ISSN: 1692-7257 - Volumen 2 – Número 46 - 2025

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Digital Object Identifier: 10.24054/rcta.v2i46.4111

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

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

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.*

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

Recibido: *24 abril 2025.* ***Aceptado:*** *03 julio 2025.* ***Publicado:*** *09 agosto 2025.*

Cómo citar: *S. Buesaco, A. Alcaraz Gaviria, J. J. Caiza Narváez, K. Marceles Villalba, y S. Amador Donado, «Herramienta digital para optimizar auditorías basadas en el estándar ISO/IEC 27001:2022», RCTA, vol. 2, n.º 46, pp. 209–216, ago. 2025. Recuperado de https://ojs.unipamplona.edu.co/index.php/rcta/article/view/4111*

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.

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.

1. INTRODUCCIÓN

En este momento, la información es esencial para garantizar la continuidad, confianza y sostenibilidad en las organizaciones, incluidas las empresariales y gubernamentales. Para las naciones de Europa y Latinoamérica, la adopción de estándares internacionales, como el ISO/IEC 27001, ha tenido un incremento notable debido al eficiente sistema que ofrece en la creación y administración de sistemas de gestión de la información, permitiendo proteger los activos digitales, mitigar riesgos y cumplir con marcos regulatorios exigentes [1], [2], [10].

Sin embargo, la implantación de este estándar aún representa significativos desafíos derivados del alto nivel de complejidad técnica, de las dificultades de adaptación a contextos específicos, y del carácter manual de muchos procesos de auditoría, los cuales suelen ser lentos, costosos y proclives al error, lo que afecta directamente la eficacia del sistema de gestión de seguridad de la información [3], [4], [11]. Tales problemáticas justifican la necesidad de un avance digital innovador que permita automatizar los procesos asociados a la evaluación y puesta en práctica del estándar ISO/IEC 27001:2022. Diversos estudios han demostrado que la utilización de tecnologías emergentes e inteligencia de negocios aporta mejoras sustanciales a los procesos de seguridad, almacenamiento de información y análisis de riesgos, proporcionando una visión más integral y precisa del estado real de la seguridad en las organizaciones [5], [6], [9], [18].

En este sentido, el propósito general de esta propuesta se centró en desarrollar una herramienta digital que, a través de un marco metodológico de desarrollo seguro, optimice los procesos de implementación del estándar ISO/IEC 27001. La herramienta propuesta busca no solo acelerar y automatizar el trabajo de auditoría, sino también enfrentar amenazas como accesos no autorizados en entornos web y móviles, además de mejorar la identificación, priorización y tratamiento del riesgo [19].

Para su desarrollo, se utilizó la metodología ágil Scrum, ampliamente empleada en proyectos tecnológicos que requieren adaptabilidad, iteración continua y entregas incrementales [7].

Cabe resaltar que una implementación efectiva de una herramienta digital basada en la norma ISO/IEC 27001 puede representar una ventaja competitiva clave, al permitir a las organizaciones adoptar una gestión más robusta, eficiente y resiliente de su ciberseguridad en un ecosistema cada vez más complejo y dinámico.

Este artículo se encuentra estructurado de la siguiente forma: en la sección dos se presenta la estructura metodológica, en la tercera sección los resultados obtenidos y en la cuarta sección conclusiones donde se encuentra la propuesta de trabajos futuros y es un espacio de discusión y aporte del autor.

2. METODOLOGÍA

El presente estudio se desarrolló con un enfoque metodológico de tipo aplicado con diseño tecnológico, orientado a resolver un problema práctico mediante la creación de una solución digital fundamentada en estándares internacionales como la norma ISO/IEC 27001:2022 [1]. La metodología empleada fue ágil, utilizando el marco de trabajo Scrum como eje para la planificación, desarrollo, evaluación y validación de la herramienta [7].

El proceso de diseño y construcción se estructuró en cuatro fases:

Fase de planeación: En esta fase se definieron los requisitos funcionales y no funcionales de la herramienta, y se estructuraron las historias de usuario. Además, se estableció una visión clara de los entregables y organización del backlog del producto [7].

