Digital Object Identifier: 10.24054/rcta.v2i46.4111

Digital tool to optimize audits based on the ISO/IEC 27001:2022 standard

Herramienta digital para optimizar auditorías basadas en el estándar ISO/IEC 27001:2022

Sebastián Buesaco[1], Alejandro Alcaraz Gaviria[1], Msc. Juan José Caiza Narváez[1], Msc. Katerine Márceles Villalba[2], PhD. (c) Siler Amador Donado[3]

*[1] **Institución Universitaria Colegio Mayor del Cauca,** Facultad de Ingeniería, Grupo de investigación I+D en Informática, Popayán, Cauca, Colombia.*
*[2] **Universidad de Antioquia,** Facultad de Ingeniería, Grupo de Investigación In2Lab, Medellín, Antioquia, Colombia.*
*[3] **Universidad del Cauca,** Facultad de Ingeniería Electrónica y Telecomunicaciones, Grupo de Investigación GTI, Popayán, Cauca, Colombia.*

***Correspondence:** katerine.marceles@udea.edu.co*

***Received:** april 24, 2025. **Accepted:** july 03, 2025. **Published:** august 09, 2025.*

***How to cite:** S. Buesaco, A. Alcaraz Gaviria, J. J. Caiza Narváez, K. Marceles Villalba, and S. Amador Donado, "Digital tool to optimize audits based on the ISO/IEC 27001:2022 standard", RCTA, vol. 2, no. 46, pp. 209–216, Aug. 2025. Recovered from https://ojs.unipamplona.edu.co/index.php/rcta/article/view/4111*

Abstract: This article presents an applied research study focused on the design, development, and validation of SECUREISO, a digital tool aimed at optimizing audit processes in information security management systems aligned with the ISO/IEC 27001:2022 standard. The study employed an agile methodological framework (Scrum), combining secure development practices with empirical validation techniques, including automated penetration testing using OWASP ZAP and the Technology Acceptance Model (TAM). Results demonstrate levels of usability, perceived usefulness, and operational efficiency. Furthermore, its flexible and scalable architecture enables adaptation to diverse sectors. This work contributes to the cybersecurity field by offering a replicable, research-based solution that enhances standard implementation and opens new avenues for investigation in automated digital auditing.

Keywords: ISO/IEC 27001, information security, audit tool, agile development, OWASP ZAP, TAM model, secure development, cybersecurity.

Resumen: Este artículo presenta una investigación aplicada orientada al diseño, desarrollo y validación de SECUREISO, una herramienta digital concebida para optimizar los procesos de auditoría en sistemas de gestión de seguridad de la información, bajo el estándar ISO/IEC 27001:2022. La investigación adoptó un enfoque metodológico ágil (Scrum), combinando desarrollo seguro con técnicas de validación empírica, como pruebas de penetración automatizadas con OWASP ZAP y el Modelo de Aceptación Tecnológica (TAM). Los resultados evidencian niveles de usabilidad, utilidad y eficiencia percibida por los usuarios. Además, se destaca su arquitectura flexible y escalable, lo que permite su adaptación a diferentes sectores. Este trabajo contribuye al campo de la ciberseguridad con una solución replicable y fundamentada, que mejora la implementación normativa y promueve nuevas líneas de investigación en auditoría digital automatizada.

Palabras clave: ISO/IEC 27001, seguridad de la información, herramienta de auditoría, desarrollo ágil, OWASP ZAP, modelo TAM, desarrollo seguro, ciberseguridad.

1. INTRODUCTION

Currently, information is essential to ensure continuity, trust, and sustainability within organizations, including both business and governmental entities. In Europe and Latin America, the adoption of international standards such as ISO/IEC 27001 has increased significantly due to the efficient framework it provides for creating and managing information security management systems. This framework allows organizations to protect digital assets, mitigate risks, and comply with demanding regulatory frameworks [1], [2], [10].

However, implementing this standard still poses significant challenges stemming from its high technical complexity, difficulties in adapting to specific contexts, and the manual nature of many auditing processes, which are often slow, costly, and prone to errors. These issues directly affect the effectiveness of information security management systems [3], [4], [11].

These challenges justify the need for innovative digital advancements that enable automation of processes related to the evaluation and implementation of the ISO/IEC 27001:2022 standard. Various studies have shown that the use of emerging technologies and business intelligence contributes significantly to enhancing security processes, information storage, and risk analysis, offering a more comprehensive and accurate view of the actual state of organizational security [5], [6], [9], [18].

