Data and Metadata. 2025; 4:185
doi: 10.56294/dm2025185

ORIGINAL

Evaluation of the information technology security of the GAD municipal de Esmeraldas based on internal control standards

Evaluación de la seguridad de tecnología de información del GAD municipal de Esmeraldas basado en las normas de control interno

David Leonardo Rodríguez Portes[1], Mario Bernabé Ron Egas[1], Daisy Elizabeth Imbaquingo Esparza[1]

[1]Universidad Técnica del Norte, Postgrados. Ibarra, Ecuador.

Cite as: Rodríguez Portes DL, Ron Egas MB, Imbaquingo Esparza DE. Evaluation of the information technology security of the GAD municipal de Esmeraldas based on internal control standards. Data and Metadata. 2025; 4:185. https://doi.org/10.56294/dm2025185

Submitted: 07-05-2024 **Revised:** 21-10-2024 **Accepted:** 27-04-2025 **Published:** 28-04-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding author: David Leonardo Rodríguez Portes

ABSTRACT

This research focuses on an audit of information technology security, compliance with current legal regulations, Internal Control Standard (ICS) 410, and the need to constantly evaluate the control environment of a municipality. The type of research was mixed: bibliographic-descriptive, bibliographic for the elaboration of the frame of reference with the collection of existing information in similar research, articles, and regulations; descriptive to collect, analyze and present the information obtained, both through the techniques used (survey, interview, and observation) in the field work and with the application of analytical, deductive and inductive methods, which provided a more complete view of the problem. During the presentation and discussion of the results, an analytical and refined exposition of the main findings was made, evidencing the level of IT risk and the low level of compliance with internal control standards, both those promulgated by the Comptroller General of the State and those established by ISO27001:2022. In the final report, due to the low incidence of the mechanisms implemented on the security of IT assets and existing technological infrastructure, in addition to the conclusions, recommendations and corrective actions that the institution should incorporate to formalize and strengthen its information security management system, through an improvement plan that involves the implementation of institutional security policies, were alsoincluded.

Keywords: ISO27001:2022; IT Risk; Internal Control Standard 410; Security Policies.

RESUMEN

Esta investigación se centra en una auditoria de la seguridad de tecnologías de información, elcumplimiento de la normativa legal vigente, normas de control interno (NCI) 410, y la necesidad de evaluar constantemente el ambiente de control de un municipio. El tipo de investigación fue mixta: bibliográfica-descriptiva, bibliográfica para la elaboración del marco de referencia conla recopilación de información existente en investigaciones similares, artículos, y normativas; Descriptiva para recopilar, analizar y presentar la información obtenida, tanto a través de las técnicas utilizadas (encuesta, entrevista, y observación) en el trabajo de campo como con la aplicación de los métodos analítico, deductivo e inductivo, que proporcionaron una visión más completa de la problemática. Durante la presentación y discusión de los resultados se realizó una exposición analítica y depurada de los principales hallazgos, evidenciado el nivel de riesgo informático, y el bajo nivel de cumplimiento que tiene de las normas de control interno, tanto las promulgadas por la Contraloría General del Estado, como las establecidas por la norma ISO27001:2022. En el informe final, debido a la baja incidencia que tienen los mecanismos implementados sobre la seguridad de los activos informáticos e infraestructura tecnológica existente; además de las conclusiones sobre las cuales la institución deberá incorporar acciones correctivas para formalizar y fortalecer su sistema de gestión de seguridad de Información, a través de un

plan de mejoras que supone la implementación de políticas de seguridad institucional.

Palabras clave: ISO27001:2022; Riesgo Informático; Norma de Control Interno 410; Políticas de Seguridad.