Fase de desarrollo iterativo: Se ejecutaron múltiples sprints de dos semanas, durante los cuales se diseñaron e implementaron los módulos de la herramienta. Se emplearon tecnologías como Flutter para el frontend, Node.js para el backend, y PostgreSQL como sistema gestor de bases de datos. La arquitectura técnica adoptada fue Modelo-Vista-Controlador (MVC), lo que garantizó la modularidad, mantenibilidad y escalabilidad del sistema.

Fase de evaluación y pruebas: Se llevaron a cabo pruebas automatizadas de seguridad con la herramienta OWASP ZAP, identificando vulnerabilidades comunes como inyecciones y problemas de autenticación, en línea con los controles exigidos por la norma ISO/IEC 27002:2022 [6]. Para la evaluación de la aceptación tecnológica por parte de los usuarios finales, se utilizó el Modelo de Aceptación Tecnológica (TAM) propuesto por Davis [8], permitiendo medir

la percepción de utilidad, facilidad de uso y disposición para adoptar la herramienta.

Fase de validación final: Se integraron observaciones derivadas de la experiencia de los usuarios, se desarrolló una prueba de aceptación funcional y se documentaron los hallazgos. Esta fase concluyó con recomendaciones prácticas para mejorar y escalar la solución, teniendo en cuenta entornos organizacionales reales.

Es importante resaltar, los elementos diferenciadores del enfoque metodológico:

- **Alineación normativa**: La herramienta fue desarrollada considerando de manera explícita los nuevos controles definidos en la versión 2022 de la **ISO/IEC 27001**, lo cual permitió integrar aspectos actualizados de seguridad de la información en su arquitectura y funcionalidades [1], [6], [12].
- **Metodología híbrida**: Se combinó el enfoque ágil **Scrum** con técnicas de evaluación cuantitativa y cualitativa, lo que aseguró una iteración continua en el desarrollo y una validación empírica basada en evidencia [7], [8].
- **Seguridad desde el diseño**: Las pruebas de seguridad se integraron desde las primeras etapas del desarrollo, adoptando principios de **desarrollo seguro** y metodologías de prueba ampliamente reconocidas en la industria [11].
- **Validación empírica**: Se aplicaron instrumentos estructurados basados en TAM para validar la usabilidad, efectividad y eficiencia de la herramienta en contextos reales, permitiendo su mejora y adaptación continua [8], [20].

3. RESULTADOS

La evaluación de la herramienta digital desarrollada permitió validar su funcionalidad, seguridad y percepción por parte de los usuarios. A continuación, se presentan los hallazgos obtenidos en las fases descritas previamente.

Durante la fase de desarrollo, se construyó una herramienta modular con una interfaz limpia e intuitiva, desarrollada en Flutter, y basada en el modelo MVC. Se integraron funcionalidades clave como la gestión de controles, auditoría automatizada, generación de informes y análisis del cumplimiento de los requisitos definidos por la norma ISO/IEC 27001:2022 [1]. Este enfoque técnico permitió una mayor escalabilidad y mantenibilidad de la solución, alineándose con las buenas prácticas de desarrollo seguro propuestas en [7], [15].

En la Figura 1, se presenta un enfoque de cada una de las fases de evolución del desarrollo de la aplicación.

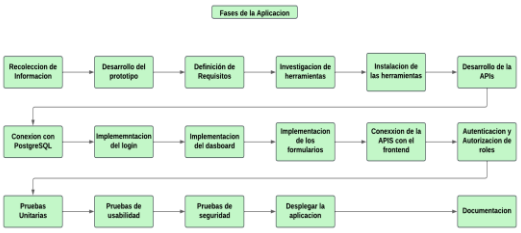

Fig. 1. *Diagrama fases de evolución de la aplicación.*
Fuente: *elaboración propia.*

Dado a lo anterior, se obtuvo una herramienta el cual fue estructurandose basado en un desarrollo iterativo e incremental ver figuras siguientes.

