Article **ECORFAN Journal-Republic of Paraguay**
June, 2021 Vol.7 No.12 1-7

A methodology to evaluate the safety-based witch ISO 25010:2011

Una metodología para evaluar la seguridad basada en la ISO 25010:2011

MEX-ALVAREZ, Diana Concepción†*, HERNANDEZ-CRUZ, Luz María, ORTIZ-CUEVAS, Nancy Georgina and BARRERA-LAO, Francisco Javier

Universidad Autónoma de Campeche

ID 1st Author: *Diana Concepción, Mex-Alvarez* / **ORC ID**: 0000-0001-9419-7868, **Researcher ID Thomson**: I-4164-2018, **CVU CONACYT ID**: 842039

ID 1st Co-author: *Luz María, Hernández-Cruz* / **ORC ID**: 0000-0002-0469-5298, **Researcher ID Thomson**: H3153-2018, **CVU CONACYT ID**: 662220 ID

ID 2nd Co-author: *Nancy Georgina, Ortiz-Cuevas* / **ORC ID**: 0000-0001-9639-1736, **Researcher ID Thomson**: ABC-6473-2021, **CVU CONACYT ID**: 964285

ID 3rd Co-author: *Francisco Javier, Barrera Lao* / **ORC ID**: 0000-0001-5144-8305

DOI: 10.35429/EJROP.2021.12.7.1.7 Received April 08, 2021; Accepted June 30, 2021

Abstract

This paper proposes a methodology to evaluate the security of a web portal based on the international standard ISO 25010:2011. The methodology includes an evaluation instrument, a table of criteria and the formulas necessary to calculate the five security sub-characteristics. Subsequently, the evaluation is executed in the case study "Sistema Institucional de Seguimiento de Convenios" of San Francisco de Campeche as planned, obtaining satisfactory results.

ISO/IEC 25010, Product Quality, Software, SecurityAbstract

Resumen

El presente trabajo propone una metodología para evaluar la seguridad de un portal web con base en la norma estándar internacional ISO 25010:2011. La metodología incluye un instrumento de evaluación, una tabla de criterios y las fórmulas necesarias para calcular las cinco subcaracterísticas de la seguridad. Posteriormente se ejecuta la evaluación en el caso de estudio Sistema Institucional de Seguimiento de Convenios de San Francisco de Campeche según lo planificado, obteniendo resultados satisfactorios.

ISO/IEC 25010, Calidad del producto, Software, Seguridad

Citation: MEX-ALVAREZ, Diana Concepción, HERNANDEZ-CRUZ, Luz María, ORTIZ-CUEVAS, Nancy Georgina and BARRERA-LAO, Francisco Javier. A methodology to evaluate the safety-based witch ISO 25010:2011. ECORFAN Journal-Republic of Paraguay. 2021. 7-12: 1-7

† Researcher contributing as first author.

1. Introduction

With the growing demand for IT, problems have also arisen that compromise people's IT security (Avilés, 2015). Because of this one of the primary objectives is the development of applications that meet the appropriate security quality standards.

Software quality refers to the degree to which the software possesses a combination of desired attributes (Blas *et al*., 2016). There are several models to assess software quality, however, ISO 25010:2011 is a comprehensive model that covers important characteristics such as structure, expression, definitions and relationships (Shiratuddin, 2015).

ISO 25010:2011 defines two quality models (Figure 1):

Quality-in-use model: it is composed of five characteristics related to the degree to which a product or system can be used by specific users and context of uses.

Product quality model: it is composed of eight characteristics related to the static properties of the software and the dynamic properties of the computer system. (Estdale & Georgiadou, 2018)

