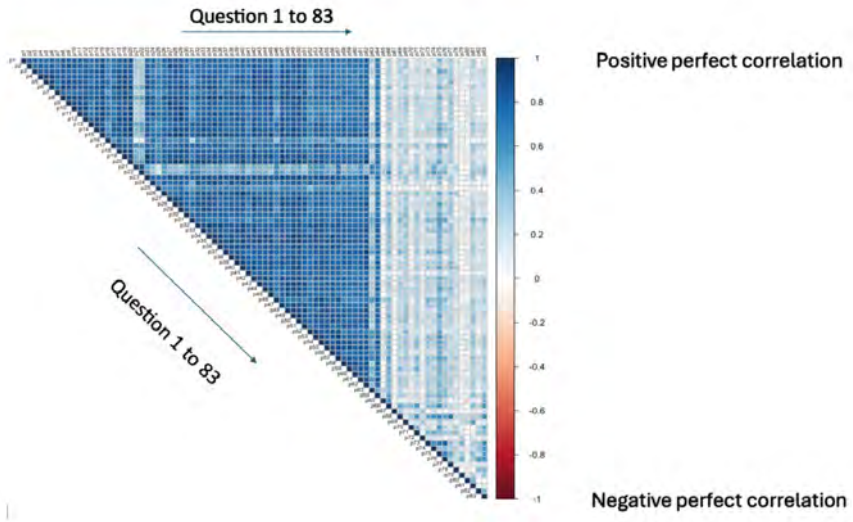

Figure 3. Multivariate correlation matrix for each possible pair of items that comprise the instrument

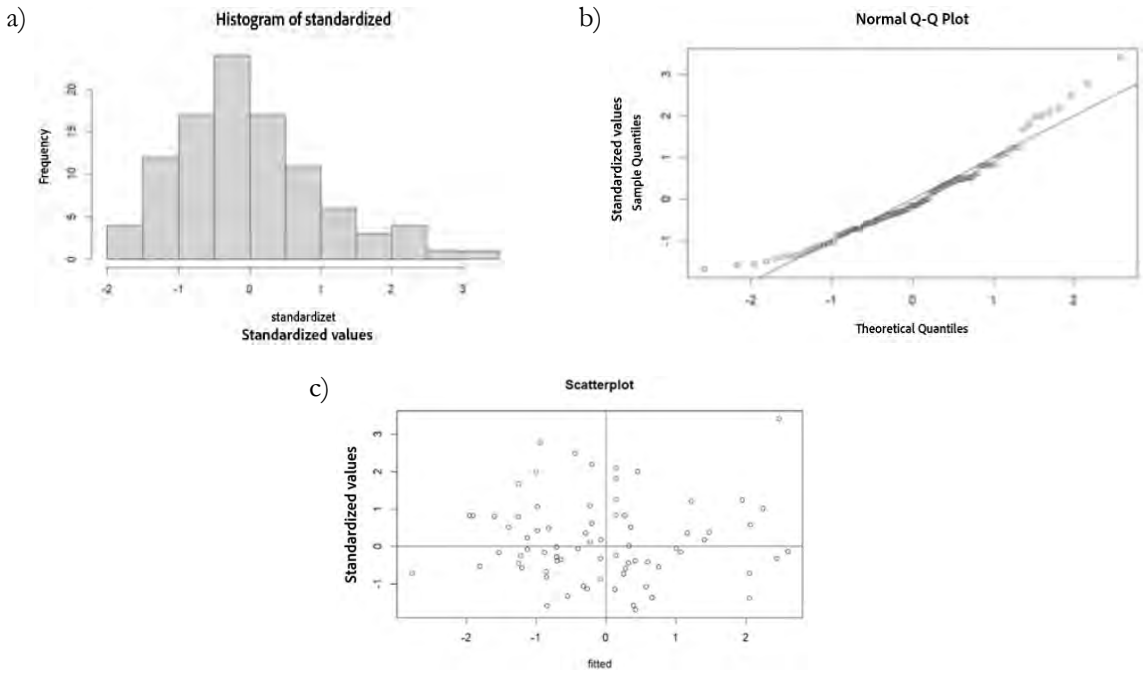

Figure 4. Parametric assumptions: (a) histogram of standardized values; (b) quantile diagram (QQ Plot); (c) scatter plot (Scatter-plot)

Once the assumptions were verified, it was concluded that the sample was parametric and met the requirements for applying CFA as a technique for verifying the validity and reliability of the instrument. The CFA results for each dimension are presented in Figures 5 to 6 and Table 3.