INTRODUCTION

A problem in the public sector is the age and obsolescence of the IT equipment of the vast majority of institutions, coupled with budgetary constraints and low investment in licenses and licensed software, to the point of having a decree that limits spending on this, making it one of the challenges for administrative management when ensuring information protection. Organizations are subject to countless attempts every day by computer criminals to gain access to information and control of their equipment. For institutions that have been victims of cyberattacks, it has not been a priority to train staff and research on possible security measures to be taken to prevent them. In this regard, in April 2021, the National Cybersecurity Policy was approved in the country with application to the public and private sectors.[1]

In Ecuador, there is a reference framework based on ISO 27001 called Governmental Information Security Scheme (EGSI), issued by MINTEL, which is mandatory for Executive institutions, GADS,and State companies and subject to control by the CGE,[2] which facilitated the compilation of a series of ISO27001:2022 templates, it´s mean, updated to the latest version.[3] It was also possible to establish that the CGE standards were updated in 2023,[4] presenting changes and modifications for IT standard 410, where IT Security Standard 410-10 was reformed in its entirety, being now standard 410-11, and significantly changing its provisions, by including aspects such as compliance with the LOPD and the use of standards, enriching the frame of reference with which the research was carried out.[5]

The processes of digital transformation of the institution and the IT risks caused by the use of technologies in the processes, services, infrastructure and facilities of the institution; the lackof real plans; the low level of awareness of public officials; and the failure to comply with current regulations in relation to security; implies the adoption of control mechanisms and the evaluation of compliance with the regulations established by the CGE, Given this, the following question emerges as a general problem: How to evaluate the degree of compliance with the internal control standards of the Comptroller General of the State at the level of information technology security in the Municipal Government of Esmeraldas?, In response to this question, the objective is to evaluate the information technology security of the GADMCE through the internal control standards (ICS); under the hypothesis that the mechanisms applied based on the ICS impact the information security of a municipality with: one thousand employees, 72 000 properties, 10 000 recurring users; in a city with around 300 000 inhabitants.[6]

METHOD

In the collection of primary information for this research, traditional techniques such as interview, observation and survey were used, combined with the application of information collection instruments such as templates and checklists, which together were used in the fieldwork. The survey, through a questionnaire with closed questions based on ISO 27001:2022,was applied to employees to measure the level of awareness of the role of information securityand the security risk to which they are exposed in the institution. These instruments were applied randomly and stratified at the beginning of the first quarter of 2024 to the administrative staff of the directorates or units considered IT users. Once the questionnaires were completed, they were recoded in SPSS by coding all the factors, considering that the instrument used the same scales for all the questions.

From the SPSS version 26 statistical package, the primary data collected through the survey were systematized and analyzed comparing the quantitative results, as well as establishing thelevel of confidence of the instrument, as illustrated in table 1, obtaining a high reliability in the result of Cronbach's Alpha α: 0,857. This means that, by having a higher consistency amongthe survey questions, it implies a higher reliability of the survey.

Table 1. Reliability statistics of the instrument

Cronbach's alpha	Cronbach's alpha based on standardized items	Number of items
,857	,855	20

The interviews were conducted from the last quarter of 2023 to the first quarter of 2024, both with the director and the officials of the ICT Directorate of the Municipality, combined with theuse of templates (matrix) for assessing the IT risk of the institution's assets; two templates wereused to evaluate the degree of compliance in each of the essential aspects of the ISMS and thecontrols included in the ISO 27001 standard updated to 2022.

The observation form was applied to gather information on the facilities, work areas, and IT assets, such as:

the data center (datacenter), computer park, meeting room, servers, network, communication equipment, and the existing technological infrastructure; therefore, multiple visits to the facilities were necessary during the last quarter of 2023 and the beginning of 2024.

DEVELOPMENT

A wide bibliographic and documentary review of the different aspects related to the research topic was carried out: information security, information security audits and evaluation, risk analysis and management, risk management methodologies, internal control, data protection auditing, and the legal regulations in force both at national level with the ICS 410 and 500, and internationally with the ISO 27001:2022 and its related ones; the topics consulted andsummarized according to their taxonomy and dimension were at a general level. Efforts were made to have current sources of information, i.e. less than five years of publication, and of high scientific relevance. We reviewed the basic concepts and definitions, their importance andthe approaches presented by the different methodologies or industry standards, the internal control standards of the CGE updated to 2023, their most important aspects and the new provisions contained therein (standard 410-11), which includes: intellectual property, data protection law, information security and the use of standards, systems and platforms for the public sector.

