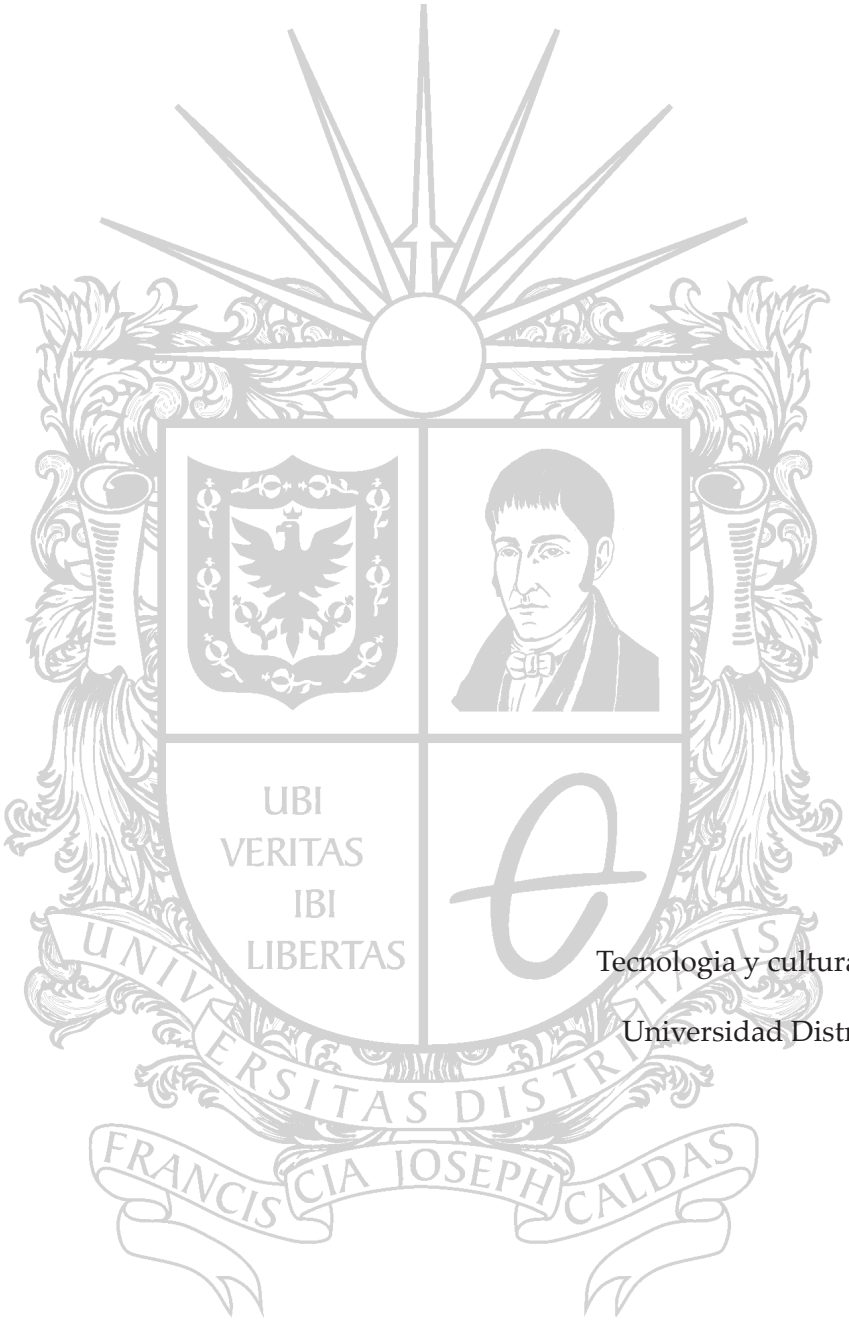

Tecnura

Tecnologia y cultura, afirmando el conocimiento

Universidad Distrital Francisco Jose de Caldas
Facultad Tecnologica

Volumen 30 - Numero 88
Abril - Junio de 2026

p-ISSN: 0123-921X
e-ISSN: 2248-7638

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista TECNURA
Tecnología y cultura, afirmando el conocimiento
Universidad Distrital Francisco José de Caldas
Facultad Tecnológica

Volumen 30 - Numero 88
Abril - Junio de 2026
p-ISSN: 0123-921X - e-ISSN: 2248-7638

COORDINACIÓN EDITORIAL

Fernando Piraquive
Oficina de Investigaciones
Universidad Distrital Francisco José de Caldas

DISEÑADORES

Andres Enciso
David Valero

CORRECTOR DE ESTILO EN INGLES

José Daniel Gutiérrez Mendoza

Tecnura
Abril - Junio de 2026

REVISTA TECNURA

La revista Tecnura es una publicacion institucional de la Facultad Tecnologica de la Universidad Distrital Francisco Jose de Caldas de caracter cientifico-tecnologico, arbitrada mediante un proceso de revision entre pares de doble ciego. La periodicidad de la conformacion de sus comites Cientifico y Editorial esta sujeta a la publicacion de articulos en revistas indexadas internacionalmente por parte de sus respectivos miembros.