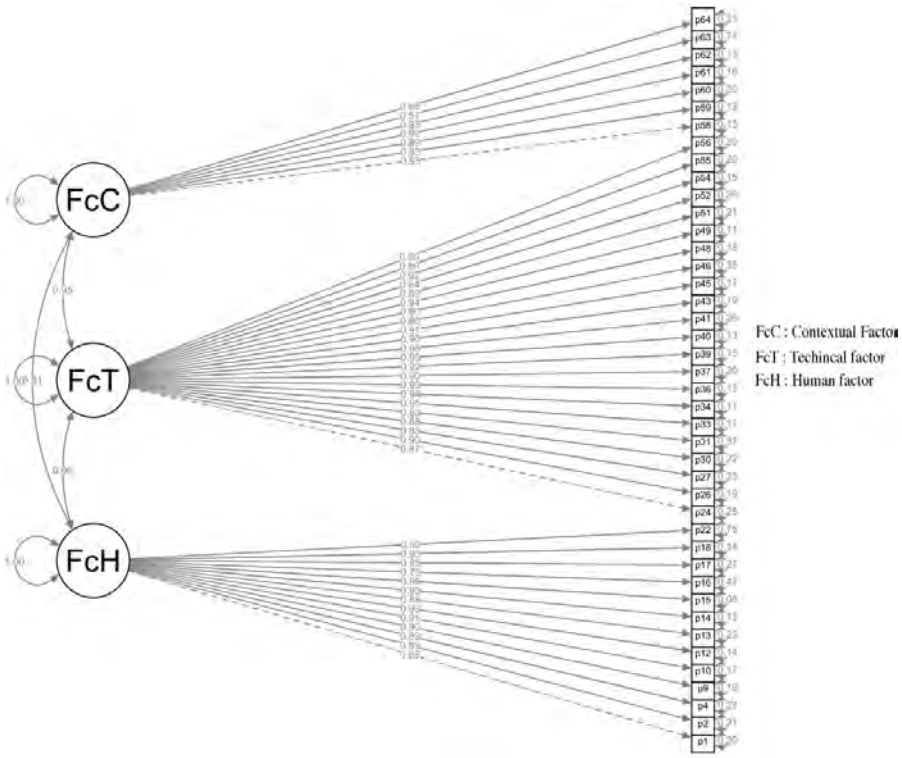

Figure 5. Path -diagram for the CFA applied to the Quality dimension

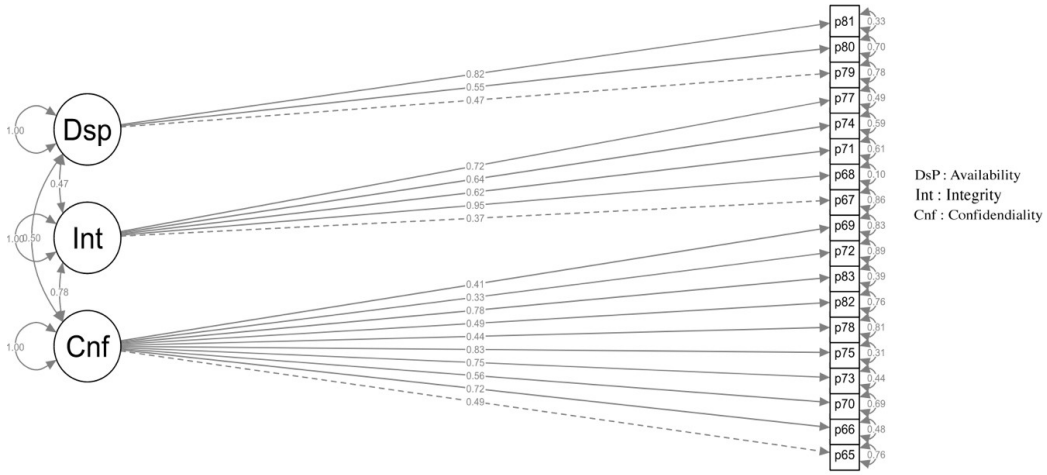

Figure 6. Path -diagram for the CFA applied to the Security dimension

npar	***fmin***	***chisq***	***df***	***pvalue***
39.000	0.681	210,978	132,000	0,000
cfi	***tli***	***cfi***	***rmsea***	***srmr***
0.904	0.913	0.913	0.037	0.049

Table 3. CFA goodness-of-fit indices

As shown in Figures 6 and 7, questions p3, p5, p6, p7, p8, p11, p19, p20, p21, p23, p25, p28, p29, p32, p35, p38, p42, p44, p47, p50, p53, p57, p67, and p76 were removed from the instrument because their saturations were not sufficiently large to contribute to the factorial structure. In addition, all the loadings of each question towards their respective factors were greater than 0.3, and the correlations between factors were quite far from perfect (0.95, 0.91, and 0.96, respectively, and 0.50, 0.47, and 0.78, respectively), so there were no indications of invalidity in the construct. Table 3 shows the most important goodness-of-fit indices obtained through the CFA, where it can be seen that the CFI (Comparative fit Index), TLI (Tucker-Lewis Index), and the NNFI (Not-normed fit index) reached values of 0.904, 0.913 and 0.913 respectively, evidencing the reliability of the construct. In contrast, the root mean squared error of approximation (RMSEA) and Standardized Root Mean- Square (SRMR) were 0.037 and 0.049, respectively, indicating the instrument's reliability.

One of the most important output variables that can be obtained through CFA is the coefficient of determination r^2 for each question of the construct, which represents the amount of variance that each question can explain for its respective unobserved latent variable (factor). The determination coefficients for each factor of the two observed dimensions are presented in Figures 7 and 8, respectively.

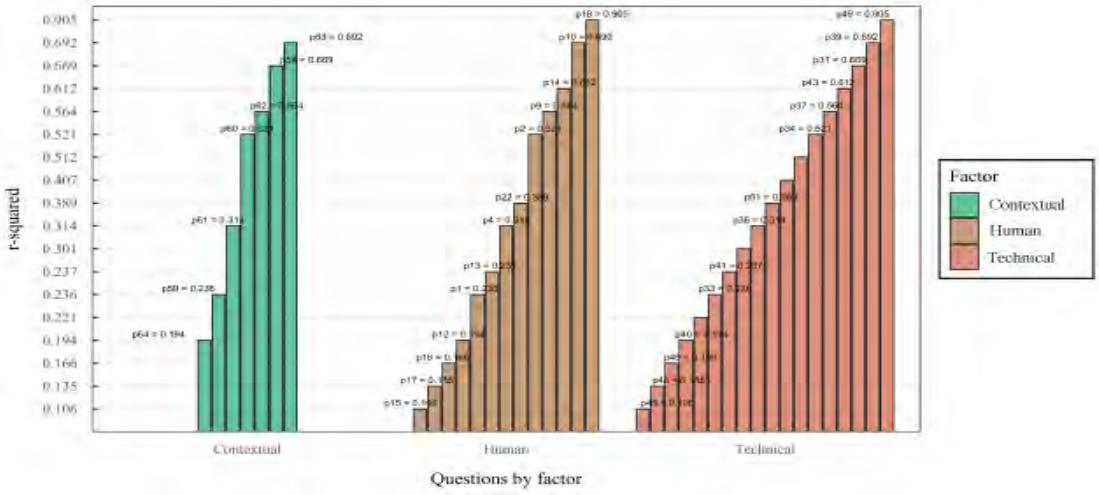

Figure 7. Determination coefficients r^2 for each question of the factors contextual, human, and technical