Accordingly, the general aim of this proposal was to develop a digital tool that, through a secure development methodological framework, optimizes the processes of implementing the ISO/IEC 27001 standard. The proposed tool aims not only to accelerate and automate the auditing work but also to address threats such as unauthorized access in web and mobile environments, as well as improve the identification, prioritization, and treatment of risk [19].

The development was carried out using the Scrum agile methodology, which is widely employed in technological projects requiring adaptability, continuous iteration, and incremental delivery [7].

It is worth noting that the effective implementation of a digital tool based on the ISO/IEC 27001 standard can represent a key competitive advantage by enabling organizations to adopt a more robust, efficient, and resilient cybersecurity management approach in an increasingly complex and dynamic ecosystem.

This article is structured as follows: Section two presents the methodological framework; Section three outlines the results obtained; and Section four includes the conclusions, a discussion space, future work proposals, and the author's contribution.

2. METHODOLOGY

The present study was conducted using an applied methodological approach with a technological design, aimed at solving a practical problem through the creation of a digital solution based on international standards such as the ISO/IEC 27001:2022 standard [1]. An agile methodology was employed, using the Scrum framework as the foundation for planning, development, evaluation, and validation of the tool [7].

The design and construction process was structured into four phases:

Planning Phase: In this phase, the functional and non-functional requirements of the tool were defined, and user stories were structured. A clear vision of deliverables and product backlog organization was also established [7].
Iterative Development Phase: Multiple two-week sprints were executed, during which the tool's modules were designed and implemented. Technologies such as Flutter for the frontend, Node.js for the backend, and PostgreSQL as the database management system were used. The adopted technical architecture followed the Model-View-Controller (MVC) pattern, ensuring system modularity, maintainability, and scalability.
Evaluation and Testing Phase: Automated security tests were performed using the OWASP ZAP tool, identifying common vulnerabilities such as injection flaws and authentication issues, in line with the controls required by the ISO/IEC 27002:2022 standard [6]. To assess user acceptance of the technology, the Technology Acceptance Model (TAM) proposed by Davis [8] was applied, allowing measurement of perceived usefulness, ease of use, and willingness to adopt the tool.
Final Validation Phase: Feedback derived from user experience was integrated, a functional acceptance test was conducted, and findings were documented. This phase concluded with practical recommendations to improve and scale the solution, taking real organizational environments into account.

It is important to highlight the differentiating elements of the methodological approach:

- **Regulatory Alignment:** The tool was explicitly developed in accordance with the new controls defined in the 2022 version of ISO/IEC 27001, which enabled the integration of updated information security aspects into its architecture and functionalities [1], [6], [12].
- **Hybrid Methodology:** The agile Scrum approach was combined with both quantitative and qualitative evaluation techniques, ensuring continuous iteration during development and empirical validation based on evidence [7], [8].
- **Security by Design:** Security testing was integrated from the early stages of development, adopting secure development principles and testing methodologies widely recognized in the industry [11].
- **Empirical Validation:** Structured instruments based on the Technology Acceptance Model (TAM) were applied to validate the tool's usability, effectiveness, and efficiency in real-world contexts, enabling ongoing improvement and adaptation [8], [20].

3. RESULTS

The evaluation of the developed digital tool validated its functionality, security, and user perception. The findings obtained from the previously described phases are presented below.
During the development phase, a modular tool was built with a clean and intuitive interface, developed using Flutter, and based on the Model-View-Controller (MVC) design pattern. Key functionalities were integrated, including control management, automated auditing, report generation, and analysis of compliance with the requirements defined by the ISO/IEC 27001:2022 standard [1]. This technical approach allowed for greater scalability and maintainability of the solution, aligning with secure development best practices as proposed in [7], [15].

Figure 1 presents an overview of each phase in the evolution of the application development.

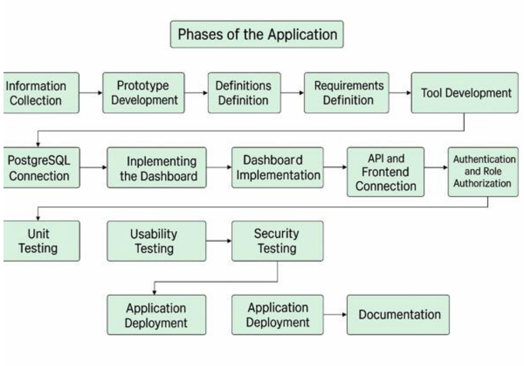


Fig. 1. Diagram of the application's development phases.
***Source:** Own elaboration.*

Based on the above, a tool was obtained that was structured through an iterative and incremental development process (see the following figures).