Fig. 2. *Imagen de Inicio de sesión.*

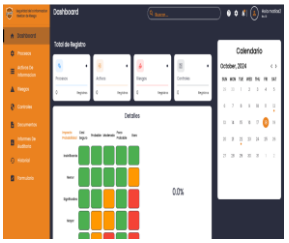

Fig. 3. *Versión final del sistema de gestión de riesgos, con la matriz de impacto.*

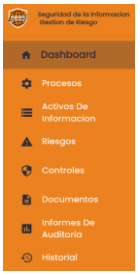

Fig. 4 *Funciones Dashboard.*

Fuente: *elaboración propia.*

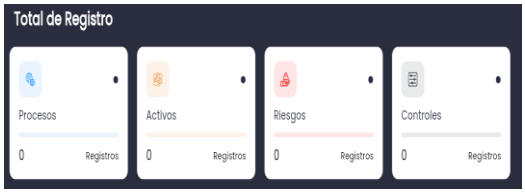

Fig. 5. *Imagen de Total Registro*
Fuente: *elaboración propia.*

En la fase de evaluación y pruebas, se realizaron análisis de seguridad utilizando OWASP ZAP. Como resultado, se identificaron y mitigaron vulnerabilidades relacionadas con cabeceras de seguridad ausentes, sugerencias de mejora en el uso de tokens y advertencias sobre exposición de información sensible [11], [15]. Estas pruebas incluyeron técnicas como *spidering* e *input fuzzing* sobre los formularios de frontend y backend. Los hallazgos permitieron reforzar los mecanismos de autenticación y autorización de la herramienta, en concordancia con lineamientos establecidos en estudios previos [5], [13].

La implementación de pruebas desde etapas tempranas se basó en recomendaciones de seguridad en el ciclo de vida del software. En ese mismo sentido es importante mencionar que el proceso de evaluación de la herramienta digital SECUREISO se centró en su eficiencia y efectividad en el marco de la norma ISO/IEC 27001:2022 [1]. La eficiencia fue entendida como el uso racional de los recursos, minimizando tiempo y esfuerzo; mientras que la efectividad se relacionó con el cumplimiento exitoso de los objetivos de seguridad establecidos en la norma.

Para esta evaluación se empleó el Modelo de Aceptación de Tecnología (TAM), reconocido por medir la percepción de los usuarios frente a la utilidad y facilidad de uso de soluciones tecnológicas [8]. El estudio se aplicó en contextos organizacionales que buscan implementar sistemas de gestión de seguridad de la información más ágiles y seguros con una muestra de 5 usuarios asumiendo rol desde auditor y otros como empresa [20].

Se elaboró un cuestionario con 14 preguntas: nueve enfocadas en la efectividad (como el cumplimiento de los requisitos de la norma y la reducción del tiempo de implementación), y cinco en la eficiencia (como la organización de los controles y la gestión clara de la información). Las preguntas abordaron distintos niveles de experiencia y buscaban evaluar aspectos clave como facilidad de navegación, practicidad y claridad en la aplicación de los controles.

Los resultados obtenidos reflejaron una percepción altamente positiva, en cuanto a efectividad, el 97.5% de los usuarios consideró que la herramienta facilita el cumplimiento de los requisitos de la norma y prefieren su uso frente a métodos tradicionales como hojas de cálculo [12] ver figura 6.

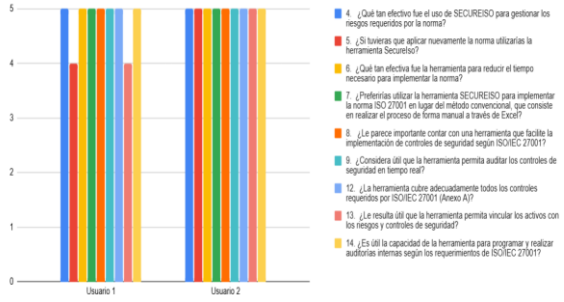

Fig. 6. *Categorización de preguntas efectividad.*
Fuente: *elaboración propia.*

Respecto a la eficiencia, la herramienta obtuvo una valoración promedio del 89%, destacándose su facilidad de navegación, aunque con oportunidades de mejora en la claridad de algunos controles [14] ver figura 7.

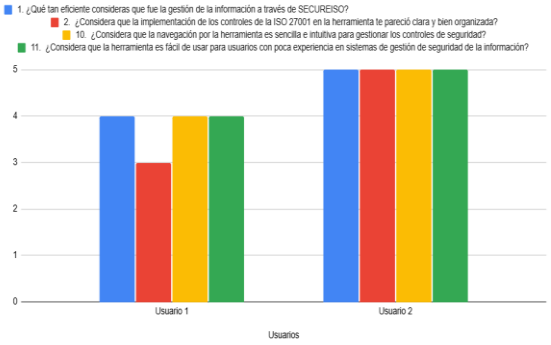

Fig. 7. *Categorización de preguntas eficiencia.*
Fuente: *elaboración propia.*

Estas métricas evidencian que SECUREISO logra optimizar el proceso de implementación del estándar ISO/IEC 27001, ofreciendo una experiencia intuitiva y accesible para diversos perfiles de usuario. Además, el análisis TAM permitió establecer correlaciones entre la utilidad percibida y los niveles de aceptación, validando que la herramienta no solo cumple su propósito funcional, sino que también facilita su adopción en escenarios reales [8], [20].