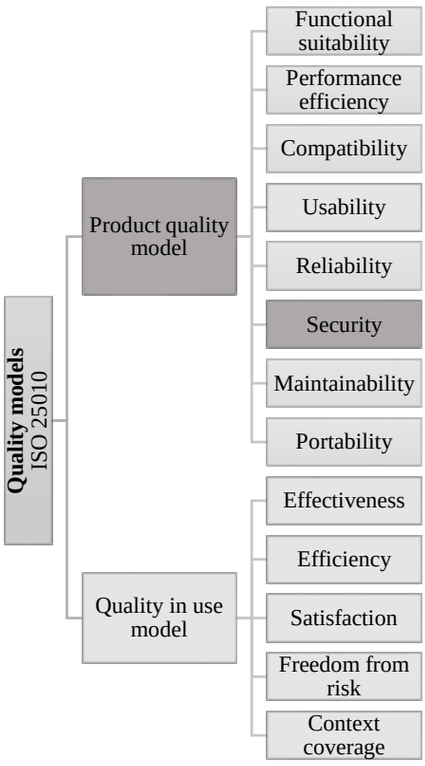


Figure 1 Quality models ISO 25010
Source: Prepared by the authors

The product quality model will be addressed because within its characteristics, it allows evaluating the security section and its sub-characteristics (Figure 2) in a software product (Sekarini *et al*., 2020).

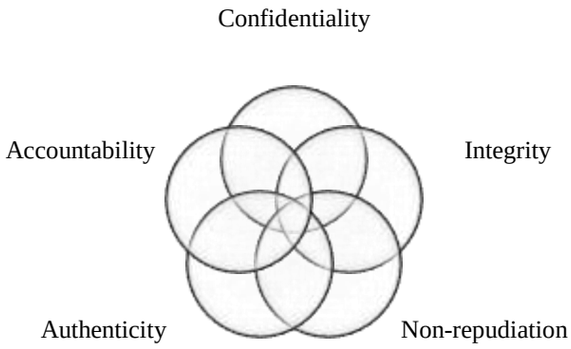


Figure 2 Safety sub-characteristics in Product Quality Model, ISO 25010
Source: Prepared by the authors

Within the product quality model, security refers to the ability of the software product to achieve the protection of users' information and data, where no one, except those authorized, can read or modify them. It presents the following sub-characteristics (ISO/IEC, 2011):

Confidentiality. It is used to evaluate the degree to which a system allows only authorized users to access data.

Integrity. It is used to evaluate the degree to which the system prevents unauthorized access that could modify programs or data.

Non-repudiation. It allows evaluating the degree to which actions or events can be proven to have taken place in the system, so that such actions or events cannot be subsequently repudiated.

Authenticity. Allows to evaluate the degree to which the identity of a subject or resource can be proven.

Accountability. Used to assess the degree to which an entity's actions can be traced unequivocally.

ISSN-On line: 2414-4827

The "Sistema Institucional de Seguimiento de Convenios" (SISC) is a web application that stores the scanned copies of the agreements signed by the "Universidad Autónoma de Campeche" (UAC) with other institutions, facilitating the process of consultation and storage of the results that have been generated in the exercise of the agreement, thus offering a follow-up of the linkage of the UAC with the various institutions (Mex Alvarez *et al*., 2020).

The main objective of this work is to identify whether a web portal complies with the product quality characteristics in its security category defined in the ISO 25010 standard by applying the methodology to the case study defined above as SISC for its subsequent adjustment and improvement, and thus be able to benefit the university community, future generations and research.

The central hypothesis of the case study presented is that the SISC does not comply with most of the security sub-characteristics of the ISO 25010 standard.

The methodology includes an evaluation instrument, a table of criteria and the formulas necessary to calculate the sub-characteristics of security which will help to resolve the central hypothesis of the research.

2. Methodology

The proposed methodology is based on empirical methods consisting of techniques and instruments that require the participation of a target population. (Rubin & Dana, 2008).

The empirical method contemplates the design and application of a data collection instrument that evaluates indicators and metrics obtained from the collection of information from primary sources.

The methodology proposes four phases for the evaluation of a web site considering the Security sub-characteristics in the Product Quality Model, ISO 25010 Standard.

Each of the phases contains a series of actions that guide the conduct of the study.

In Figure 3, we can observe each of the phases with their activities.