PERIODICIDAD

Es una publicacion de caracter cientifico-tecnologico con periodicidad trimestral, que se publica los meses de enero, abril, julio y octubre. Su primer numero aparecio en el segundo semestre del ano 1997 y hasta la fecha ha mantenido su regularidad.

COBERTURA TEMATICA

Las areas tematicas de interes de la revista Tecnura estan enfocadas a todos los campos de la ingenieria, como la electronica, telecomunicaciones, electricidad, sistemas, industrial, mecanica, catastral, civil, ambiental, entre otras. Sin embargo, no se restringe unicamente a estas, tambien tienen cabida los temas de educacion y salud, siempre y cuando esten relacionados con la ingenieria. La revista publicara unicamente articulos de investigacion cientifica y tecnologica, de reflexion y de revision.

MISION

La revista Tecnura tiene como mision divulgar resultados de proyectos de investigacion realizados en el area de la ingenieria, a traves de la publicacion de articulos originales e ineditos, realizados por academicos y profesionales pertenecientes a instituciones nacionales o extranjeras del orden publico o privado.

PUBLICO OBJETIVO

La revista Tecnura esta dirigida a docentes, investigadores, estudiantes y profesionales interesados en la actualizacion permanente de sus conocimientos y el seguimiento de los procesos de investigacion cientifico-tecnologica, en el campo de la ingenieria.

INDEXACION

Tecnura es una publicacion de caracter academico indexada en los indices regionales publindex indexada y clasificada en categoria B, Scielo Colombia y Redalyc (Mexico); ademas de las siguientes bases bibliograficas: INSPEC del Institution of Engineering and Technology (Inglaterra), Fuente Academica Premier de EBSCO (Estados Unidos), CABI (Inglaterra), IndexCorpernicus (Polonia), Informe Academico de Gale Cengage Learning (Mexico), Periodica de la Universidad Nacional Autonoma de Mexico (Mexico), Oceanet (Espana) y Dialnet de la Universidad de la Rioja (Espana); tambien hace parte de los siguientes directorios: Sistema Regional de Informacion en Linea para Revistas Cientificas de America Latina, el Caribe, Espana y Portugal Latindex (Mexico); Indice Bibliografico Actualidad Iberoamericana (Chile), e-Revistas (Espana), DOAJ (Suecia), Ulrich de Proquest (Estados Unidos).

FORMA DE ADQUISICION

La revista Tecnura se puede adquirir a traves de canje o suscripcion en el portal de la de la revista.

REPRODUCCION

DIRECCION POSTAL

Enviar a Ph.D. Lely Adriana Luengas Contreras
Director y Editor Revista Tecnura
Sala de Revistas, Bloque 5, Oficina 305
Facultad Tecnologica
Universidad Distrital Francisco Jose de Caldas
Direccion: Cl. 68d Bis A Sur # 49 F - 70, Bogota
Telefono: 571–3239300
Bogota, D.C., Colombia
Correo electronico:
tecnura.ud@udistrital.edu.co
Tecnura en internet:
https://revistas.udistrital.edu.co/ojs/index.php/Tecnura

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista TECNURA
Tecnología y cultura, afirmando el conocimiento
Universidad Distrital Francisco José de Caldas
Facultad Tecnológica

Volumen 30 - Numero 88
Abril - Junio de 2026
p-ISSN: 0123-921X - e-ISSN: 2248-7638

EDITORIAL COORDINATION

Fernando Piraquive
Oficina de Investigaciones
Universidad Distrital Francisco José de Caldas

DESIGN

Andres Enciso
David Valero

STYLE CORRECTION IN ENGLISH

Jose Daniel Gutierrez Mendoza

Tecnura
April - June of 2026

TECNURA JOURNAL

La revista Tecnura es una publicacion institucional de la Facultad Tecnologica de la Universidad Distrital Francisco Jose de Caldas de caracter cientifico-tecnologico, arbitrada mediante un proceso de revision entre pares de doble ciego. La periodicidad de la conformacion de sus comites Cientifico y Editorial esta sujeta a la publicacion de articulos en revistas indexadas internacionalmente por parte de sus respectivos miembros.

PERIODICITY

Es una publicacion de caracter cientifico-tecnologico con periodicidad trimestral, que se publica los meses de enero, abril, julio y octubre. Su primer numero aparecio en el segundo semestre del ano 1997 y hasta la fecha ha mantenido su regularidad.