Fig. 2. Imagen de Inicio de sesión.

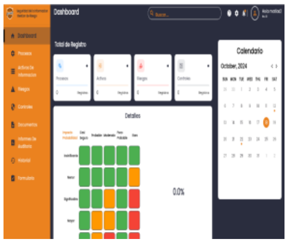


Fig. 3. Versión final del sistema de gestión de riesgos, con la matriz de impacto.

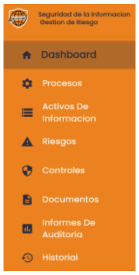
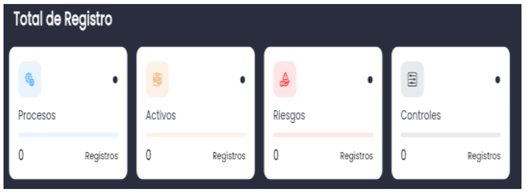


Fig. 4 Funciones Dashboard.

***Fuente:** elaboración propia.*



Total de Registro

Procesos 0 Registros
Activos 0 Registros
Riesgos 0 Registros
Controles 0 Registros

Fig. 5. Imagen de Total Registro
***Fuente:** elaboración propia.*

During the evaluation and testing phase, security analyses were carried out using OWASP ZAP. As a result, vulnerabilities related to missing security headers, improvement suggestions in token usage, and warnings about sensitive information exposure were identified and mitigated [11], [15]. These tests included techniques such as spidering and input fuzzing on frontend and backend forms. The findings helped reinforce the authentication and authorization mechanisms of the tool, in line with the guidelines established in previous studies [5], [13].

The implementation of testing from the early stages was based on security recommendations in the software development lifecycle. In the same vein, it is important to mention that the evaluation process of the SECUREISO digital tool focused on its efficiency and effectiveness within the framework of the ISO/IEC 27001:2022 standard [1]. Efficiency was understood as the rational use of resources, minimizing time and effort; while effectiveness was related to the successful achievement of the security objectives established in the standard.

For this evaluation, the Technology Acceptance Model (TAM) was used, recognized for measuring users' perception of the usefulness and ease of use of technological solutions [8]. The study was applied in organizational contexts seeking to implement more agile and secure information security management systems, with a sample of 5 users, some assuming the role of auditor and others as the organization [20].

A questionnaire consisting of 14 questions was developed: nine focused on effectiveness (such as compliance with the standard's requirements and reduction in implementation time), and five on efficiency (such as the organization of controls and clear information management). The questions addressed different levels of user experience and aimed to evaluate key aspects such as ease of navigation, practicality, and clarity in the application of controls.

The results obtained reflected a highly positive perception: Regarding effectiveness, 97.5% of users considered that the tool facilitates compliance with the standard's requirements and prefer its use over traditional methods such as spreadsheets [12] (see Figure 6).

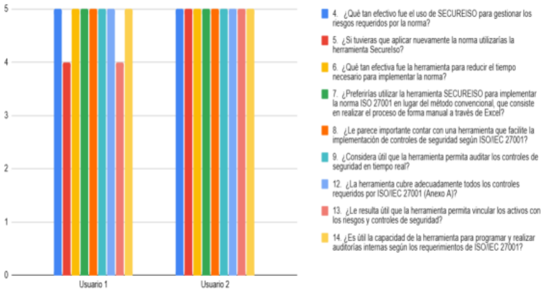


Fig. 6. *Categorization of effectiveness questions.*
Source: *Own elaboration.*

Regarding efficiency, the tool received an average rating of 89%, standing out for its ease of navigation, although with opportunities for improvement in the clarity of some controls [14] (see Figure 7).