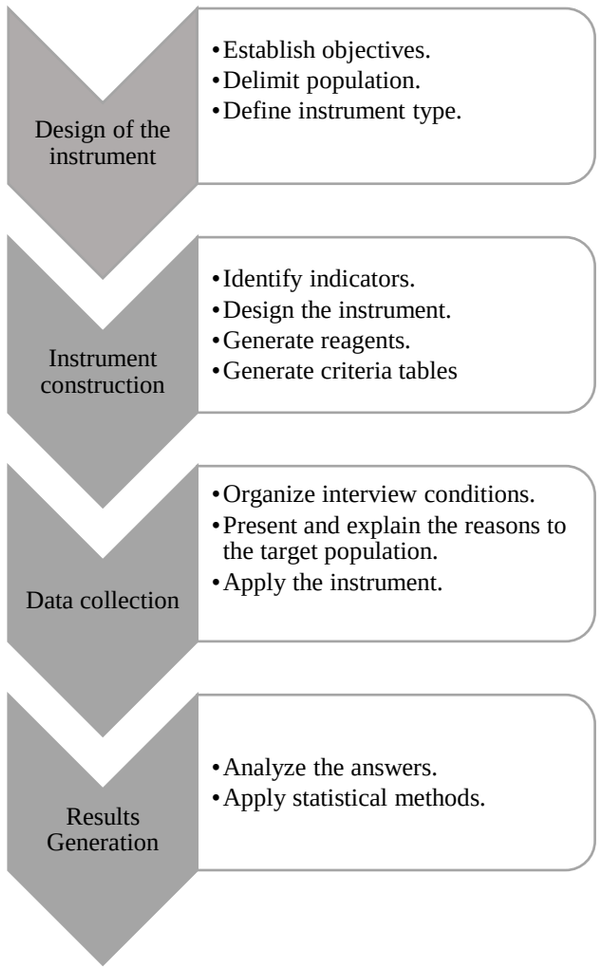


Figure 3. Study phases with their activities to evaluate the security of a web site with the ISO 25010
Source: Prepared by the authors

Each of the phases is described below.

2.1. Design of the instrument

2.1.1. Establish objectives

The objectives of the evaluation are twofold:

– To know the degree of compliance of the product quality subcategories of ISO 25010 in its security category.
– Determine according to the degree of compliance of the subcategories if it is an admissible software product or not.

2.1.2. Delimit the population

The target population is the three web site developers because security issues are considered during the software development stage.

ISSN-On line: 2414-4827

2.1.3. Define instrument type

Due to the fact that the population is a small group and that the information to be obtained is very precise according to the requirements of the standard, the structured interview was chosen as a technique for data collection, which consists of collecting information through a direct communication process between the interviewer and the interviewees, in which the interviewee responds to questions previously designed according to the dimensions to be studied, posed by the interviewer (Bernal, 2010). According to Corbetta (2007), it was decided to conduct a structured interview where the researcher carries out a previous planning of all the questions he/she wants to ask. Questions are prepared and coordinated by a sequenced and directed script. The interviewee will not be able to make any comments or appreciations. The questions will be of a closed type and it will only be possible to affirm, deny or answer a concrete and exact answer about what is being asked.

2.2. Instrument construction

2.2.1. Identify indicators

As mentioned above, ISO 25010 in its safety category establishes five subcategories to establish the instrument's indicators. Based on the above, each of the subcategories was considered as a basis. Table 1 shows the subcategories of the Safety characteristic of the ISO 25010 Standard with the corresponding evaluation indicator and the section of the data collection instrument to which it relates. (França & Soares, 2015)

Product Quality Subcategory for the Safety Feature	Indicator
Confidentiality	The degree to which the system protects unauthorized data and information from accidental or deliberate access.
Integrity	The degree to which the system can prevent unauthorized modifications to data or information.
Non-repudiation	The degree to which the system proves the performance of actions or events, so that such actions or events cannot be subsequently denied
Accountability	The degree to which the system can unambiguously track the actions of an entity.
Authenticity	The degree to which the system demonstrates the identity of a subject or resource.

Table 1. Relationship of subcharacteristic/indicator
Source: Prepared by the authors

2.2.2. Design the instrument

The data collection instrument was divided into 5 sections, so that each section represented 25% of the total. Each section was planned to consist of 4 questions for a total of twenty. The questions, as analyzed, were dichotomous in order to preserve the objectivity of the interviewees. Each section of the questionnaire has a sub-characteristic and an indicator associated with it.

Table 2 shows the relationship of each security subcharacteristic defined in ISO 25010 with the questions of the data collection instrument and the percentages they represent.

Section of the instrument according to the subcategory of Security	Number of questions associated with the indicator	Percentage of total questions
Confidentiality	1-4	20%
Integrity	5-8	20%
Non-repudiation	9-12	20%
Accountability	13-16	20%
Authenticity	17-20	20%

Table 2 Instrument section, question number and total weighting
Source: Prepared by the authors.