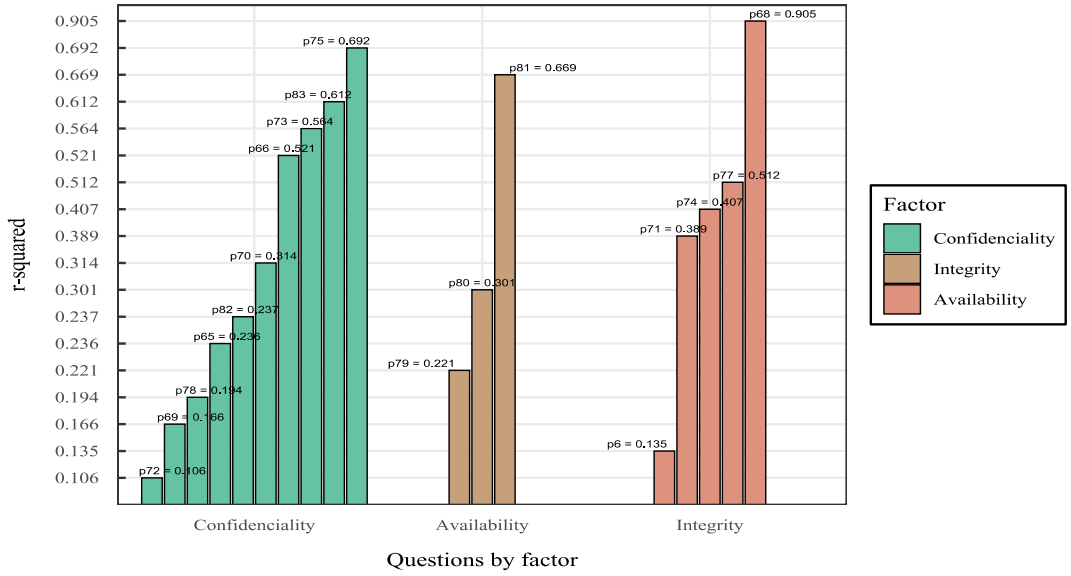

Figure 8. Determination coefficients r^2 for each question of the confidentiality, integrity, and availability factors

As seen in Figure 7, CFA allows us to obtain the determination coefficients of each question, which represent the different contributions each question has for its respective factor. These indices are coefficients that make it possible to determine the model for the appropriate weighting of each question that constitutes the proposed computer audit model. Figure 8 shows that each question has a different level of relevance for its factor; therefore, the nominal scale scores should not be summed or averaged. Instead, it is appropriate to use Equations 11 to 17 for the correct calculation of the scores of each factor (ζ) in its dimension, which is mandatory for the application of the proposed MAIIES model and has been validated through an audit of 54 educational institutions carried out by experts.

$$\zeta_{Human} = 1.01968(0.8p_1 + 0.791p_2 + 0.784p_4 + 0.808p_9 + 0.827p_{10} + 0.856p_{12} + 0.775p_{13} + 0.866p_{14} + 0.925p_{15} + 0.534p_{16} + 0.728p_{17} + 0.861p_{18} + 0.252p_{22}) \quad (11)$$

$$\zeta_{Technical} = 0.570353(0.752p_{24} + 0.807p_{26} + 0.77p_{27} + 0.782p_{30} + 0.634p_{31} + 0.827p_{33} + 0.892p_{34} + 0.867p_{36} + 0.804p_{37} + 0.852p_{39} + 0.872p_{40} + 0.735p_{41} + 0.813p_{43} + 0.827p_{45} + 0.646p_{46} + 0.818p_{48} + 0.89p_{49} + 0.79p_{51} + 0.713p_{52} + 0.847p_{54} + 0.795p_{55} + 0.8p_{52}) \quad (12)$$

$$\zeta_{Contextual} = 1.901141(0.871p_{58} + 0.869p_{59} + 0.799p_{60} + 0.818p_{61} + 0.874p_{62} + 0.261p_{63} + 0.768p_{64}) \quad (13)$$

$$\zeta_{Confidentiality} = 2.745744(0.236p_{65} + 0.521p_{66} + 0.314p_{70} + 0.564p_{73} + 0.692p_{75} + 0.194p_{78} + 0.237p_{82} + 0.612p_{83} + 0.106p_{72}\ 0.166p_{69}) \quad (14)$$

$$\zeta_{Integrity} = 4.258944(0.135p_{67} + 0.905p_{68} + 0.389p_{71} + 0.407p_{74} + 0.512p_{77}) \quad (15)$$

$$\zeta_{Availability} = 8.396306(0.2210.8p_{79} + 0.3010.8p_{80} + 0.6690.8p_{81}) \quad (16)$$

The level of correlation between each factor was analyzed using the weighted scores obtained for the audit of each HEI. In addition, because the sample was non-parametric, the Spearman's correlation coefficients were calculated. The results are shown in Figure 9.

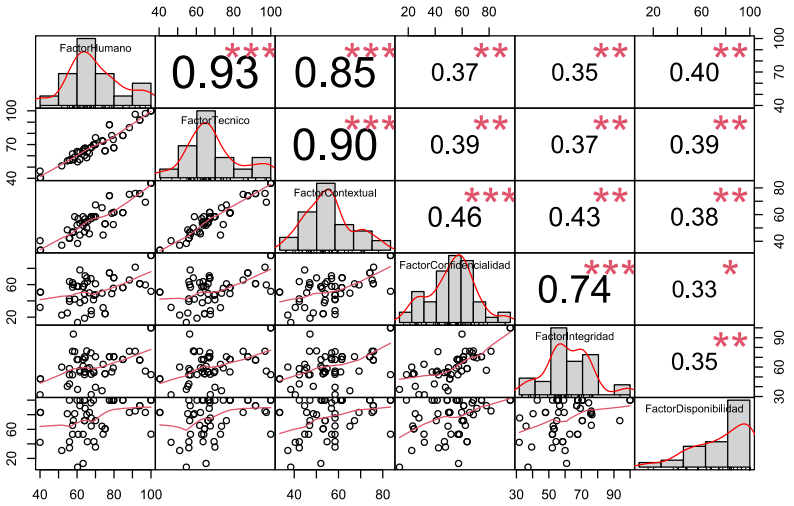

Figure 9. Spearman's correlation coefficients ρ^2, histograms, and trend curves for each possible pair of factors