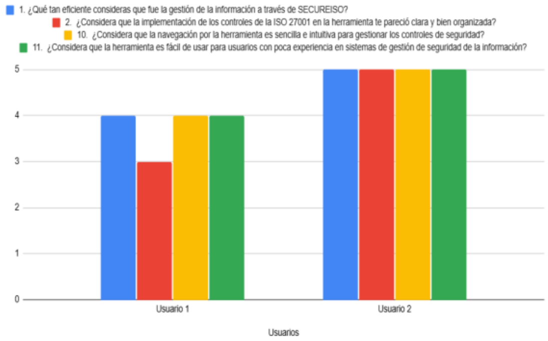
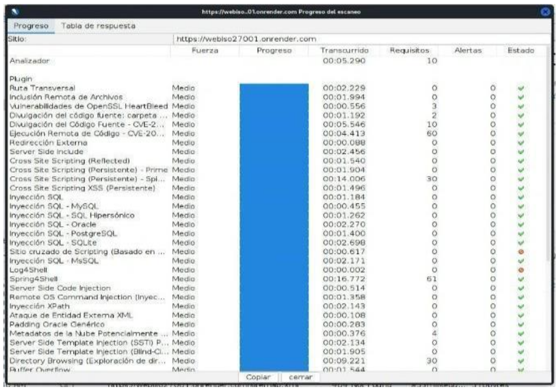


Fig. 7. *Categorization of efficiency questions.*
Source: *Own elaboration.*

These metrics demonstrate that SECUREISO successfully optimizes the implementation process of the ISO/IEC 27001 standard, offering an intuitive and accessible experience for various user profiles. Additionally, the TAM analysis made it possible to establish correlations between perceived usefulness and acceptance levels, validating that the tool not only fulfills its functional purpose but also facilitates its adoption in real-world scenarios [8], [20].

The security tests conducted on the SECUREISO tool employed OWASP ZAP as the primary tool for identifying vulnerabilities in both the frontend and backend of the system. These tests included automated attacks such as spidering and fuzzing [15].

During the spidering attack on the frontend, injection risks (example: SQL) were detected that could be exploited to manipulate or extract data. Although these risks were classified as medium-level, input validation improvements were implemented to reduce exposure (see Figure 8).



Sitio: https://webiso27001.onrender.com

	Fuerza	Progreso	Transcurrido	Requisitos	Alertas	Estado
Analizador			00:05.290	10		
Plugin						
Ruta Transversal	Medio		00:02.229	0	0	✓
Inclusión Remota de Archivos	Medio		00:01.994	0	0	✓
Vulnerabilidades de OpenSSL HeartBleed	Medio		00:00.556	3	0	✓
Divulgación del código fuente: carpeta ...	Medio		00:01.192	2	0	✓
Divulgación del Código Fuente - CVE-2...	Medio		00:05.546	10	0	✓
Ejecución Remota de Código - CVE-20...	Medio		00:04.413	60	0	✓
Redirección Externa	Medio		00:00.088	0	0	✓
Server Side Include	Medio		00:02.456	0	0	✓
Cross Site Scripting (Reflected)	Medio		00:01.540	0	0	✓
Cross Site Scripting (Persistente) - Prime	Medio		00:01.904	0	0	✓
Cross Site Scripting (Persistente) - Spi...	Medio		00:14.006	30	0	✓
Cross Site Scripting XSS (Persistente)	Medio		00:01.496	0	0	✓
Inyección SQL	Medio		00:01.184	0	0	✓
Inyección SQL - MySQL	Medio		00:00.455	0	0	✓
Inyección SQL - SQL Hipersónico	Medio		00:01.262	0	0	✓
Inyección SQL - Oracle	Medio		00:02.270	0	0	✓
Inyección SQL - PostgreSQL	Medio		00:01.400	0	0	✓
Inyección SQL - SQLite	Medio		00:02.698	0	0	✓
Sitio cruzado de Scripting (Basado en ...	Medio		00:00.617	0	0	●
Inyección SQL - MsSQL	Medio		00:02.171	0	0	✓
Log4Shell	Medio		00:00.002	0	0	●
Spring4Shell	Medio		00:16.772	61	0	✓
Server Side Code Injection	Medio		00:00.514	0	0	✓
Remote OS Command Injection (Inyec...	Medio		00:01.358	0	0	✓
Inyección XPath	Medio		00:02.143	0	0	✓
Ataque de Entidad Externa XML	Medio		00:00.108	0	0	✓
Padding Oracle Genérico	Medio		00:00.283	0	0	✓
Metadatos de la Nube Potencialmente ...	Medio		00:00.376	4	0	✓
Server Side Template Injection (SSTI) P...	Medio		00:02.134	0	0	✓
Server Side Template Injection (Blind-Cl...	Medio		00:01.905	0	0	✓
Directory Browsing (Exploración de dir...	Medio		00:09.221	30	0	✓
Buffer Overflow	Medio		00:01.544	0	0	✓

Fig. 8. *Results of spidering attack - Front-end.*
Source: *Owasp-zap.*

Additionally, the response per second graph was analyzed under multiple requests, where spikes were observed that could represent a significant load in the event of a denial-of-service attack. This revealed optimization opportunities in the server's response capacity, as recommended by stress testing standards for secure applications [5], [13] (see Figure 9).