THEMATIC COVERAGE

Las areas tematicas de interes de la revista Tecnura estan enfocadas a todos los campos de la ingenieria, como la electronica, telecomunicaciones, electricidad, sistemas, industrial, mecanica, catastral, civil, ambiental, entre otras. Sin embargo, no se restringe unicamente a estas, tambien tienen cabida los temas de educacion y salud, siempre y cuando esten relacionados con la ingenieria. La revista publicara unicamente articulos de investigacion cientifica y tecnologica, de reflexion y de revision.

MISSION

La revista Tecnura tiene como mision divulgar resultados de proyectos de investigacion realizados en el area de la ingenieria, a traves de la publicacion de articulos originales e ineditos, realizados por academicos y profesionales pertenecientes a instituciones nacionales o extranjeras del orden publico o privado.

TARGET AUDIENCE

La revista Tecnura esta dirigida a docentes, investigadores, estudiantes y profesionales interesados en la actualizacion permanente de sus conocimientos y el seguimiento de los procesos de investigacion cientifico-tecnologica, en el campo de la ingenieria.

INDEXING

Tecnura es una publicacion de caracter academico indexada en los indices regionales publindex indexada y clasificada en categoria B, Scielo Colombia y Redalyc (Mexico); ademas de las siguientes bases bibliograficas: INSPEC del Institution of Engineering and Technology (Inglaterra), Fuente Academica Premier de EBSCO (Estados Unidos), CABI (Inglaterra), IndexCorpernicus (Polonia), Informe Academico de Gale Cengage Learning (Mexico), Periodica de la Universidad Nacional Autonoma de Mexico (Mexico), Oceanet (Espana) y Dialnet de la Universidad de la Rioja (Espana); tambien hace parte de los siguientes directorios: Sistema Regional de Informacion en Linea para Revistas Cientificas de America Latina, el Caribe, Espana y Portugal Latindex (Mexico); Indice Bibliografico Actualidad Iberoamericana (Chile), e-Revistas (Espana), DOAJ (Suecia), Ulrich de Proquest (Estados Unidos).

FORM OF ACQUISITION

La revista Tecnura se puede adquirir a traves de canje o suscripcion en el portal de la de la revista.

REPRODUCTION

POSTAL ADDRESS

Enviar a Ph.D. Lely Adriana Luengas Contreras
Director y Editor Revista Tecnura
Sala de Revistas, Bloque 5, Oficina 305
Facultad Tecnologica
Universidad Distrital Francisco Jose de Caldas
Direccion: Cl. 68d Bis A Sur # 49 F - 70, Bogota
Telefono: 571–3239300
Bogota, D.C., Colombia
Correo electronico:
tecnura.ud@udistrital.edu.co
Tecnura en internet:
https://revistas.udistrital.edu.co/ojs/index.php/Tecnura

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Declaración de ética y buenas Prácticas

https://revistas.udistrital.edu.co/index.php/Tecnura/about

El comité editorial de la revista **Tecnura** está comprometido con altos estándares de ética y buenas prácticas en la difusión y transferencia del conocimiento, para garantizar el rigor y la calidad científica. Es por ello que ha adoptado como referencia el Código de Conducta que, para editores de revistas científicas, ha establecido el Comité de Ética de Publicaciones (COPE: Committee on Publication Ethics) dentro de los cuales se destaca:

Obligaciones y responsabilidades generales del equipo editorial

En su calidad de máximos responsables de la revista, el comité y el equipo editorial de Tecnura se comprometen a:

- Aunar esfuerzos para satisfacer las necesidades de los lectores y autores.
- Propender por el mejoramiento continuo de la revista.
- Asegurar la calidad del material que se publica.
- Velar por la libertad de expresión.
- Mantener la integridad académica de su contenido.
- Impedir que intereses comerciales comprometan los criterios intelectuales.
- Publicar correcciones, aclaraciones, retractaciones y disculpas cuando sea necesario.

Relaciones con los lectores

Los lectores estarán informados acerca de quién ha financiado la investigación y sobre su papel en la investigación.

Relaciones con los autores

Tecnura se compromete a asegurar la calidad del material que publica, informando sobre los objetivos y normas de la revista. Las decisiones de los editores para aceptar o rechazar un documento para su publicación se basan únicamente en la relevancia del trabajo, su originalidad y la pertinencia del estudio con relación a la línea editorial de la revista. La revista incluye una descripción de los procesos seguidos en la evaluación por pares de cada trabajo recibido. Cuenta con una guía de autores en la que se presenta esta información. Dicha guía se actualiza regularmente y contiene un vínculo a la presente declaración ética. Se reconoce el derecho de los autores a apelar las decisiones editoriales. Los editores no modificarán su decisión en la aceptación de envíos, a menos que se detecten irregularidades o situaciones extraordinarias. Cualquier cambio en los miembros del equipo editorial no afectará las decisiones ya tomadas, salvo casos excepcionales en los que confluyan graves circunstancias.