The analysis of the technological infrastructure and the existing IT security mechanisms in the GADMCE was carried out by means of a documentary review of the inventory of IT assets and the organic statute by processes, provided by the IT Director. Once the control environment, internal processes, buildings and facilities were analyzed, a survey was deployed with closed questions addressed to administrative employees, this instrument was based on the mandatory requirements and annex of the ISO 27001:2022 standard. The assignment of employees was stratified random. Due to the fact that some of them were on vacation, it was necessary to re-deliver the questionnaires to almost 50 % of the employees. This instrument was used to collect information related to the level of awareness that employees have about the role of IT security in the institution and the risks to which the IT assets assigned, used or with which they interactare exposed; becoming a validation input for management when establishing the state of compliance with these parameters.

The reliability of the instrument was validated using SPSS statistical analysis software, for which the respective coding of variables and the generation of tables and graphs of descriptive statistics were performed. For a better understanding of the results, the questions were grouped according to the sections of the ISO 272001:2022 controls, and the descriptive statisticsanalysis was generated based on the frequencies using SPSS version 26 software. This was contrasted with the interview to the Director, initially through a checklist template with closedquestions (complies / does not comply) established for each domain of the mandatoryrequirements and 93 controls established by ISO27001:2022, and classified in four sections (organizational, personnel, physical and technological), to establish the level of maturity or degree of compliance of the ISMS.

To determine the degree to which the mechanisms, procedures, controls, processes, agreements and other activities implemented by the ICT Directorate comply with current regulations, a second interview was requested with the Director and the ICT officers in order to validate the initial result, comparing the evidence and/or support of the answers provided by the Director, reaching a consensus between both parties on the degree of compliance. Thisquantification was carried out through an ISMS status assessment template based on maturity levels, in whose worksheet the status of each evaluated parameter was recorded, both the mandatory and discretionary elements as well as the ISO 27001:2022 controls.

Since the purpose of this phase was to assess the IT risk and identify the security controls implemented by the institution to safeguard the assets, several visits were made to the facilities and infrastructure in order to verify the IT assets in place. In all cases the visit was guided by the officials responsible for each sub-process, in which the technical and proceduralaspects of security were described concerning: technological infrastructure, facilities, data center, information systems, databases, personal data, applications, networks, and operational management.

For a better understanding of the results of the audit based on the confidence levels determined (presented in detail in the audit report in the following chapter), a radial graph was generatedin which the results for each of the variables are visualized.

The GADMCE audit report was prepared considering an evaluation matrix for each of the 410 standards. This document included the results of the field research, i.e. the surveys and their results that ratify the problems, so that through the analysis and interpretation of the results the respective report was prepared with tables, graphs and analysis that allowed synthesizing and evidencing the real state of the institution's technology security. This report contains the conclusions and recommendations of the findings found, as well as the non-conformities and follow-up actions that the institution must address or justify its non-treatment. For this last point, a record was provided for the follow-up of the recommendations, establishing the officerresponsible for the treatment of the nonconformity, and the time period in the event that therecommendation was not immediately complied with.

An instrument developed and used in the performance audits conducted by the CGE at the levelof internal

audits of the provincial governments was used but updated to the reforms of standard 410 of 2023. This instrument consists of a matrix of questions for each of the 17 standards, in order to show and quantify the degree of compliance with them. In this work, theradial graph is introduced as a new methodology to explain the coverage and compliance in the17 edges that represent each standard evaluated in the institution. From the figure represented in the radial chart, the level of maturity of the internal control system in the institution can beappreciated.

Based on the risks identified in the IT assets, the risk associated with the level of compliance of the ISMS, and the recommendations of the audit report that were delivered to the ICT Directorate of the GADMCE, an improvement proposal was developed through the implementation of information security policies for the institution. The purpose of this proposal was to define the objectives, guidelines and basic principles, at the highest level, issued by thehighest authority, in order to regulate the priority aspects to be met by the institution's ISMS, with a long-term validity.

The commitment and guidelines of the highest authority and senior management were definedto protect the information, always guaranteeing its confidentiality, integrity and availability; in addition to preventing and mitigating the risks that were identified both for theIT assets and for the ISMS controls, which may affect it.

RESULTS

Table 2 summarizes the status of each of the clauses of the mandatory requirements that an ISMS must have. In the case of GADMCE, in the evaluation interview conducted with the ICT director, an overall average of 24,10 % was obtained.