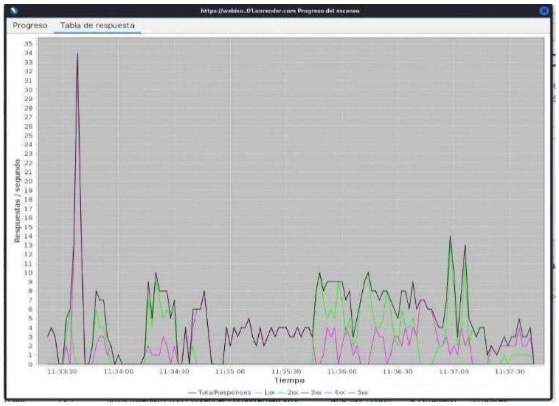
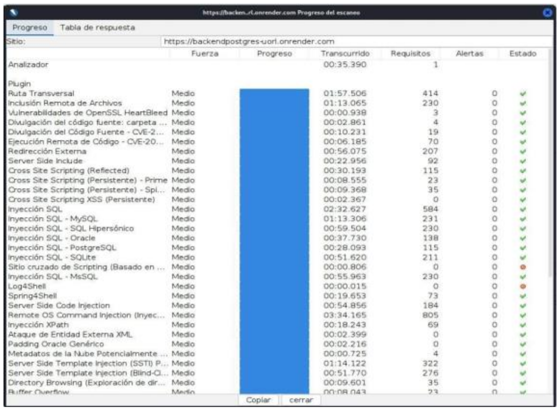


Fig. 9. *Response graph - spidering attack.*
Source: *Owasp-zap.*

In the backend, the spidering attack revealed critical vulnerabilities such as Path Traversal and SQL Injection, which could allow unauthorized access to files or manipulation of sensitive data. These vulnerabilities were prioritized in the risk mitigation plan, in accordance with the security recommendations of the ISO/IEC 27001:2022 standard [1], [15] (see Figure 10).



Sitio: https://backendpostgres-uorl.onrender.com

	Fuerza	Progreso	Transcurrido	Requisitos	Alertas	Estado
Analizador			00:35.390	1		
Plugin						
Ruta Transversal	Medio		01:57.506	414	0	✓
Inclusión Remota de Archivos	Medio		01:13.065	230	0	✓
Vulnerabilidades de OpenSSL HeartBleed	Medio		00:00.938	3	0	✓
Divulgación del código fuente: carpeta ...	Medio		00:02.861	4	0	✓
Divulgación del Código Fuente - CVE-2...	Medio		00:10.231	19	0	✓
Ejecución Remota de Código - CVE-20...	Medio		00:06.185	70	0	✓
Redirección Externa	Medio		00:56.075	207	0	✓
Server Side Include	Medio		00:22.956	92	0	✓
Cross Site Scripting (Reflected)	Medio		00:30.193	115	0	✓
Cross Site Scripting (Persistente) - Prime	Medio		00:08.555	23	0	✓
Cross Site Scripting (Persistente) - Spi...	Medio		00:09.368	35	0	✓
Cross Site Scripting XSS (Persistente)	Medio		00:02.367	0	0	✓
Inyección SQL	Medio		02:32.627	584	0	✓
Inyección SQL - MySQL	Medio		01:13.306	231	0	✓
Inyección SQL - SQL Hipersónico	Medio		00:59.504	230	0	✓
Inyección SQL - Oracle	Medio		00:37.730	138	0	✓
Inyección SQL - PostgreSQL	Medio		00:28.093	115	0	✓
Inyección SQL - SQLite	Medio		00:51.620	211	0	✓
Sitio cruzado de Scripting (Basado en ...	Medio		00:00.806	0	0	●
Inyección SQL - MsSQL	Medio		00:55.963	230	0	✓
Log4Shell	Medio		00:00.015	0	0	●
Spring4Shell	Medio		00:19.653	73	0	✓
Server Side Code Injection	Medio		00:54.856	184	0	✓
Remote OS Command Injection (Inyec...	Medio		03:34.165	805	0	✓
Inyección XPath	Medio		00:18.243	69	0	✓
Ataque de Entidad Externa XML	Medio		00:02.399	0	0	✓
Padding Oracle Genérico	Medio		00:02.216	0	0	✓
Metadatos de la Nube Potencialmente ...	Medio		00:00.725	4	0	✓
Server Side Template Injection (SSTI) P...	Medio		01:14.122	322	0	✓
Server Side Template Injection (Blind-Cl...	Medio		00:51.770	276	0	✓
Directory Browsing (Exploración de dir...	Medio		00:09.601	35	0	✓
Buffer Overflow	Medio		00:08.043	23	0	✓