Relaciones con los evaluadores

Tecnura pone a disposición de los evaluadores una guía acerca de lo que se espera de ellos. La identidad de los evaluadores se encuentra en todo momento protegida, garantizando su anonimato.

Proceso de evaluación por pares

Tecnura garantiza que el material remitido para su publicación será considerado como materia reservada y confidencial mientras que se evalúa (doble ciego).

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Declaración de ética y buenas Prácticas

https://revistas.udistrital.edu.co/index.php/Tecnura/about

Reclamaciones

Tecnura se compromete responder con rapidez a las quejas recibidas y a velar para que los demandantes insatisfechos puedan tramitar todas sus quejas. En cualquier caso, si los interesados no consiguen satisfacer sus reclamaciones, se considera que están en su derecho de elevar sus protestas a otras instancias.

Fomento de la integridad académica

Tecnura asegura que el material que publica se ajusta a las normas éticas internacionalmente aceptadas.

Protección de datos individuales

Tecnura garantiza la confidencialidad de la información individual (por ejemplo, de los profesores y/o alumnos participantes como colaboradores o sujetos de estudio en las investigaciones presentadas).

Seguimiento de malas prácticas

Tecnura asume su obligación para actuar en consecuencia en caso de sospecha de malas prácticas o conductas inadecuadas. Esta obligación se extiende tanto a los documentos publicados como a los no publicados. Los editores no sólo rechazarán los manuscritos que planteen dudas sobre una posible mala conducta, sino que se consideran éticamente obligados a denunciar los supuestos casos de mala conducta. Desde la revista se realizarán todos los esfuerzos razonables para asegurar que los trabajos sometidos a evaluación sean rigurosos y éticamente adecuados.

Integridad y rigor académico

Cada vez que se tenga constancia de que algún trabajo publicado contiene inexactitudes importantes, declaraciones engañosas o distorsionadas, debe ser corregido de forma inmediata.
En caso de detectarse algún trabajo cuyo contenido sea fraudulento, será retirado tan pronto como se conozca, informando inmediatamente tanto a los lectores como a los sistemas de indexación.
Se consideran prácticas inadmisibles, y como tal se denunciarán las siguientes: el envío simultáneo de un mismo trabajo a varias revistas, la publicación duplicada o con cambios irrelevantes o parafraseo del mismo trabajo, o la fragmentación artificial de un trabajo en varios artículos.

Relaciones con los propietarios y editores de revistas

La relación entre editores, editoriales y propietarios estará sujeta al principio de independencia editorial. **Tecnura** garantizará siempre que los artículos se publiquen con base en su calidad e idoneidad para los lectores, y no con vistas a un beneficio económico o político. En este sentido, el hecho de que la revista no se rija por intereses económicos, y defienda el ideal de libre acceso al conocimiento universal y gratuito, facilita dicha independencia.

Conflicto de intereses

Tecnura establecerá los mecanismos necesarios para evitar o resolver los posibles conflictos de intereses entre autores, evaluadores y/o el propio equipo editorial.

Quejas/denuncias

Cualquier autor, lector, evaluador o editor puede remitir sus quejas a los organismos competentes

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Code of ethics and good practice

https://revistas.udistrital.edu.co/index.php/Tecnura/about

The editorial board of Tecnura journal is committed to ethics high standards and good practice for knowledge dissemination and transfer, in order to ensure rigour and scientific quality. That is why it has taken as reference the Code of Conduct, which has been established by the Committee on Publication Ethics (COPE) for scientific journal editors; outlining the following:

General duties and responsibilities of the editorial board

As most responsible for the journal, **Tecnura** committee and the editorial board are committed to:

- Joining efforts to meet the readers and authors' needs.
- Tending to the continuous improvement of the Journal.
- Ensuring quality of published material.
- Ensuring freedom of expression.
- Maintaining the academic integrity of their content.
- Prevent commercial interests compromise intellectual standards.
- Post corrections, clarifications, retractions and apologies when necessary.
- Relations with readers.
- Readers will be informed about who has funded re- search and their role in the research.

Relations with authors

Tecnura is committed to ensuring the quality of published material, informing the goals and standards of the journal. The decisions of publishers to accept or reject a paper for publication are based solely on the relevance of the work, originality and pertinence of the study with journal editorial line. The journal includes a description of the process for peer evaluation of each received work, and has an authors guide with this information. The guide is regularly updated and contains a link to this code of ethics. The journal recognizes the right of authors to appeal editorial decisions Publishers will not change their decision in accepting or rejecting articles, unless extraordinary circumstances or irregularities are detected. Any change in the editorial board members will not affect decisions already made, except for unusual cases where serious circumstances converge.