Figure 9, several factors were significantly correlated. When analyzing the human and technical factors, a very high direct correlation was observed, reaching a Spearman ρ coefficient of 0.93, which implies that the higher the human factor score, the higher the technical factor score. Human and contextual factors showed a very high direct correlation, reaching a ρ Spearman coefficient of 0.85, which implies that the higher the human factor score, the higher the contextual factor score. Technical and contextual factors showed a very high direct correlation, reaching a Spearman coefficient ρ of 0.90, implying that the higher the technical factor score, the higher the contextual factor score. The contextual and confidentiality factors showed a high direct correlation, reaching a Spearman coefficient of 0.46, which implies that the higher the contextual factor score, the higher the confidentiality factor score. Finally, the confidentiality and integrity factors displayed a very high direct correlation, reaching a Spearman coefficientv ρ of 0.74, which implies that the higher the confidentiality factor score, the higher the integrity factor score. In addition, moderate correlations could be evidenced by comparing the remaining couples, which implies

that the instrument was constructed appropriately because the relationship between factors reflects similar behavior.

Next, through the mathematical models obtained, each of the HEIs participating in this research, the Quality and Security dimensions were evaluated, which included the following factors: human, technical, contextual, confidentiality, integrity, and availability. Table 4 presents the weighted scores obtained for each IES. Also, Figure 10 shows the Descriptive statistics of the weighted scores through the proposed methodology applied to HEIs in Ecuador.

Institution	HEI type	Auditory type	Human factor	Technical factor	Contextual factor	Confidentiality factor	Integrity factor	Availability factor
Cordillera Higher Technological Institute	private	internal	69.117	69.533	58.435	46.851	54.378	43.140
Higher Polytechnic School of the Guayaquil Coast	public	internal	65.264	58.394	50.065	68.350	76.533	80.000
Catholic University of Cuenca	private	external	100.000	100.000	83.479	95.815	100.000	100.000
University of Azuay	public	external	67.546	67.235	56.880	67.455	74.480	96.289
Hemispheres University	private	external	64.365	66.930	56.779	70.870	69.365	88.766
Nacional University of Loja	public	external	51.715	51.044	37.099	22.532	59.974	30.890
International University of Ecuador	private	internal	40.171	40.407	33.392	50.766	47.939	83.149
Higher Technological Institute H. Provincial Council of Pichincha	public	external	67.706	67.554	58.435	27.883	31.980	75.567
Higher University Institute of Technology	private	internal	55.918	56.012	42.295	39.344	42.819	100.000
PUCE Emeralds	private	internal	74.081	72.956	44.709	31.617	62.866	53.359
Carchi State Polytechnic University	public	external	69.966	76.170	67.221	61.024	70.575	71.914
North Technical University	public	internal	93.961	91.843	75.692	61.139	67.108	92.418
Higher Technological Institute "José Chiriboga Grijalva"	private	external	60.280	54.635	38.428	13.388	37.202	8.144
Private Technical University of Loja	private	external	57.578	56.880	46.475	56.851	52.147	53.098
YACHAY Experimental Technology Research University	public	internal	66.686	62.211	45.582	49.854	59.399	83.149
PUCE Ibarra	private	internal	96.945	97.654	69.245	59.646	55.933	83.149
Regional Autonomous University of the Andes UNIANDES Tulcán	private	external	40.000	46.429	40.473	31.914	31.742	42.124
Higher Technological Institute July 17	public	external	63.297	65.227	52.002	57.295	60.903	13.199
Cotacachi Higher Technological Institute	public	external	70.000	70.000	58.435	47.630	39.417	35.668
University of Otavalo	private	external	61.622	63.227	53.563	37.718	55.038	100.000
Higher Technological Institute Ibarra ITSI	private	internal	67.706	67.554	58.435	23.276	52.619	64.593
Lendan Higher Technological Institute	private	internal	55.918	56.012	42.295	42.435	52.147	34.542
National polytechnic school	public	internal	88.294	85.145	75.139	65.681	76.120	83.149

Institution	HEI type	Auditory type	Human factor	Technical factor	Contextual factor	Confidentiality factor	Integrity factor	Availability factor
Regional Autonomous University of the Andes UNIANDES	private	internal	75.184	64.413	53.034	24.138	53.194	60.680
Bolivar State University	public	external	60.636	62.857	56.916	57.823	67.683	53.098
Equinoccial Technological University UTE	private	external	64.093	60.392	47.072	18.633	52.300	100.000
SEK Ecuador International University	private	internal	61.530	56.697	44.660	78.026	56.661	92.418
National University of Education	public	internal	58.732	58.963	58.435	42.024	75.775	81.444
National University of Chimborazo	public	internal	68.936	70.000	58.435	41.442	55.933	100.000
Ikiam Amazon Regional University	public	internal	58.009	56.421	47.103	59.871	93.650	71.914
Intercultural University of Nationalities and Indigenous Peoples Amawtay Wasi	public	external	57.554	61.814	46.930	62.375	76.120	65.458
Institute of Higher National Studies IAEN	private	external	73.502	73.536	65.127	49.476	35.950	64.332
PUCE Quito	private	internal	84.776	78.151	61.451	56.351	67.836	100.000
Technical University of Babahoyo	public	external	64.042	66.295	53.937	40.783	54.800	71.914
Technical University of Manabi	public	internal	79.902	67.174	61.616	68.394	70.575	100.000
Quevedo State Technical University	public	internal	65.604	63.626	54.817	63.710	58.505	42.989
Metropolitan University of Ecuador UMET	private	internal	60.000	63.845	52.086	57.790	67.683	100.000
Amazon State University	public	internal	54.769	55.427	48.568	25.165	40.319	81.444
Luis Vargas Torres de Esmeraldas Technical University	public	external	100.000	100.000	83.479	51.705	52.300	53.359
Guayaquil University	public	external	79.620	74.488	52.542	55.505	59.080	100.000
University of the Armed Forces ESPE	public	internal	77.526	87.695	74.139	74.423	70.575	100.000
Secular Eloy Alfaro University of Manabí	public	external	64.042	66.295	53.937	48.850	55.038	100.000
Israel University of Technology	private	internal	78.801	78.065	60.954	48.850	55.038	100.000
Higher Polytechnic Agricultural School of Manabí	public	internal	91.458	96.910	75.829	81.458	76.120	85.155
Business Technological University of Guayaquil	public	internal	40.171	40.407	33.392	50.766	47.939	83.149
Iberoamerican University of Ecuador UNIBE	private	external	55.918	56.012	42.295	63.710	58.505	42.989
Latin American Faculty of Social Sciences Ecuador Headquarters FLACSO	private	external	63.275	64.044	58.435	57.823	67.683	53.098
Salesian Polytechnic University	private	internal	93.961	91.843	75.692	61.139	67.108	92.418
Technical university of Cotopaxi	public	external	75.184	64.413	53.034	24.138	53.194	60.680
Vicente Rocafuerte Secular University of Guayaquil	private	external	79.902	67.174	61.616	68.394	70.575	100.000