Table 2. Results of the evaluation of the status of the mandatory clauses of the ISMS

Clauses	Requirements ISO/IEC 27001	Compliance level	Status
4	Organizational context	20,00 %	Initial
5	Leadership	60,00 %	Definite
6	Planning	33,33 %	Limited
7	Support	32,00 %	Limited
8	Operation	13,33 %	Initial
9	Performance Evaluation	0,00 %	Non-existent
10	Improvement	10,00 %	Initial
	Overall average	24,10 %	Initial

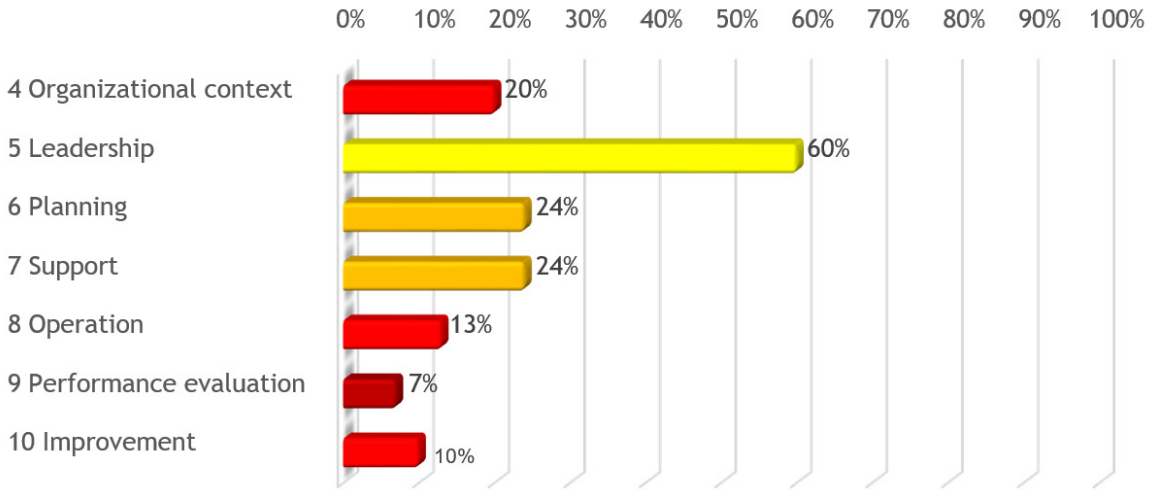

Figure 1. Degree of compliance with mandatory requirements ISO 27001:2022

Figure 1 shows the degree of compliance of each section or clause, where non-compliance wasevidenced in its sections, with the exception of number five (leadership), being the best evaluated with a status of "defined" because its development is partially completed, and this ISMS is not yet implemented, nor has it been endorsed by the highest authority; therefore, thegeneral status of this parameter is "initial", that is: its development has just begun and requires completing a series of activities to meet the requirements established by the regulations to satisfaction. Annex B shows the weighting assigned to each parameter and the calculation madeto quantify the level of maturity of the institution's ISMS based on the status of compliance with each clause.

https://doi.org/10.56294/dm2025185

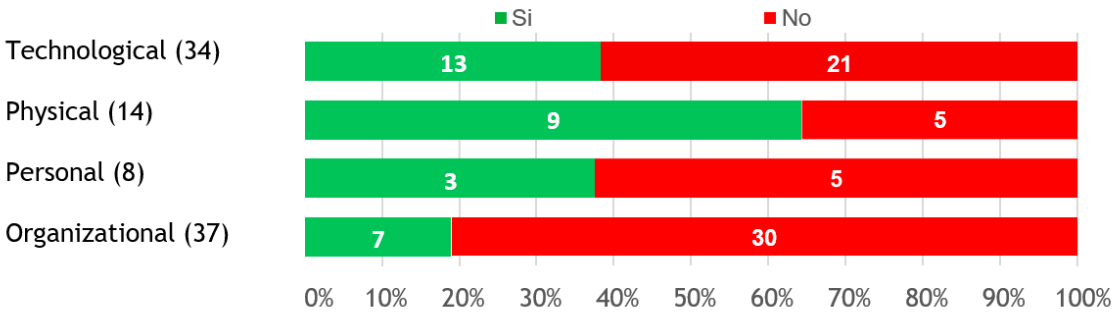

Figure 2. Compliance with ISO 27001:2022 annex controls by category

Figure 2 summarizes (by categories) the result of the evaluation of compliance with the 93 security controls established in the ISO 27001 standard in its annexes of 2022, where it is evident that only 32 of the 93 controls defined by the standard are complied with, i.e. 34 %. Observing the figure, this non-compliance is found in the organizational controls, since only 19 % of them are complied with.