Relations with evaluators

Tecnura makes available to reviewers a guide to what is expected from them. Reviewers' identity is protected at all times, ensuring anonymity

Peer review process

Tecnura ensures that material submitted for publication will be considered private and confidential issue while being reviewed (double blind).

Claims

Tecnura is committed to respond quickly to complaints and ensure that dissatisfied claimant can process all complaints. In any case, if applicants fail to satisfy their claims, the journal considers that they have the right to raise their protests to other instances.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Code of ethics and good practice

https://revistas.udistrital.edu.co/index.php/Tecnura/about

Promoting Academic Integrity

Tecnura ensures that the published material conforms to internationally accepted ethical standards.

Protection of individual data

Tecnura guarantees the confidentiality of individual information (e.g. participant teachers and/or students as collaborators or subjects of study in the presented research).

Tracking malpractice

Tecnura accepts the obligation to act accordingly in case of suspected malpractice or misconduct. This obligation extends both to publish and unpublished documents. The editors not only reject manuscripts with doubts about possible misconduct, but they are considered ethically obligated to report suspected cases of misconduct. From the journal every reasonable effort is made to ensure that works submitted for evaluation are rigorous and ethically appropriate.

Integrity and academic rigour

Whenever evidence that a published work contains significant misstatements, misleading or distorted statements, it must be corrected immediately
In case of any work with fraudulent content is detected, it will be removed as soon as it is known, and immediately informing both readers and indexing systems.
Practices that are considered unacceptable and as such will be reported: simultaneous sending of the same work to various journals, duplicate publication with irrelevant changes or paraphrase of the same work, or the artificial fragmentation of a work in several articles.

Relations with owners and journal editors

The relation between editors, publishers and owners will be subject to the principle of editorial independence. **Tecnura** will ensure that articles are published based on their quality and suitability for readers, and not for an economic or political gain. In this sense, the fact that the journal is not governed by economic interests, and defends the ideal of universal and free access to knowledge, provides that independence.

Conflict of interest

Tecnura will establish the necessary mechanisms to avoid or resolve potential conflicts of interest between authors, reviewers and/or the editorial board itself.

Complaints / allegations

Any author, reader, reviewer or editor may refer their complaints to the competent authorities.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tabla de Contenidos

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tabla de Contenidos

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura
https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

EDITORIAL

NOTA DE LA EDITORA

Editorial del Volumen 30 - Numero 88, 2026

Las construcciones, las edificaciones y, en general, las obras civiles, las máquinas, las aplicaciones de software, la automatización de los procesos, es decir, lo tangible, lo que se ve, lo que se escucha, son lo que, durante muchas épocas, ha dado validez al desarrollo ingenieril. Pero ¿qué sucede con todo lo que hay detrás para llegar a estos desarrollos? La innovación aparece antes del surgimiento de un prototipo físico, puesto que incluye diseño, cálculos, simulaciones y, en el trasfondo, el conocimiento; con su apropiación, es lo que permite el avance de la tecnología. El intangible en investigación es lo requerido desde el inicio para poder alcanzar el desarrollo de todos esos elementos que tienen validez en ingeniería.

Para solventar las necesidades de la sociedad y dar soluciones concretas técnicamente sólidas, la investigación en ingeniería cada vez más está resaltando la importancia de los activos intangibles; cada vez se incluye con más fuerza el diseño conceptual, el modelado para predecir y optimizar el comportamiento del diseño y las maquetas, es decir, aquellos elementos abstractos, lógicos e intelectuales que, aunque no se pueden tocar, resultan indispensables para concebir, diseñar y materializar cualquier solución técnica u obra física. Pero no basta con tener estas premisas conceptuales: el conocimiento sobre ellos debe circular para poder ser entendido, adaptado y empleado.

En este contexto surge la democratización del conocimiento, como esa herramienta que se convierte en una condición de la calidad científica; hacer uso de constructivos teóricos; replicar una metodología; validar los hallazgos de investigaciones previas, es la verdadera razón del avance ingenieril.

El volumen 30, No. 88 de *Tecnura* (abril-junio de 2026) se ubica esencialmente en ese contorno decisivo: la obtención de metodologías diseñadas para dar respuesta a puntos críticos presentes en la sociedad, transfiriendo el conocimiento hacia situaciones con necesidades específicas, como el caso de la formación médica, las métricas de documentación de proyectos de software, la ciberseguridad en redes eléctricas y el diseño apropiado de mecanismos. Los artículos que integran este número demuestran que la apropiación del conocimiento para generar modelos es la garantía de que los sistemas físicos no fallen cuando se requieran y entren en operación.