Institution	HEI type	Auditory type	Human factor	Technical factor	Contextual factor	Confidentiality factor	Integrity factor	Availability factor
Simón Bolívar Andean University Ecuador Headquarters	private	internal	77.526	87.695	74.139	74.423	70.575	100.000
Technical University of machala	public	internal	84.776	78.151	61.451	56.351	67.836	100.000
San Gregorio de Portoviejo University	private	internal	100.000	100.000	83.479	95.815	100.000	100.000
Espíritu Santo Private University of Specialties	private	external	64.042	66.295	53.937	61.024	70.575	71.914

Table 4. Weighted scores for the performance of each HEI in the Quality and Safety dimensions

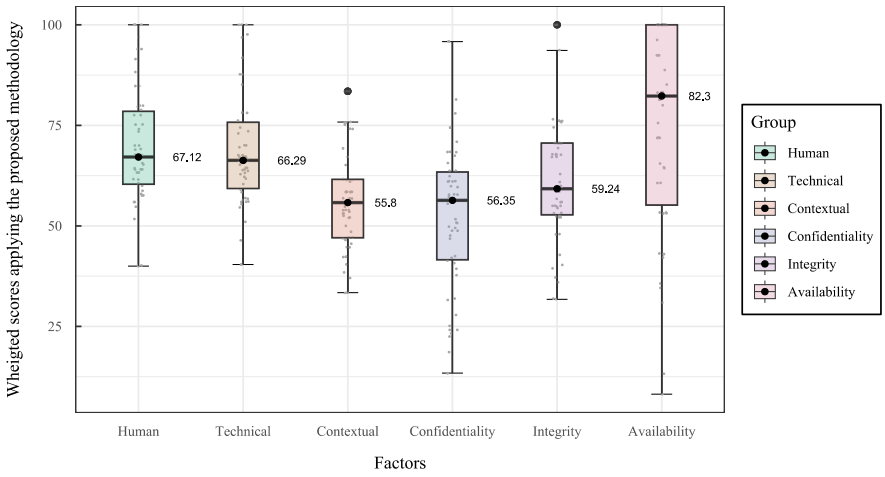

Figure 10. Descriptive statistics of the weighted scores through the proposed methodology applied to HEIs in Ecuador

Finally, all possible difference tests were carried out using categorical variables to evaluate their respective groups based on the weighted scores obtained for each factor. The analysis began using the HEI-type categorical variable, which contemplates private and public categories. As this categorical variable presented only two groups, the Mann-Whitney U test was used for analysis. The results are presented in Table 5 and Figures 11, respectively.

As seen in Table 5, the difference test carried out did not reach the level of significance, so there is not enough evidence to affirm that private higher education institutions perform better in terms of quality and safety. However, public institutions observed a slightly higher performance in both dimensions. Additionally, a difference test was carried out for the quality and security dimensions using the categorical variable defined to distinguish the type of audit carried out in each institution. The results are presented in Tables 6 and Figure 12.

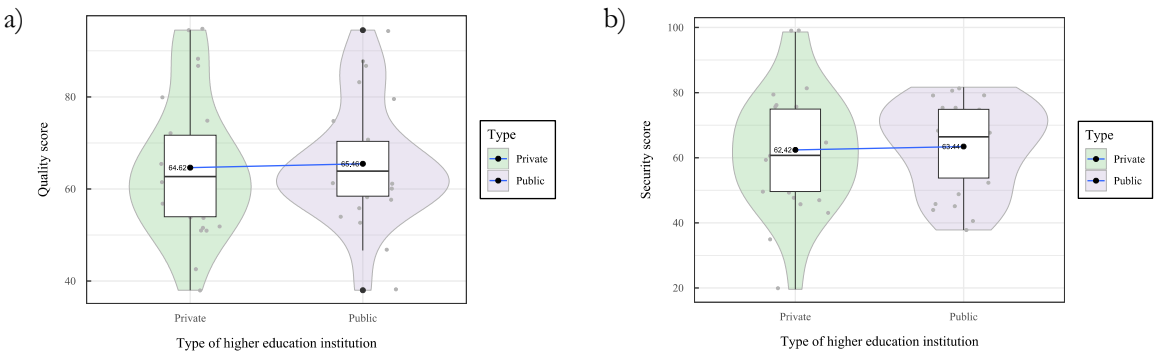

Figure 11. Box and dispersion plots of the scores obtained by type of HEI; a) quality scores; b) safety scores

Factors	value	U Man-Whitney test with continuity correction
Quality Dimension	*U*	341.5
	p – value	0.697 Not significant
	Min.: 95 % confidence Interval	-9.393691
	Max.: 95 % confidence Interval	7.336756
Security Dimension	*U*	350
	p – value	0.8086 Not significant
	Min.: 95 % confidence Interval	-10.476877
	Max.: 95 % confidence Interval	7.218164

Table 5. Mann-Whitney U test for the quality and safety dimensions scores for the HEI type categorical variable