Of the four categories in which the controls are classified by the standard, it was observed thatonly in the case of physical controls there is a satisfactory level of compliance with 9 of the 14controls established, i.e. 64 %. The following is a summary and general analysis for each category of controls and the details of the state of compliance based on the evidence and supports presented by the ICT Director, i.e. their level of maturity.

Table 3. Results of the evaluation of the status of compliance with controls by category

Category	Non-existent	Initial	Limited	Defined	Managed	Optimized	Total
Organizational	9	14	7	1	4	2	37
Personal	1	2	2	1	1	1	8
Physical	3	1	1	2	6	1	14
Technological	6	10	5	3	9	1	34
Total	20	26	15	6	21	5	93

Table 3 shows the distribution of security controls classified by category and by status or degreeof compliance. The high number of controls in “non-existent”, “initial” or limited status, i.e. notsatisfactorily complied with in the institution, was noted. This is best seen in Figure 3, where the percentage distributions show that only in the category of physical controls is more than half of the controls complied with, while the remaining three categories, especially the organizational controls, contain the majority of nonconformities.

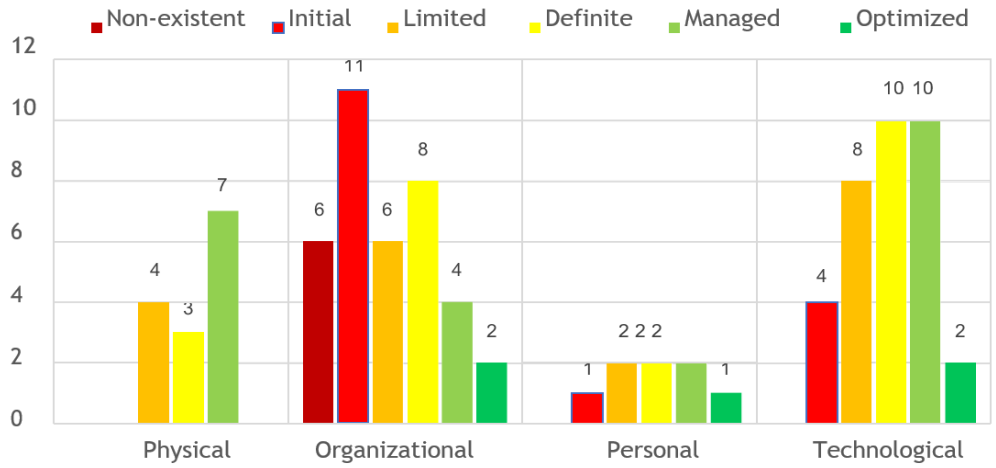

Figure 3. Degree of compliance with ISO 27001:2022 controls by category

Annex B shows the details of all the parameters analyzed for each of the 93 controls and the degree of compliance assigned according to the evaluation carried out, i.e. their level of maturity. This annex contains the evidence presented by the ICT Director, the questionnaire used in the interview with the evaluation question for each control, and the response with the systematized information.

https://doi.org/10.56294/dm2025185

Table 4. Maturity level degree of compliance organizational controls

Status	Meaning of status	Mandatory requirements	Controls Annex A
Non-existent	Complete or legible absence of a policy, procedure, regulation, process, control, etc.	26,09 %	20,43 %
Initial	Development has just begun, and will require considerable work to satisfy the requirements.	39,13 %	29,03 %
Limited	Evidence of progress, progressing well but no evidence of completion or near completion.	17,39 %	16,13 %
Defined	Development is more or less complete but lacking indetail and/or is not yet implemented, compliant, current, or actively endorsed by top management	17,39 %	7,53 %
Managed	Development is complete, the process / control has been implemented and recently started operating	0,00 %	21,51 %
Optimized	The requirement is fully compliant and completed, is fully operational as expected, is being activelymonitored and improved, and there is substantial evidence to demonstrate all of the above to the auditors.	0,00 %	5,38 %
	Total	100,00 %	100,00 %