Esta edición concentra la modelación matemática y la validación formal de eventos complejos, tal como se observa en el escrito *Modelado con Redes de Petri de un Laboratorio Teleoperado para entrenamiento en Ventilación Mecánica* donde los autores demuestran cómo la lógica de eventos discretos previene fallas

críticas de sincronización y bloqueos mutuos (*deadlocks*) en la teleoperación médica, transfiriendo seguridad en la formación de personal asistencial en escenarios donde el error de un sistema cuesta vidas. También se tiene el artículo *Análisis del Centro Instantáneo de Rotación de un Mecanismo de Seis Barras usando Coordenadas Nodale,* que aborda la cinemática predictiva para el diseño de hardware, enfocado en el análisis del centro instantáneo de rotación en mecanismos de seis barras utilizando coordenadas nodales, para redefinir la síntesis cinemática tradicional; al sustituir las aproximaciones geométricas clásicas por un modelo de coordenadas nodales de alta precisión, la investigación entrega un algoritmo aplicable al diseño predictivo de hardware, con aplicación desde sistemas de suspensión vehicular hasta prótesis biomecánicas, reduciendo drásticamente el costo computacional antes de pasar a la manufactura física. El trabajo *Oportunidades del Aprendizaje Automático Adversarial (AML) para fortalecer la ciberseguridad de la IA en el contexto colombiano* analiza la forma de hackear modelos predictivos locales mediante manipulación de datos y propone contra monitoreos específicos para blindar la toma de decisiones automatizada en entornos de alta incertidumbre; investigación de impacto en sectores que trabajan con datos sensibles, ya sean financieros y crediticios, privados, semiprivados o públicos. Los autores de *Evaluación manual de accesibilidad web: estudio de caso en portal de estudiantes de una universidad pública* realizaron una auditoría para medir la accesibilidad que se presenta en el portal web de estudiantes de la Universidad Veracruzana, demostrando que al contar con portales accesibles se mejora la usabilidad y se favorece la experiencia de usuario en general, incluyendo las personas con discapacidad; así mismo, que análisis de este tipo, al hacer uso de métodos automáticos, no siempre detectan todos los problemas, principalmente los vinculados con la experiencia del usuario. En *Métricas para la evaluación del formato de la documentación en proyectos de software ágil* se aborda el problema de la consolidación de la documentación que respalda los desarrollos, ya que una de las causas de riesgos en la producción de software es la deficiencia de un formato que no contempla métricas para la evaluación del usuario que incluyan indicadores de complejidad estructural; por ello proponen una arquitectura de cinco dimensiones con métricas para el formato, considerando legibilidad, concisión y claridad.

Adicionalmente, se incluyen dos revisiones bibliográficas que resaltan el tema de lo intangible como elemento imprescindible en ingeniería. En *Ciberseguridad cuántica en sistemas ciberfísicos e infraestructuras críticas* se reconoce que debido al avance en computación cuántica se ha incrementado la fragilidad de los sistemas hardware-software presentes en instalaciones estratégicas esenciales para el funcionamiento de una comunidad; de allí la necesidad de revisar y ajustar los esquemas actuales de criptografía, por ello se realizó una investigación documental que permitió caracterizar los estándares, marcos de trabajo y las vulnerabilidades emergentes encontradas en estudios científicos y se evidenció la carencia de medidas de control específicas frente a amenazas cuánticas, de tal modo que se propuso una hoja de ruta para la creación de modelos ontológicos que unifiquen la gestión de riesgos en esta era tecnológica. En una línea distinta, *Análisis de prácticas para reducir el consumo de energía en las pruebas de software: una revisión sistemática de la literatura* reúne la evidencia disponible sobre estrategias que disminuyen el gasto

energético durante las actividades de prueba y verificación, se demuestra que la calidad del software no solo depende de su funcionalidad o confiabilidad; también involucra decisiones de diseño que repercuten en el consumo de recursos y, en consecuencia, en la sostenibilidad de las infraestructuras digitales.

Los escritos que componen este número confluyen en un propósito franco y riguroso: darle el lugar que se merece a lo intangible, ya que un gran fragmento de los adelantos transformados hoy en día gracias a la ingeniería proviene de aquello que no siempre es visible. Modelos, métricas, algoritmos, protocolos, métodos de evaluación y formas de compartir conocimiento sostienen las soluciones que finalmente llegan a la sociedad. Formalizar esos elementos invisibles sigue siendo una condición indispensable para construir tecnologías útiles, confiables y perdurables.

El equipo editorial de Tecnura expresa su agradecimiento a los autores por confiar en la revista como espacio para divulgar sus investigaciones, a los evaluadores por el rigor y la dedicación con que fortalecen cada manuscrito, y a los lectores, cuya mirada crítica mantiene vivo el propósito esencial de la ciencia: contrastar, discutir y hacer avanzar el conocimiento. Gracias a todos por su tiempo, por exigir rigor a las publicaciones y por recordarnos que investigar solo tiene sentido si hay una comunidad dispuesta a transformar la realidad con ello.