Las pruebas de seguridad realizadas sobre la herramienta SECUREISO utilizaron OWASP ZAP como herramienta principal para identificar vulnerabilidades tanto en el frontend como en el backend del sistema. Estas pruebas incluyeron ataques automatizados como spidering y fuzzing [15]. Durante el ataque de spidering al frontend, se detectaron riesgos de inyección (por ejemplo, SQL) que podrían ser explotados para manipular o extraer datos. Aunque estos riesgos se clasificaron como de nivel medio, se implementaron mejoras en las validaciones de entradas para reducir la exposición ver figura 8.

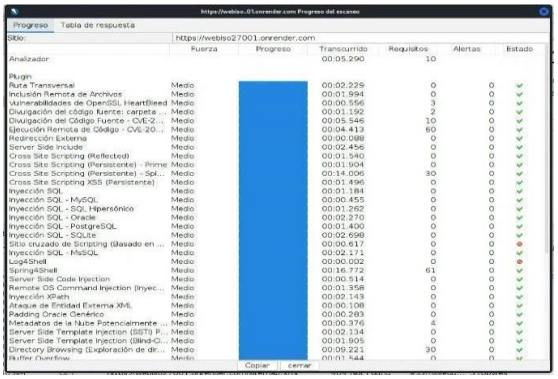

Fig. 8. *Resultados ataque spidering Front-end.*
Fuente*: Owasp-zap.*

Adicionalmente, se analizó la gráfica de respuestas por segundo ante múltiples solicitudes, donde se observaron picos que podrían representar una carga significativa en caso de un ataque de denegación de servicio. Esto reveló oportunidades de optimización en la capacidad de respuesta del servidor, tal como recomiendan estándares de pruebas de estrés para aplicaciones seguras [5], [13], ver figura 9.

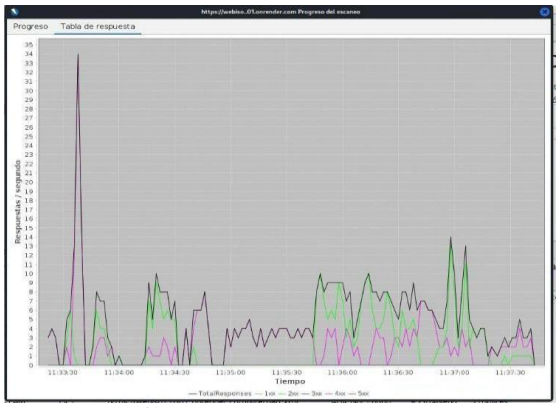

Fig. 9. *Gráfica tabla de respuesta - ataque spidering.*
Fuente*: Owasp-zap.*

En el backend, el ataque spidering reveló vulnerabilidades críticas como Ruta Transversal e Inyección SQL, que podrían permitir acceso no autorizado a archivos o manipulación de datos sensibles. Estas vulnerabilidades fueron priorizadas en el plan de mitigación de riesgos, en coherencia con las recomendaciones de seguridad de la norma ISO/IEC 27001:2022 [1], [15], ver figura 10.

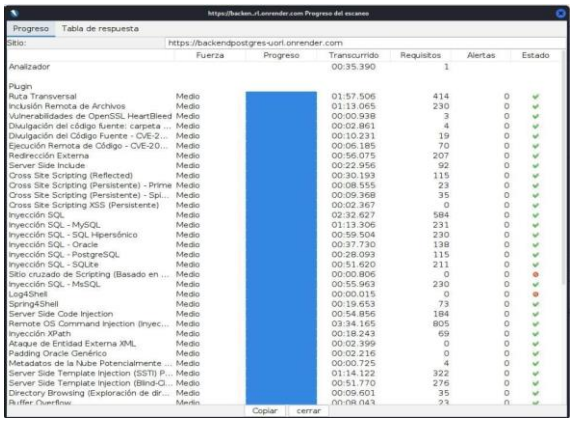

Fig. 10. *Resultados ataque spidering Backend.*
Fuente*: Owasp-zap.*

También se analizó la respuesta del servidor backend durante la simulación de carga y escaneo masivo. Se identificaron errores 500 y 403 en momentos de alta concurrencia, lo que sugiere la necesidad de ajustes en la lógica de manejo de sesiones y en los mecanismos internos de validación [9], [11], ver figura 11.