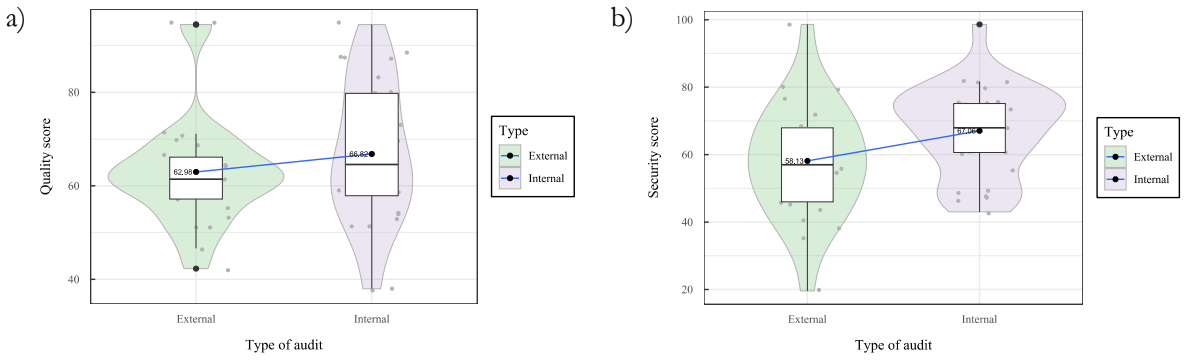

Figure 12. Box plots and dispersion of the scores obtained by type of HEI; a) quality scores; b) safety scores

Factors	value	U Man-Whitney test with continuity correction
Quality Dimension	*U*	305.5
	p – value	0.3268 Not significant
	Min.: 95 % confidence Interval	-12.090806
	Max.: 95 % confidence Interval	3.517231
Security Dimension	*U*	W = 240.5
	p – value	0.03502 Not significant
	Min.: 95 % confidence Interval	-18.005784
	Max.: 95 % confidence Interval	-1.083089

Table 6. Mann-Whitney U test for the scores of the quality and security dimensions for the categorical variable type of audit.

As shown in Table 6, when comparing the quality and security scores obtained based on the type of computer audit, significant differences were determined from the sample. When comparing the quality dimension, slightly higher scores were observed in the internal audits; however, the scores did not reach significance. In contrast, when comparing the scores of the security dimension, it was observed that the scores obtained through internal audits were significantly higher, with a p-value of 0.03502, so it can be affirmed that the results obtained through internal audits are significantly different than those obtained through internal audits. obtained by the external evaluators.

4. Discussion

HEIs need a computerized audit method that incorporates phases and activities adapted to their needs, which are easy to follow and understand. Something similar occurs in the work of (Aliyu et al., 2020)

where it is stated that HEIs need specific evaluations according to the nature, information, and technology that is managed in the institutions. In the proposed method, two additional phases (validation and monitoring) are proposed to the traditional ones (planning, execution, and opinion), which allow feedback on how the audit exercise was executed with quality and safety evaluation metrics and a checklist of activities compliance, which are indicators of the success of the audit.

Because audit quality revolves around key elements that increase the probability that an audit will be carried out efficiently and consistently (Contact Committee of the Heads of the SAIs of the European Union, 2004), the factors related to the computer audit were identified: human, technical, and contextual factors; the human factor that involves the auditor or audit professionals; the client or auditee; and the management and key interactions of all process participants. Technical factors address the behavior or performance of activities during the process, including organization, strategy and planning, selection of methodologies, fieldwork, results and reports, evidence-based decision-making, control quality, and audit improvement. Finally, the contextual factor, which is connected to factors external to the auditor and the audit process, includes the social and institutional strength of both the audited company and the audit firm, its regulatory environment, and perceptions and management of resources (Imbaquingo et al., 2021).

With the 91 metrics, an analysis was conducted focusing specifically on computer audits within HEIs, obtaining a response from 54 HEIs in Ecuador that had previously implemented some type of computer audit, thus having a vision of the requirements for an audit to be always of quality and secure information. Finally, 42 quality and 18 security metrics were obtained, which are part of the MAIIES evaluation and validation instruments.

According to the results of the statistical analysis, it can be ensured that the human and technical factors are highly correlated because if the selection of the audit team meets all the requirements and adequate knowledge for the audit, the selection of tools, methodologies, and technology will be based on the expertise of the personnel involved, which directly ensures a successful audit with quality results. The same happens with the human and contextual factors because trained and experienced auditors know and study the internal and external environment of an institution to define the audit.

Simultaneously, the technical and contextual factors reached a very high direct correlation, which reveals that the execution of the audit implemented under the planning and selection of appropriate tools ensures the quality of the contextual factor because resources, organizational culture, and the external environment are considered by the audited institution.

It is important to mention that a well-designed audit process must be executed by trained and duly motivated auditors who understand the contextual factors and adjust appropriately to each unique condition of the audit (Imbaquingo et al., 2022).

Among the security factors (confidentiality, integrity, and availability), there is a high correlation between the three, which confirms that by complying with the three pillars of security, the assets and information of any institution can be safeguarded.

By applying the proposed method, HEIs can improve their processes because a successful audit exercise identifies weaknesses and failures to provide recommendations that support decision-making and the continuous improvement of the process within the IT area to benefit the entire organization. Furthermore, as a university achieves generic and specific objectives at a maturity level, it increases its maturity and simultaneously achieves compliance with relevant national laws and regulations.

5. Conclusions

MAIIES considers a comparison and analysis of referential frameworks for computer auditing of international organizations (ISO, ISSAI, ITAF, and IIA'S) recognized worldwide with validity and compliance with the general structure of a computer audit, frequent use, and implementation in audit

processes, used by experts in computer auditing, and that their activities adapt to the processes of HEIs. The creation of the MAIIES involves the phases and activities resulting from the identification and analysis of each framework to be used as a basis for the proposed method, resulting in a complete proposal focused on institutional needs.

An audit must ensure the quality and safety of the results obtained, considering all aspects in each of the phases and their activities, to avoid problems of subjectivity, unqualified reports, lack of credibility in the institutions, loss or alteration of information, unauthorized access, and technical failures that occur with low levels of these indicators. Therefore, when implementing MAIIES, considering the resulting quality and security factors and metrics, the results of a computer audit process can be improved.