Cordialmente

Ing. Lely A. Luengas-C., PhD
Editora
Universidad Distrital Francisco José de Caldas
laluengasc@udistrital.edu.co

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.23730

INVESTIGACIÓN

Analysis of the Instantaneous Center of Rotation of a Six-Bar Mechanism Using Nodal Coordinates

Análisis del Centro Instantáneo de Rotación de un Mecanismo de Seis Barras usando Coordenadas Nodales

Neider Nadid Romero N.[1], Gonzalo Moreno Contreras[2], Rafael Villalba González[3], Daniel Martins[4]

Fecha de Recepción: 14 de junio de 2025 **Fecha de Aceptación**: 2 de abril de 2026

Cómo citar: N.N. Romero N., G. Moreno Contreras, R.Villalba, D. Martins, «Analysis of the Instantaneous Center of Rotation of a Six-Bar Mechanism Using Nodal Coordinates», *Tecnura*, vol. 30, n.° 88, jun. 2026. 4–18. https://doi.org/10.14483/22487638.23730

Abstract

Objective: Knowledge of the instantaneous center associated with two bodies in a mechanism is important for both analy-sis and synthesis, because it can simplify velocity and acceleration analysis. Moreover, accurate determination of the instantaneous center position is a key requirement for synthesis in many practical applications. The purpose of this work is to propose an analytical method for calculating the instantaneous center of rotation of a floating link in a six-bar mechanism with respect to the fixed link.

Methodology: The proposed procedure consists of the following steps. First, the variables representing the mechanism dimensions are defined. Unlike traditional approaches, this work uses initial nodal coordinates. The constraint equations are then formulated using both the current and initial nodal coordinates. Next, the Levenberg-Marquardt method is applied to solve the constraint equations robustly. Finally, the kinematic constraint equations for the instantaneous centers are established using the Aronhold-Kennedy theorem and solved to determine the coordinates of the desired instantaneous center.

1 Mechanical Engineer (University of Pamplona, Colombia); M.Sc. and Ph.D. in Mechanical Engineering – Mechanical Sys-tems Design (Federal University of Santa Catarina, Brazil). Currently full-time professor at the University of Pamplona, working in multibody system dynamics and optimal design of mechanisms. Email: neider.romero@unipamplona.co

2 Mechanical Engineer (Francisco de Paula Santander University, Colombia); M.Sc. in Mechanical Engineering (University of the Andes, Colombia); Ph.D. in Mechanical Engineering (Federal University of Santa Catarina, Brazil). Currently pro-fessor in the Mechanical Engineering Department at the University of Pamplona. Email: gmoren@unipamplona.edu.co

3 Mechanical Engineer (University of Pamplona, Colombia); currently pursuing a specialization in Integrated Management Systems (HSEQ). Currently professor in the Mechanical Engineering program at the University of Pamplona, working on design and optimization of steering mechanisms. Email: rafael.villalba@unipamplona.edu.co

4 B.Sc., M.Sc., and Ph.D. in Mechanical Engineering (Federal University of Santa Catarina, Brazil); Postdoctoral fellow (King's College London). Currently full professor at the Federal University of Santa Catarina (UFSC), specializing in me-chanism design, robotics, and intellectual property. Email: daniel.martins@ufsc.br

Results: Using nodal coordinates and the Aronhold-Kennedy theorem, a procedure was developed to determine the ins-tantaneous center of rotation of a link with respect to the fixed link of a six-bar mechanism. The proposed method is sufficiently robust for use in optimal synthesis processes, which will be addressed in future work.
Conclusions: A method was developed to determine the instantaneous center in a six-bar mechanism using nodal coordinates. The method was validated by implementing the proposed procedure in a mechanism with arbitrary dimensions and comparing the results with those obtained using GIM (Geometric Interactive Method).
Keywords: Instantaneous center, nodal coordinates, six-bar mechanism, Aronhold-Kennedy theorem.