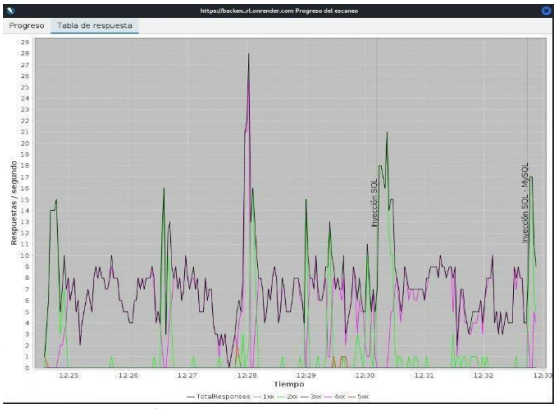

Fig. 11. *Gráfica tabla de respuesta - ataque spidering.*
Fuente*: Owasp-zap.*

Además, se aplicó un ataque *fuzzing* que reveló riesgos informativos relacionados con la exposición de mensajes técnicos sobre sesiones y errores de autenticación. Estos detalles, aunque no constituyen vulnerabilidades críticas, pueden ser aprovechados para ingeniería social o reconocimiento del entorno por parte de un atacante. Se recomendó entonces fortalecer los mensajes de error y aplicar sanitización en las respuestas del servidor [5], [15]. Estas pruebas fueron esenciales para reforzar la seguridad de la herramienta y garantizar su preparación ante ataques comunes, cumpliendo con las mejores prácticas de prueba de penetración descritas en marcos como NIST y OWASP [5], [9].

La fase de validación final representó un momento clave en el ciclo de desarrollo de SECUREISO, ya que permitió consolidar la herramienta a partir de la retroalimentación directa de los usuarios. Esta retroalimentación se obtuvo mediante pruebas funcionales y entrevistas semiestructuradas que capturaron percepciones cualitativas sobre el uso de la herramienta en escenarios simulados de auditoría [20].

Entre los comentarios más frecuentes estuvieron: la necesidad de incorporar una guía paso a paso para nuevos usuarios, la optimización de los tiempos de carga en los módulos de consulta, y la mejora en la visualización de mensajes de alerta. Estas observaciones fueron priorizadas y resueltas en un último sprint de ajustes, tal como lo sugiere la metodología Scrum en procesos iterativos centrados en el usuario [7].

El producto final resultante integró mejoras en la interfaz, reorganización de menús e inclusión de ayudas contextuales, lo que permitió refinar la experiencia del usuario en tareas clave como: la gestión de activos, la vinculación de riesgos, el

cumplimiento normativo y la generación de informes de auditoría, ver figura 12.

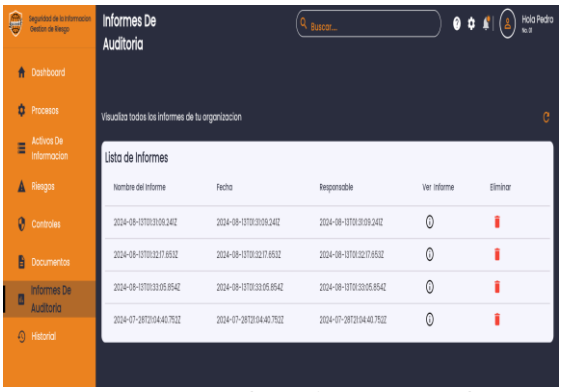

Fig. 12. *Visualización de informes de auditoría.*
Fuente*: Owasp-zap.*

Una de las fortalezas más destacadas en esta etapa fue la flexibilidad de la arquitectura de la herramienta, que permite parametrizar los controles de seguridad según el tipo de organización o sector auditado. Esta capacidad de configuración fue valorada positivamente por los usuarios y coincide con las recomendaciones del mapeo sistemático inicial realizado en este estudio [12], [14], ver figura 13.