Fig. 10. *Results of spidering attack - Backend.*
Source: *Owasp-zap.*

The backend server's response was also analyzed during load simulation and mass scanning. HTTP 500 and 403 errors were identified at times of high concurrency, suggesting the need for adjustments in session handling logic and internal validation mechanisms [9], [11] (see Figure 11).

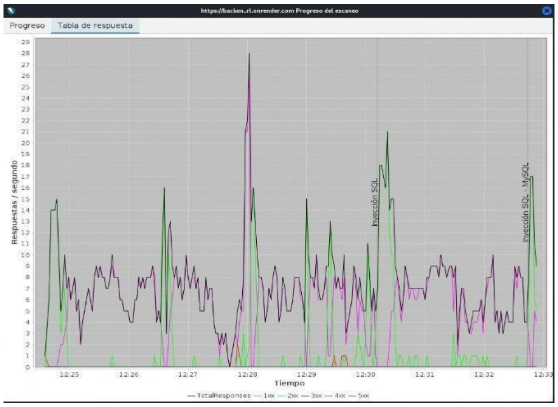


Fig. 11. *Response graph - spidering attack.*
Source: *Owasp-zap.*

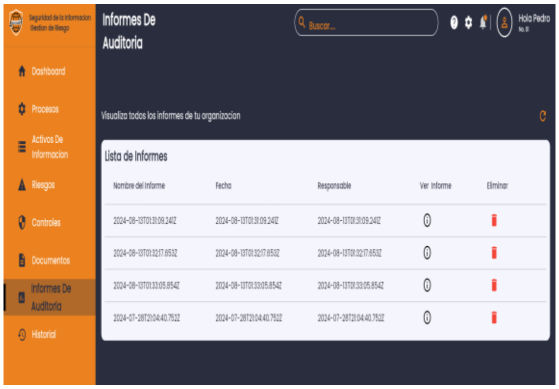
Additionally, a fuzzing attack was conducted, which revealed informational risks related to the exposure of technical messages concerning sessions and authentication errors. While these details do not constitute critical vulnerabilities, they could be exploited for social engineering or environmental reconnaissance by an attacker. It was recommended to strengthen error messages and apply sanitization in server responses [5], [15].

These tests were essential to reinforce the security of the tool and ensure its readiness against common attacks, complying with penetration testing best practices described in frameworks such as NIST and OWASP [5], [9].

The final validation phase represented a key moment in the SECUREISO development cycle, as it allowed the consolidation of the tool based on direct user feedback. This feedback was obtained through functional testing and semi-structured interviews that captured qualitative perceptions of the tool's use in simulated audit scenarios [20].

Among the most frequent comments were: the need to incorporate a step-by-step guide for new users, optimization of loading times in query modules, and improvement in the display of alert messages. These observations were prioritized and addressed in a final adjustment sprint, as suggested by the Scrum methodology in user-centered iterative processes [7].

The resulting final product integrated improvements to the interface, reorganization of menus, and inclusion of contextual aids, which refined the user experience in key tasks such as: asset management, risk linking, regulatory compliance, and generation of audit reports (see Figure 12).



Informes De Auditoria

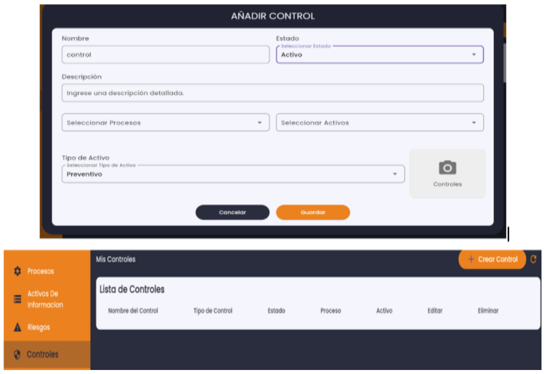
Visualiza todos los informes de tu organizacion