Source: ISO27001security[7]

Table 4 presents a comparative summary of the result of the evaluation of each of the clausesconsidered as mandatory requirements of the ISMS versus the security controls (mechanisms) established in ISO 27001:2022. Being the level of maturity or states of measurement much lowerin the first case with 19 of 23 non-compliance clauses representing 82,61 % of the total of mandatory requirements evaluated, and even without any parameter in a state of managed oroptimal compliance, the only clause where it meets a state of “defined” is number 5, corresponding to leadership.

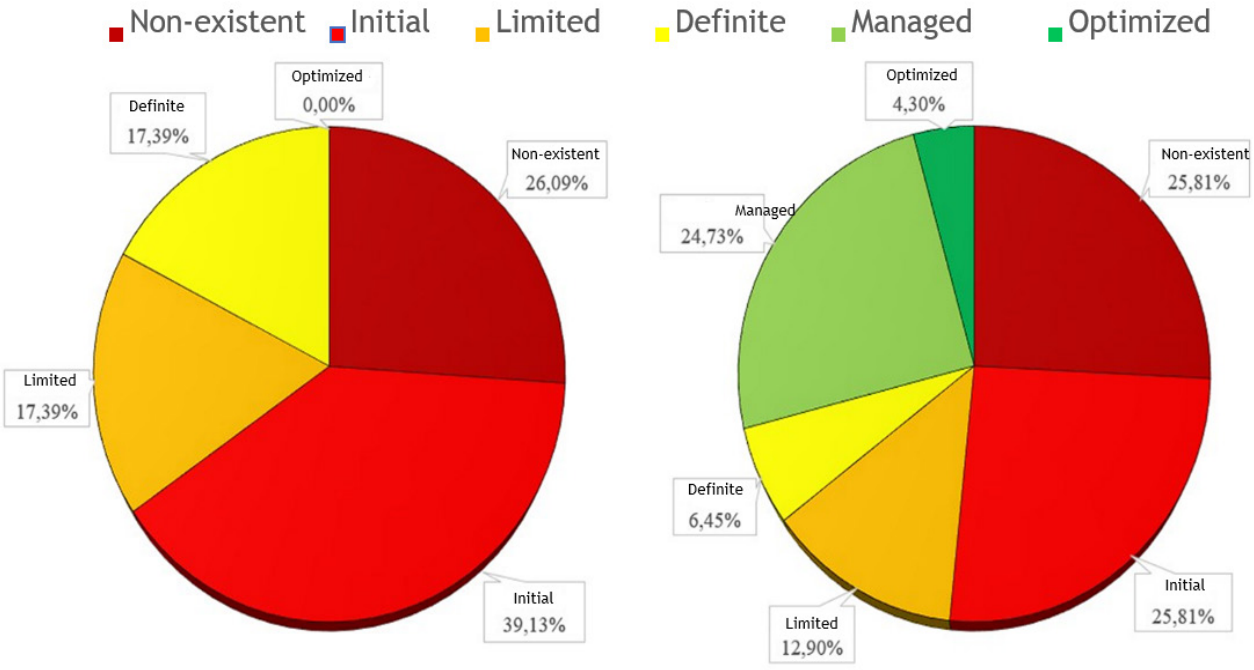

Figure 4. ISMS compliance comparison: Mandatory requirements VS Controls

Figure 4 shows the proportion of compliance (optimal, managed or defined) and non- compliance (non-existent, initial or limited) for each of the two aspects evaluated; however, to better understand the details of the results it is necessary to review the evaluation instrument of the mandatory clauses of the ISMS and the information gathering matrix of the ISMS controls, both are at the end of this document as Annex A and Annex B, respectively.

The second pie chart shows the level of compliance with the controls established in the annexto the standard.

https://doi.org/10.56294/dm2025185

As can be seen, the number of controls that do comply is 32 out of the total of 93, representing 34,41 % of the total number of controls evaluated.