2.2.3. Generate reagents

According to the instrument design shown in Table 2, the items were generated to obtain dichotomous answers of true or false.

1. Does the system offer the user the option of data privacy?
2. In the system, is there a way for unregistered users to access the data of registered users?
3. In the system, is there a way for the web site managers to view the personal information of the users?
4. Does the system store in the database an access control?
5. Does the system consider an authenticity step?
6. Does the system ask for a password confirmation when changing user data?
7. Does the system send any notification to the user when there is a data modification?
8. Does the system consider a hierarchy in the access of various data among the site managers?

ISSN-On line: 2414-4827

9. Does the system stores the contact messages that have been sent by users?
10. Does the system sends a confirmation notification when a message is sent?
11. Does the system store in the database a log of the registered items?
12. Does the system consider any kind of requirement to send a message to the contact?
13. Does the system have a regulation?
14. Are the users made aware of the rules and regulations?
15. Are users made aware of the consequences of violating the rules and regulations?
16. If the system has regulations, do the algorithms identify the users who do not comply with these regulations?
17. Does the system allow the connection of the same user in two different access instances?
18. Does the system provide an assistant for the registration of new users?
19. Does the system contemplate that there cannot be two accounts with the same e-mail or user name, but different data?
20. Does the system contemplate the e-mail verification step, when a user is generated?

2.2.4. Generate criteria tables.

A scale was generated to classify the acceptance of the percentage obtained of the total positive criteria. Table 3 shows the proposed ranges and criteria.

Criteria	Range of positive responses
Ineligible	0 <= X < 40%
Minimum allowable	40 <= X < 60%
Admissible	60% <= X < 90%
Excellent	90 < X <= 100%

Table 3 Criteria classification according to percentage of positive responses
Source: Prepared by the authors.

2.3. Data collection

2.3.1. Organize interview conditions

As a case study of the present work, the participation of the three developers of the Institutional Agreement Monitoring System was requested for a group interview to obtain the information. Due to the global contingency due to Covid-19, the interview was conducted virtually with the Meet application.

For the interview, the developers were contacted via e-mail, explaining the reason for the meeting, who would be conducting the interview, the date and time, as well as the link to access the interview.

Present and explain the reasons to the target population.

After starting the connection through the Meet application, the interviewer explained to the interviewees the objective of the interview, which is to know if the system is an admissible software product or not, according to the degree of compliance with the subcharacteristics of ISO 25010.

2.3.2. Present and explain the reasons to the target population

The interviewer explained to the interviewees how the interview is composed, how many questions are included and of what type.

2.3.3. Apply the instrument

The interviewer proceeded to read the questions to the interviewees and asked for their affirmative or negative answers. In some questions it was necessary for the interviewer to elaborate a little more on the question. The interviewees, for their part, gave some answers by showing the system and its components.

2.4. Results Generation

2.4.1. Analyze the answers

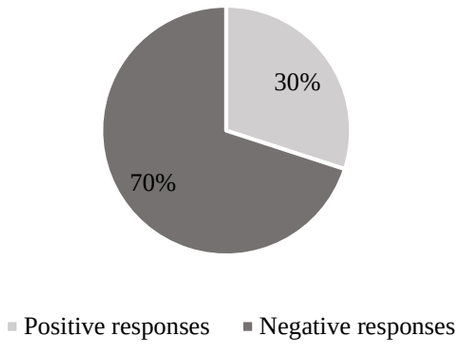
After having responded, the results of which were as follows (Table 4).

Section of the instrument according to Security subcategories	Number of positive responses	Percentage of total questions
Confidentiality	2/4	10%
Integrity	2/4	10%
Non-repudiation	0/4	0%
Accountability	0/4	0%
Authenticity	2/4	10%
	Total	30%

Table 4 Subcategory ratio with respect to positive SISC responses
Source: Prepared by the authors.

ISSN-On line: 2414-4827

Analyzing the results obtained, we observe that in the items of confidentiality, integrity and authenticity, out of 4 questions only 2 were positive, contributing 30% of the total percentage of questions.