The quality of the audit considers three main factors: human, technical, and contextual or environmental factors, each with a group of metrics associated with well-trained and motivated auditors who can design a good audit process, understand the contextual factors, and fully attune to the unique conditions of each audit. The identification of computer audit quality factors and metrics guides the technology departments of HEIs on the relevant aspects of evaluation, control, and management so that future audits can obtain high-quality results, ensuring the reliability and efficiency of the process.

The identification of the pillars and metrics that affect information security and an appropriate statistical multivariate model provides a guide for the prevention, control, and management of vulnerabilities and risks that affect the security of information technology assets of organizations and their users. Thus, the implementation of measures and decision-making in the future have reliable results to maintain effective security within the institution. In addition, the security pillars and their metrics can be used to identify and evaluate security within different institutions that store large amounts of data; they are also of great importance in identifying vulnerabilities for proper audit trails and risk assessment.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3568830

Ahmed, M., & Pathan, A.S.K. (2020). False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, 8(1), 4. https://doi.org/10.1186/s40294-020-00070-w

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A. et al. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences*, 10(10), 3660. https://doi.org/10.3390/app10103660

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 219-238. https://doi.org/10.3390/jcp1020012

Arcentales-Fernández, D., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias*, 3(3), 157-173.

Bates, T. (2018). The 2017 national survey of online learning in Canadian post-secondary education: methodology and results. *International Journal of Educational Technology in Higher Education*, 15(1), 29. https://doi.org/10.1186/s41239-018-0112-3

Cadena, S., Córdova, J., Enríquez, R., & Padilla, R. (2019). *Estado de las Tecnologías de la Información y la Comunicación en las Universidades Ecuatorianas* (CEDIA).

Campos-Pacurucu, J.O., Narváez-Zurita, C.I., Eràzo-Álvarez, J.C., & Ordoñez-Parra, Y.L. (2019). Aplicación del sistema COBIT en los procesos de auditoría informática para las cooperativas de ahorro y crédito del segmento 5. *Visionario Digital*, 3(2.1.), 445-475. https://doi.org/10.33262/visionariodigital.v3i2.1..584

Carpenter, R., & McGregor, D. (2020). The implications, applications, and benefits of emerging technologies in audit. *The Business and Management Review*, 11(02), 36-44. https://doi.org/10.24052/BMR/V11NU02/ART-05

Cienfuegos, S., Gómez, N., & Millas, Y. (2021). *Guía para la realización de las auditorías internas de los sistemas de gestión* (AENOR Ediciones).

Contact Committee of the Heads of the SAIs of the European Union (2004). *Guidelines on Audit Quality*.

Detzen, D., & Gold, A. (2021). The different shades of audit quality: A review of the academic literature. *Maandblad Voor Accountancy en Bedrijfseconomie*, 95(1/2), 5-15. https://doi.org/10.5117/mab.95.60608

Dunn, O. (1958). Estimation of the Means of Dependent Variables. *The Annals of Mathematical Statistics*, 29(4), 1095-1011.

Eom, T., Hong, J.B., An, S., Park, J.S., & Kim, D.S. (2019). A Systematic Approach to Threat Modeling and Security Analysis for Software Defined Networking. *IEEE Access*, 7, 137432-137445. https://doi.org/10.1109/ACCESS.2019.2940039

Esparza, D.E.I., Diaz, F.J., Egas, M.B.R., Sinchiguano, F.A.C., & Misacango, R.A.L. (2020). Evaluation model of computer audit methodologies based on inherent risk. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-7. https://doi.org/10.23919/CISTI49556.2020.9140877

Francis, J.R. (2004). What do we know about audit quality? *The British Accounting Review*, 36(4), 345-368. https://doi.org/10.1016/j.bar.2004.09.003

Francis, J.R. (2011). A Framework for Understanding and Researching Audit Quality. *AUDITING: A Journal of Practice & Theory*, 30(2), 125-152. https://doi.org/10.2308/ajpt-50006

Francis, J.R. (2023). What exactly do we mean by audit quality? *Accounting in Europe*, 1-11. https://doi.org/10.1080/17449480.2023.2247410

García, R., & González, M. (2020). Percepción sobre la integración de las funciones sustantivas en la Universidad Católica de Cuenca. *Varona Revista Científico Metodológica*, 70, 42-47.

Ghazvini, A., Shukur, Z., & Hood, Z. (2018). Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. *International Journal of Advanced Computer Science and Applications*, 9(8). https://doi.org/10.14569/IJACSA.2018.090853

Gkrimpizi, T., Peristeras, V., & Magnisalis, I. (2023). Classification of Barriers to Digital Transformation in Higher Education Institutions: Systematic Literature Review. *Education Sciences*, 13(7), 746. https://doi.org/10.3390/educsci13070746

Guevara, C., Herrera, E., García, I., & Quiña, J. (2020). Incidence of a web application implementation for high school students learning evaluation: A case study. *Revista Iberica de Sistemas e Tecnologias de Informacao*, 509-523.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, 103, 102196. https://doi.org/10.1016/j.cose.2021.102196

Harris, M.K., & Williams, L.T. (2020). Audit quality indicators: Perspectives from Non-Big Four audit firms and small company audit committees. *Advances in Accounting*, 50, 100485. https://doi.org/10.1016/j.adiac.2020.100485

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2022). A process framework for information security management. *International Journal of Information Systems and Project Management*, 4(4), 27-47. https://doi.org/10.12821/ijispm040402

Havelka, D., & Merhout, J.W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, 14(3), 165-192. https://doi.org/10.1016/j.accinf.2012.12.001

Hohan, A.I., Olaru, M., & Pirnea, I.C. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, 32, 352-359. https://doi.org/10.1016/S2212-5671(15)01404-5

Holm, C., & Zaman, M. (2012). Regulating audit quality: Restoring trust and legitimacy. *Accounting Forum*, 36(1), 51-61. https://doi.org/10.1016/j.accfor.2011.11.004

Imbaquingo, D., Pedro, L.S., Diaz, J., Saltos, T., & Arciniega, S. (2021). Let's talk about Computer Audit Quality: A systematic literature review. *2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM)*, 1-7. https://doi.org/10.1109/ICMIAM54662.2021.9715192

Imbaquingo, D., San Pedro, L., Díaz, J., Arciniega, S., Saltos, T., & Ortega, C. (2022). *Computer Auditing Quality Assessment Based on Human, Technical and Contextual Factors* (320-338). https://doi.org/10.1007/978-3-031-20316-9_25

International Auditing and Assurance Standards Board (2014). *A framework for audit quality.* International Federation of Accountants (IFAC).