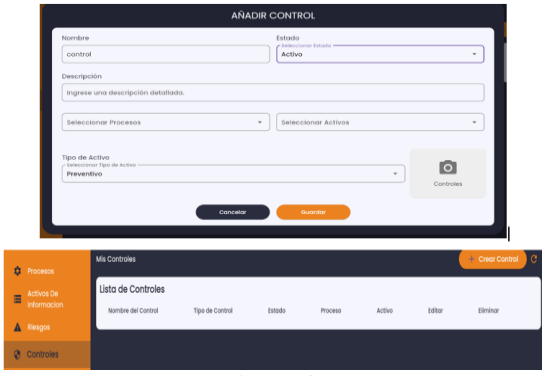

Fig. 13. *Configuración de control.*
Fuente*: Owasp-zap.*

Finalmente, esta validación reafirmó el cumplimiento del objetivo general de este trabajo que fue diseñar una herramienta digital innovadora que no solo mejore la eficiencia en los procesos de auditoría, sino que también ofrezca una experiencia segura, accesible y adaptable para distintos entornos organizacionales.

4. CONCLUSION

Los resultados de este estudio permitieron evidenciar que el diseño de herramientas digitales en ciberseguridad puede ir más allá de la simple automatización de tareas, al convertirse en una estrategia integral de apoyo a la gobernanza de la seguridad de la información. La propuesta desarrollada, SECUREISO, demostró que es posible estructurar soluciones accesibles, modulares y seguras que contribuyan al cumplimiento normativo sin perder de vista la experiencia de usuario y la adaptabilidad organizacional.

Uno de los aprendizajes más valiosos de este proceso fue la constatación de que la rigidez de las normas, como ISO/IEC 27001, puede superarse mediante componentes de software parametrizables que respeten la lógica normativa sin imponer barreras técnicas a las organizaciones, especialmente en sectores con recursos limitados. Esta visión coincide con lo planteado por estudios que analizan las dificultades de adopción del estándar en entornos universitarios o educativos, donde el nivel de especialización técnica suele ser bajo [17].

Desde una mirada crítica, la investigación también revela que los modelos tradicionales de auditoría, anclados en formatos estáticos como hojas de cálculo o listas de verificación impresas, están siendo superados por sistemas dinámicos que permiten visualizar el riesgo en tiempo real, registrar evidencia de forma integrada y construir historiales de cumplimiento auditables. Esta transición fue reconocida por los usuarios participantes, quienes destacaron la utilidad del módulo de reportes como punto fuerte del sistema.
En cuanto a proyección investigativa, un espacio aún poco explorado es la correlación entre la madurez organizacional y la eficiencia del uso de herramientas como SECUREISO. Esto abre la posibilidad de diseñar indicadores de madurez digital vinculados a métricas de implementación del estándar, línea de análisis abordada parcialmente en trabajos como los de Lara y Corella [16].

A nivel técnico, la necesidad de escalar hacia arquitecturas distribuidas y compatibles con APIs de gestión de riesgos u otras normas de ciberseguridad como NIST [5] o COBIT [2] representa una oportunidad concreta de evolución para el sistema. La implementación futura de dashboards predictivos, alertas inteligentes y sincronización con plataformas de gestión de activos consolidaría un ecosistema más robusto para la toma de decisiones.
Finalmente, este trabajo permite reflexionar sobre el rol del investigador como integrador de conocimiento técnico, normativo y pedagógico. Diseñar una herramienta segura no es solo una tarea de programación, sino un ejercicio de síntesis entre regulación, usabilidad y visión estratégica de la seguridad. SECUREISO es el resultado de ese cruce

de saberes, y como tal, se propone no solo como un producto funcional, sino como un punto de partida para nuevas iniciativas académicas, empresariales o institucionales en el ámbito de la gestión de la seguridad de la información.

RECONOCIMIENTO

Gracias a la Universidad del Cauca, especialmente al grupo de investigación GTI, a la Institución Universitaria Colegio Mayor del Cauca, y a la Universidad de Antioquia y su grupo In2lab por proporcionar los recursos y el apoyo para el desarrollo de esta propuesta.

REFERENCIAS

[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