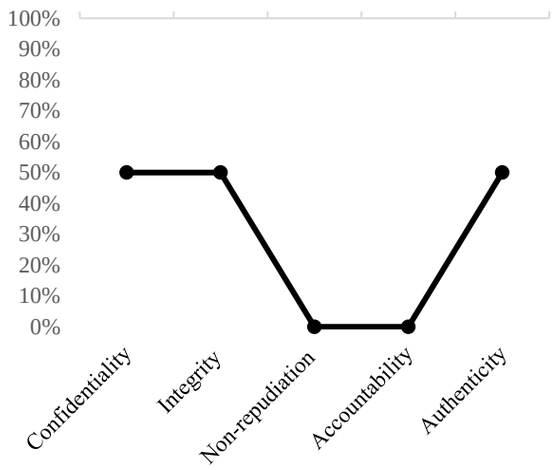
Graphic 1 Percentage of SISC responses
Source: Prepared by the authors

2.4.2. Apply statistical methods

According to the results shown in Graph 1, only 30% of the safety questions were met and 70% were not favorable. According to Table 4, on the classification of acceptance of criteria, its classification is in the range of unacceptable. The above leads us to conclude that the degree of compliance with each indicator is as shown in the table 5.

Indicator	Degree of compliance
Degree to which the system protects unauthorized data and information from accidental or deliberate access.	50%
Extent to which the system can prevent unauthorized modifications to data or information.	50%
Degree to which the system tests the performance of actions or events, so that such actions or events cannot be subsequently denied.	0%
Extent to which the system can unambiguously track the actions of an entity.	0%
Degree to which the system demonstrates the identity of a subject or resource.	50%

Table 5 Ratio of indicator/degree of compliance
Source: Prepared by the authors



Graphic 2 Percentage of compliance by subcategory
Source: Prepared by the authors

3. Conclusions

The hypothesis stated at the beginning proved to be true, since the study showed that 70% of the questions on security were negative, classifying the Institutional Agreement Monitoring System as ineligible.

The security evaluation showed that it is necessary to reinforce the protection of unauthorized data and information against accidental or deliberate access, as well as to prevent unauthorized modifications to data or information, in addition to improving the monitoring of the identity of a subject or resource.

However, the characteristics that require complete attention are those related to non-repudiation and responsibility, therefore, it must be considered that the user in case of an error can deny performing actions or events later, on the other hand, it is essential to generate a regulation on the management of the system.

4. Thanks

The authors thank the Faculty of Engineering of the Autonomous University of Campeche for the facilities granted to carry out and disseminate this work.

ISSN-On line: 2414-4827

5. References

Avilés, G. G. (2015). Seguridad en bases de datos y aplicaciones web. IT Campus Academy. Bernal, C. (2010). Metodología de la Investigación: administración, economía, humanidades y ciencias sociales. 3ra. Edición. Pearson Educación: Colombia.

Blas, M. J., Gonnet, S. M., & Leone, H. P. (2016). Especificación de la Calidad en Software-as-a-Service: Definición de un Esquema de Calidad basado en el Estándar ISO/IEC 25010. In Simposio Argentino de Ingeniería de Software (ASSE 2016)-JAIIO 45. Corbetta, P. (2007). Métodos de investigación educativa. Madrid: La muralla.

Estdale, J., & Georgiadou, E. (2018). Applying the ISO/IEC 25010 quality models to software product. In European Conference on Software Process Improvement (pp. 492-503). Springer, Cham.

ISO/IEC. (2011). ISO/IEC 25010: 2011 Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models.

Mex Alvarez, D. C., Perera Abreu, E., Ortiz Cuevas, N. G., & Gutiérrez González, J. A. (2020). Construcción de Indicadores del Sistema Institucional de Seguimiento de Convenios. Multidisciplinas de la Ingeniería, Año VII. No. 10.

Rubin, J., & Dana, C. (2008). Handbook of Usability Testing: How to plan, Desing, and Conduct Effective Tests. Indianápolis (Indiana): Wiley Publishing, Inc.

Sekarini, D., Alfiani, F. S., & Rochimah, S. (2020). Security Characteristic Evaluation of New Students Admission Information System Based on ISO/IEC 25010 Quality Standard. In 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE) (pp. 120-124). IEEE.

Shiratuddin, N. (2015). Evaluation of e-Book applications using ISO 25010. In 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET) (pp. 114-118). IEEE.

ISSN-On line: 2414-4827