Jácome, A., Herrera, E., Herrera, I., Caraguay, J., Basantes, A., & Ortega, C. (2019). Análisis temporal y pronóstico del uso de las TIC, a partir del instrumento de evaluación docente de una Institución de Educación Superior. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 399-412.

Knechel, W.R., Krishnan, G.V., Pevzner, M., Shefchik, L.B., & Velury, U.K. (2013). Audit Quality: Insights from the Academic Literature. *AUDITING: A Journal of Practice & Theory*, 32(Supplement 1), 385-421. https://doi.org/10.2308/ajpt-50350

Kure, H., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, 8(6), 898. https://doi.org/10.3390/app8060898

Kurt, S. (2017). Accessibility of Turkish university Web sites. *Universal Access in the Information Society*, 16(2), 505-515. https://doi.org/10.1007/s10209-016-0468-x

Lehmann, E. (2006). *Nonparametrics: Statistical Methods Based on Ranks* (1st ed.). Springer.

Ley Orgánica de Educación Superior (LOES) (2018).

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, 112, 102526. https://doi.org/10.1016/j.cose.2021.102526

Normas Internacionales de Ética para Contadores (IESBA) (2021). Manual del Código Internacional de Ética para Contadores Profesionales incluye Normas Internacionales de Independencia. In *Consejo de Normas Internacionales de Ética para Contadores*.

Nwobi, F., & Akanno, F. (2021). Power comparison of ANOVA and Kruskal−Wallis tests when error assumptions are violated. *Advances in Methodology and Statistics*, 18(2). https://doi.org/10.51936/ltgt2135

O'Hanley, R., & Tiller, J.S. (Eds.) (2013). *Information Security Management Handbook* (7). Auerbach Publications. https://doi.org/10.1201/b15440

Otero, A.R. (2018). Information Technology Control and Audit. In *Information Technology Control and Audit*. Auerbach Publications. https://doi.org/10.1201/9780429465000

Palos-Sanchez, P., Reyes-Menendez, A., & Saura, J.R. (2019). Modelos de Adopción de Tecnologías de la Información y Cloud Computing en las Organizaciones. *Información Tecnológica*, 30(3), 3-12. https://doi.org/10.4067/S0718-07642019000300003

Reguant, M., & Torrado, M. (2016). El método Delphi. *REIRE. Revista d'Innovació i Recerca en Educació*, 9(1). https://doi.org/10.1344/reire2016.9.1916

Rodríguez-Labrada, Y.K., Cano-Inclán, A., & Cuesta-Rodríguez, F. (2018). Estado del arte de la Auditoría de Información. *E-Ciencias de La Información*. https://doi.org/10.15517/eci.v1i1.35409

Rosseel, Y. (2012). lavaan: An *R* Package for Structural Equation Modeling. *Journal of Statistical Software*, 48(2). https://doi.org/10.18637/jss.v048.i02

Salazar, J., & Silvestre, S. (2017). Internet de las cosas (IoT) - Cisco. *Cisco*, 0(0), 7-34.

Sanchez-Puchol, F., Pastor-Collado, J.A., & Borrell, B. (2017). Towards an Unified Information Systems Reference Model for Higher Education Institutions. *Procedia Computer Science*, 121, 542-553. https://doi.org/10.1016/j.procs.2017.11.072

Saputra, T.S., & Ismandra (2023). A Mixed Study into Role of the Internal Audit and Risk Management on the Private Higher Education. In *Proceedings of the International Conference of Economics, Business, and Entrepreneur (ICEBE 2022)* (392-398). https://doi.org/10.2991/978-2-38476-064-0_41

Siyaya, M., Epizitone, A., Jali, L., & Olugbara, O. (2021). Determinants of Internal Auditing Effectiveness in a Public Higher Education Institution. *Academy of Accounting and Financial Studies Journal*, 25(2).

Soy-i-Aumatell, C. (2003). La auditoría de la información, componente clave de la gestión estratégica de la información. *El Profesional de La Informacion*, 12(4), 261-268. https://doi.org/10.1076/epri.12.4.261.16889

Stoel, D., Havelka, D., & Merhout, J.W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*, 13(1), 60-79. https://doi.org/10.1016/j.accinf.2011.11.001

Sulaiman, N.A., Mat-Yasin, F., & Muhamad, R. (2018). Perspectives of Audit Quality: An Analysis. *Asian Journal of Accounting Perspectives*, 11(1), 1-27. https://doi.org/10.22452/AJAP.vol11no1.1

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards–A Review and Comprehensive Overview. In *Electronics (Switzerland),* 11(14), 2181. MDPI. https://doi.org/10.3390/electronics11142181

Taşkın, G., & Sandıkkaya, M.T. (2023). Comparison of Security Frameworks for SMEs. *2023 14th International Conference on Electrical and Electronics Engineering (ELECO)* (1-5). https://doi.org/10.1109/ELECO60389.2023.10416030

Wagner, I., & Eckhoff, D. (2019). Technical Privacy Metrics. *ACM Computing Surveys*, 51(3), 1-38. https://doi.org/10.1145/3168389

Widjajanto, B., Agustini-Santoso, D., & Riiati, N. (2018). Alignment Model of Quality Assurance System of Higher Education And Performance Measurement Based on on Framework CobiT 5. *2018*

International Seminar on Application for Technology of Information and Communication (207-213). https://doi.org/10.1109/ISEMANTIC.2018.8549728

Yang-Wallentin, F., Joreskog, K., & Luo, H. (2010). Confirmatory Factor Analysis of Ordinal Variables With Misspecified Models. *Structural Equation Modeling: A Multidisciplinary Journal*, 17(3), 392-423. https://doi.org/10.1080/10705511.2010.489003

Published by OmniaScience (www.omniascience.com)

Journal of Technology and Science Education, 2024 (www.jotse.org)