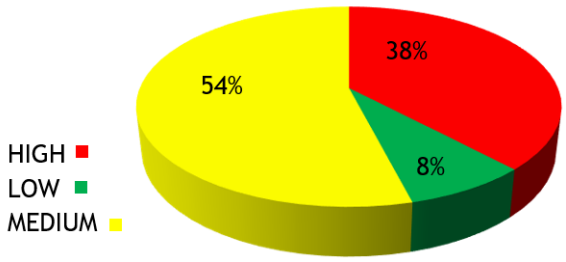

Figure 5. Risk level of GADMCE's IT assets

Figure 5, obtained from the risk analysis of the 50 computer assets considered as critical, where 90 % of the monetary value is concentrated, shows that 38 % present a high security risk. In other words, it can be corroborated that the high-risk equipment represents 59 % of the total inventory of the institution's IT assets, which makes it imperative to apply controls as treatment measures for the risks determined in the evaluation. Of the sample with which the IT risk analysis was carried out, the low-risk assets represent only 8 % of the total and are equivalent to 2 % of the total monetary value. This means that the mechanisms implemented by the ICT Directorate are not affecting the security of the GADMCE's information technology.

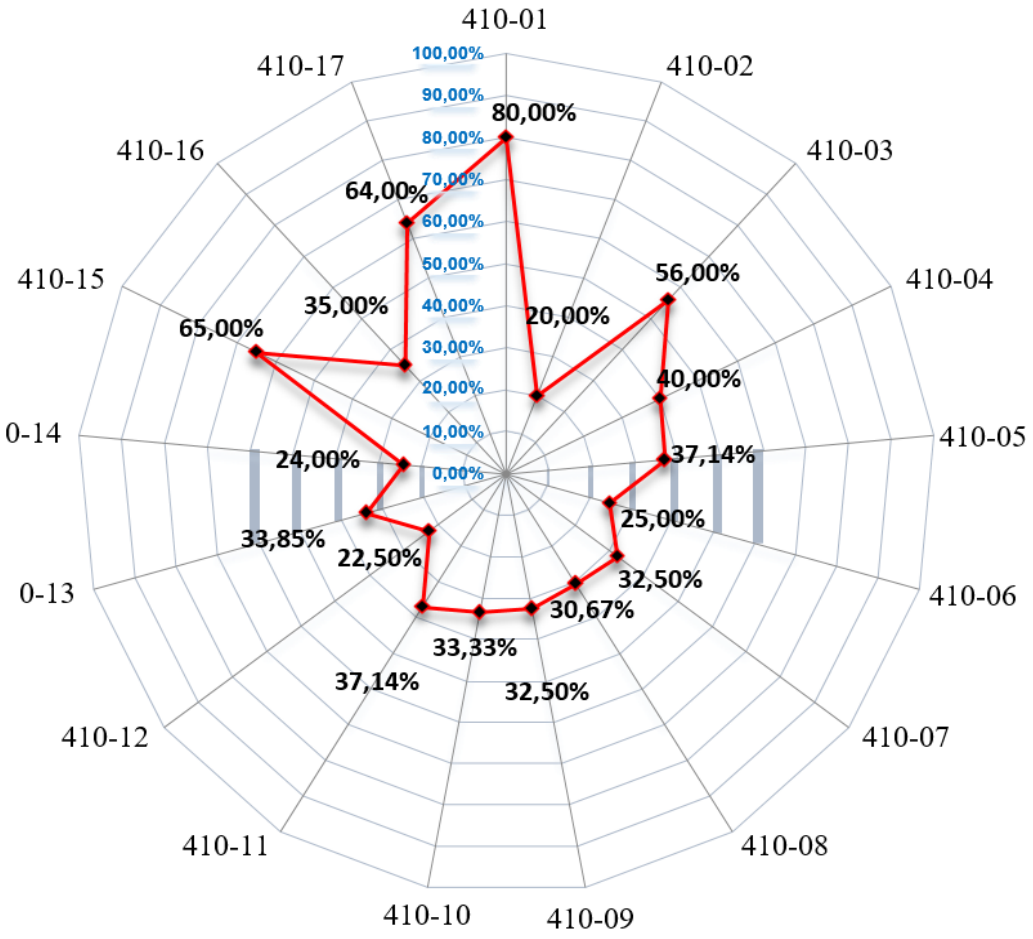

Figure 6. Control environment confidence level - standard 410

From figure 6 represented in the radial graph, the confidence levels determined for each of the variables, i.e. the 17 standards (presented in detail in the audit report in the following chapter), are deduced, obtaining a confidence level (degree of compliance) of 39,33, which implies a high IT risk. The detail of each quantification can be reviewed in Annex F, which also details for each control evaluated, the means of verification that was