Lista de Informes

Nombre del Informe	Fecha	Responsable	Ver Informe	Eliminar
2024-08-13T01:31:09.241Z	2024-08-13T01:31:09.241Z	2024-08-13T01:31:09.241Z	ⓘ	🗑
2024-08-13T01:32:17.653Z	2024-08-13T01:32:17.653Z	2024-08-13T01:32:17.653Z	ⓘ	🗑
2024-08-13T01:33:05.854Z	2024-08-13T01:33:05.854Z	2024-08-13T01:33:05.854Z	ⓘ	🗑
2024-07-28T21:04:40.752Z	2024-07-28T21:04:40.752Z	2024-07-28T21:04:40.752Z	ⓘ	🗑

Fig. 12. *Audit report visualization.*
Source: *Owasp-zap.*

One of the most notable strengths at this stage was the flexibility of the tool's architecture, which allows security controls to be parameterized according to the type of organization or sector being audited. This configuration capability was positively valued by users and aligns with the recommendations from the initial systematic mapping conducted in this study [12], [14] (see Figure 13).



AÑADIR CONTROL

Nombre: control

Estado – Seleccionar Estado: Activo

Descripción: Ingrese una descripción detallada.

Seleccionar Procesos

Seleccionar Activos

Tipo de Activo – Seleccionar Tipo de Activo: Preventivo

Mis Controles

Lista de Controles

Nombre del Control	Tipo de Control	Estado	Proceso	Activo	Editar	Eliminar

Fig. 13. *Control configuration.*
Source: *Owasp-zap.*

Finally, this validation reaffirmed the achievement of the general objective of this work, which was to design an innovative digital tool that not only improves the efficiency of audit processes but also provides a secure, accessible, and adaptable experience for different organizational environments.

4. CONCLUSIONS

The results of this study demonstrated that the design of digital cybersecurity tools can go beyond simple task automation to become a comprehensive strategy for supporting information security governance. The developed proposal, SECUREISO, showed that it is possible to structure accessible, modular, and secure solutions that contribute to regulatory compliance without overlooking user experience and organizational adaptability.

One of the most valuable lessons learned from this process was the confirmation that the rigidity of standards such as ISO/IEC 27001 can be overcome through customizable software components that adhere to regulatory logic without imposing technical barriers on organizations, especially those with limited resources. This perspective aligns with studies analyzing the adoption difficulties of the standard in university or educational environments, where technical specialization is usually low [17].

From a critical perspective, the research also reveals that traditional audit models, based on static formats such as spreadsheets or printed checklists, are being surpassed by dynamic systems that allow real-time risk visualization, integrated evidence recording, and the construction of auditable compliance histories. This transition was acknowledged by participating users, who highlighted the usefulness of the reporting module as a strong point of the system.

In terms of research projection, an underexplored area is the correlation between organizational maturity and the efficient use of tools like SECUREISO. This opens the possibility of designing digital maturity indicators linked to standard implementation metrics, a line of analysis partially addressed in works such as those by Lara and Corella [16].

At the technical level, the need to scale toward distributed architectures and compatibility with risk management APIs or other cybersecurity standards such as NIST [5] or COBIT [2] represents a concrete evolution opportunity for the system. The future implementation of predictive dashboards, intelligent alerts, and synchronization with consolidated asset management platforms would establish a more robust ecosystem for decision-making.

Finally, this work invites reflection on the role of the researcher as an integrator of technical, regulatory, and pedagogical knowledge. Designing a secure tool is not just a programming task, but an exercise in synthesizing regulation, usability, and a strategic vision of security. SECUREISO is the result of this convergence of knowledge and is proposed not only as a functional product but also as a starting point for new academic, business, or institutional initiatives in the field of information security management.

ACKNOWLEDGMENTS

Thanks to the University of Cauca, especially the GTI research group, the Institución Universitaria Colegio Mayor del Cauca, and the University of Antioquia and its In2lab group for providing the resources and support for the development of this proposal.

REFERENCES

[1] ISO/IEC 27001:2022. “Information security, cybersecurity and privacy protection — Information security management systems — Requirements.” International Organization for Standardization, 2022.

[2] ISACA, “COBIT 2019 Framework: Introduction and Methodology.” ISACA, 2019.

[3] A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, 7ma edición, Kogan Page, 2020.

[4] R. Arévalo, J. Bayona y D. Bautista, “Aplicación de herramientas para el análisis de sistemas de información usando la norma ISO/IEC 27001:2005,” Revista Tecnura, vol. 19, no. 46, pp. 77–85, 2015.

[5] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” National Institute of Standards and Technology, 2018.

[6] Organización Internacional de Normalización, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, ISO, 2022.

[7] K. Schwaber y J. Sutherland, “The Scrum Guide,” Scrum.org, 2020. [Online]. Available: https://www.scrumguides.org

[8] F. Davis, “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989.

[9] S. AlGhamdi, K. T. Win, y E. Vlahu-Gjorgievska, «Information security governance challenges and critical success factors: Systematic review», Computers & Security, vol. 99, p. 102030, dic. 2020, doi: 10.1016/j.cose.2020.102030.

[10] M. A. Arévalo Álvarez and D. A. . Hernández Ladino, “Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense”, Cuad. Investig. Semilleros Andin., no. 14, Dec. 2021, doi: 10.33132/26196301.1950.

[11] M. M. M. Macías, R. Macías, M. L. I. Navarrete y J. A. I. Navarrete, “Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática,” Rev. Científica Arbitrada Multidiscip. PENTACIENCIAS, vol. 5, no. 4, pp. 584–599, jun. 2023, doi: 10.59169/pentaciencias.v5i4.700

[12] L. E. Salinas Suárez, Análisis entre las normativas ISO/IEC 27001:2022 versus ISO/IEC 27001:2013 e implementación de los nuevos controles en un sistema de gestión, en entidades financieras, desarrollo de software y una empresa de servicios de infraestructura de TI, Trabajo Fin de Máster, Univ. de Alcalá, 2023

[13] G. S. Babilonia Presentacion, “Beneficios de las normas ISO 27000”, HIGH TECH-ENG. J., vol. 3, n.º 2, pp. 86–88, septiembre de 2023. Accedido el 27 de julio de 2025. [En línea]. Disponible: https://doi.org/10.46363/high-tech.v3i2.4

[14] M. S. Herrera Olivares, A. J. Rada Martínez y I. E. Palacio Salcedo, “Framework gestión de la seguridad de la información para universidades”, Proyectos finales Pregrado en Ingeniería de Sist. y Computación, 2020. [En línea]. Disponible: https://manglar.uninorte.edu.co/handle/10584/8868?show=full

[15] J. L. Aguayo Morales, R. A. Ponce Bedoya y O. R. Rojas Cevallos, “Estudio de mejora en la seguridad de aplicaciones web y de aplicaciones móviles mediante el protocolo OpenID Connect opensource utilizado en IdentityServer4,” Trabajo de Titulación, Universidad Politécnica Salesiana, sede Quito, Ecuador, feb. 2020

[16] E. Lara y F. Corella, “Comparación de modelos tradicionales de seguridad de la información para centros de educación,” Tierra Infinita, 2018. doi: 10.32645/26028131.74

[17] D. L. Quijano, F. J. Iñiguez y D. A. Minda, “Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 en la Universidad Nacional de Loja,” Revista

Tierra Infinita, vol. 9, no. 1, pp. 84–93, 2023. Disponible en: https://revistasdigitales.upec.edu.ec/index.php/tierrainfinita/article/view/742/3028

[18] G. S. Babilonia Presentacion, “Beneficios de las normas ISO 27000”, HIGH TECH-ENG. J., vol. 3, n.º 2, pp. 86–88, septiembre de 2023. Accedido el 27 de julio de 2025. [En línea]. Disponible: https://doi.org/10.46363/high-tech.v3i2.4

[19] N. De la Cruz Lopez, D. M. Jerónimo Jiménez, W. B. López Rodríguez y R. M. Martínez Jiménez, “Impacto de la auditoría como una herramienta de control, para el mejoramiento de la empresa”, Publicaciones Investig., vol. 16, n.º 1, enero de 2022. Accedido el 27 de julio de 2025. [En línea]. Disponible: https://doi.org/10.22490/25394088.5769

[20] B. D. Morales Toapanta, “Construcción de una aplicación móvil para evaluar el desempeño docente de la Universidad Politécnica Salesiana”, Trabajo de grado, Univ. Politec. Sales. Sede Quito, Quito, 2021. Accedido el 1 de julio de 2024. [En línea]. Disponible: https://dspace.ups.edu.ec/bitstream/123456789/26782/1/TTS1621.pdf