https://doi.org/10.56294/dm2025185

used or presented as evidence by the ICT Directorate and contrasted with the responses of the surveys of the employees of the company.

DISCUSSION

In this quantified summary of the evaluation interview of each of the information technology standards carried out with the Director and officials responsible for each IT process, it can be noted that the only standard evaluated with a high level of confidence is 410-01, which impliesa low level of risk related to the organization of the ICT unit in the GADMCE. Likewise, it was possible to identify that only 3 standards (410-03, 410-15 and 410-17) have a medium risk level;and, on the contrary, it was possible to establish that 13 of the 17 standards evaluated have ahigh-risk level, i.e. 76,47 %.

It was proved that the hypothesis raised, once the control environment, the IT assets, and the ISMS of the institution were analyzed under the reference framework of ISO 27001:2022 and ICS 410, it is evidenced that the lack of information security policies causes the implemented mechanisms to have a low degree of compliance in both standards; therefore, they have a negative impact.

CONCLUSIONS

- IT risk is the starting point for implementing IT security mechanisms. ISO 27001:2022 standards specify the controls and mandatory requirements that an institution must comply with in order for an ISMS to be efficient.
- In practice, the IT evaluation based on CEM's internal control standards constitutes an audit of the institutional ISMS, through which it is determined whether the IT securitymechanisms implemented guarantee compliance with the legal regulations in force.
- In every audit report it is necessary that the observations or findings contain the criterion, condition, cause and impact on information security in order to ensure an adequate control environment that safeguards information assets.
- The implementation of security policies, in addition to ensuring compliance with the ICS or ISO 27001, represents the best strategy to turn security into an institutional legacy that not only safeguards information assets, but also public resources in general.
- None of the IT security mechanisms implemented by organizations to protect their technological infrastructure, however costly or complex they may be, are sufficient orefficient if they do not comply with the ICS and do not have an adequate internal control environment that generates trust among users and ensures the availability, integrity and confidentiality of information.

REFERENCES

1. Ecuador. Ministry of Telecommunications and Information Society. Cybersecurity Policy of Ecuador. Ministerial Agreement 006-2021. Registro Oficial del Ecuador Nº479. (June 23, 2019).

2. Ecuador. Ministry of Telecommunications and Information Society. Governmental Information Security Scheme - EGSI. Ministerial Agreement Nº MINTEL-2024-0003. Registro Oficial del Ecuador Nº509. (March 1, 2024).

3. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security controls. (October 25, 2022).

4. Ecuador. Office of the Comptroller General of the State. Internal Control Standards for Entities, Public Sector Agencies and Legal Entities under Private Law that have public resources. Agreement No. 004-CG-2023. Official Gazette (February 7, 2023).

5. European Parliament and Council. Regulation (EU) on ENISA (European Union Cybersecurity Agency) and on the certification of information and communications technology cybersecurity. (April 17, 2019).

6. ISO27001security. 2022. [Accessed December 13, 2023]. Available from: https://www.iso27001security.com/html/27001.ht

7. Decentralized Autonomous Municipal Government of Esmeraldas Canton (GADMCE). Plan de Ordenamiento y Desarrollo Territorial del Cantón Esmeraldas (Territorial Planning and Development Plan of Esmeraldas Canton) (2020).

FINANCING

The authors did not receive funding for the development of this research, that is, it was the author's own

funding.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHOR CONTRIBUTION

Conceptualization: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Data curation: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Formal analysis: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Research: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Methodology: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Project management: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Resources: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Software: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Supervision: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Validation: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Visualization: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Writing – original draft: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.

Writing – review and editing: David Leonardo Rodríguez Portes, Mario Bernabé Ron Egas, Daisy Elizabeth Imbaquingo Esparza.