Resumen

Objetivo: El conocimiento del centro instantáneo asociado a dos cuerpos en un mecanismo es importante tanto para el análisis como para la síntesis, dado que puede simplificar el análisis de velocidades y aceleraciones. Asimismo, la determinación precisa de la posición del centro instantáneo es un requisito clave para la síntesis en muchas aplicaciones prácticas. El propósito de este trabajo es proponer un método analítico para calcular el centro instantáneo de rotación de un eslabón flotante en un mecanismo de seis barras con respecto al eslabón fijo.
Metodología: El procedimiento propuesto consta de los siguientes pasos. En primer lugar, se definen las variables que representan las dimensiones del mecanismo. A diferencia de los enfoques tradicionales, este trabajo emplea coordenadas nodales iniciales. A continuación, se formulan las ecuaciones de restricción utilizando tanto las coordenadas nodales actuales como las iniciales. Posteriormente, se aplica el método de Levenberg-Marquardt para resolver de manera robusta las ecuaciones de restricción. Finalmente, se establecen las ecuaciones de restricción cinemática para los centros instantáneos mediante el teorema de Aronhold-Kennedy y se resuelven para determinar las coordenadas del centro instantáneo deseado.
Resultados: Utilizando coordenadas nodales y el teorema de Aronhold-Kennedy, se desarrolló un procedimiento para determinar el centro instantáneo de rotación de un eslabón con respecto al eslabón fijo de un mecanismo de seis barras. El método propuesto es suficientemente robusto para ser empleado en procesos de síntesis óptima, los cuales serán abordados en trabajos futuros.
Conclusiones: Se desarrolló un método para determinar el centro instantáneo en un mecanismo de seis barras utilizando coordenadas nodales. El método fue validado mediante la implementación del procedimiento propuesto en un mecanismo con dimensiones arbitrarias y la comparación de los resultados con los obtenidos mediante GIM (Método Interactivo Geométrico).
Palabras clave: Centro instantáneo, coordenadas nodales, mecanismo de seis barras, teorema de Aronhold-Kennedy.

Introduction

The computation of instantaneous centers of rotation (ICRs) is crucial in several aspects of pla-nar mechanism analysis. ICRs are particularly important for velocity and singularity analysis (1, 2), because they support the prediction of mechanism behavior under different operating conditions. Accurate ICR identification is also essential for configuration synthesis, allowing designers to create mechanisms that satisfy specific motion requirements. In addition, a clear understanding of ICRs is necessary for dynamic modeling, as it provides a basis for accurate simulations and predictions of mechanism behavior under dynamic loads (3). The importance of this analysis is reflected in the many publications devoted to refining and extending these techniques, particularly for complex me-chanisms for which traditional methods are insufficient.

Kennedy's theorem is a fundamental tool in planar mechanism kinematics, providing a graphical method for locating instantaneous centers of rotation (ICRs) in four-bar linkages (1, 2, 4). The theorem is based on the principle that the ICRs of three links in relative motion are collinear. By identifying the intersection of lines connecting known ICRs, the remaining ICRs can be determined systemati-cally. This geometric approach is particularly useful for simpler mechanisms, as it offers an intuitive visualization of instantaneous kinematic behavior. The simplicity and efficiency of the theorem have made it a standard topic in introductory kinematics courses and textbooks.

However, Kennedy's theorem has significant limitations when applied to more complex planar mechanisms. Its applicability is strongly restricted for mechanisms beyond the simple four-bar configuration. For multidegree-of-freedom (multi-DOF) linkages and mechanisms classified as complex or indeterminate, Kennedy's theorem often fails to identify all ICRs (4–6). This limitation stems from the theorem's reliance on readily identifiable four-bar loops within the mechanism structure. In me-chanisms with insufficient four-bar loops or intricate interconnections, the graphical approach of Kennedy's theorem becomes inadequate. The distinction between primary and secondary instant centers further complicates its application. Primary ICRs can often be identified directly by inspec-ting the mechanism geometry, whereas secondary ICRs require more sophisticated techniques (2, 6). The difficulty of locating secondary ICRs using purely graphical methods underscores the need for alternative, more robust approaches. Therefore, the limitations of Kennedy's theorem highlight the need for advanced techniques capable of handling the complexities of multi-DOF and indeterminate linkages.

Screw theory provides a powerful algebraic framework for analyzing the kinematics of planar and spatial mechanisms. This approach has been extended to planar mechanisms, offering an alterna-tive method for determining ICRs, particularly in indeterminate linkages. Valderrama Rodríguez (7) demonstrates the applicability of screw theory to both planar and spherical indeterminate mechanisms. This approach simplifies the equations involved compared with earlier methods, making it more computationally efficient.

Another approach for determining instantaneous centers is based on constraint equations. These equations can be greatly simplified through the use of natural coordinates (8–10) and can then be solved using numerical or analytical methods. In the literature, this methodology is documented only in the work of Sancibrian R. et al. (11), where it is applied to the optimal design of motorcycle suspensions, knee prosthesis mechanisms, and mechanical advantage mechanisms. It is important to note that, although that study uses constraint equations, it does not use natural coordinates.

This paper presents a robust methodology for analyzing the instantaneous centers of a six-bar mechanism using nodal coordinates. The main idea is to formulate Kennedy's theorem in terms of kinematic constraints, which are solved numerically using the Levenberg-Marquardt method. This formulation

makes it possible to obtain solutions even when the mechanism reaches singular posi-tions. The results are compared with those obtained from a kinematic analysis program, demonstra-ting the effectiveness of the method. Although the technique is not directly applicable to indetermi-nate mechanisms, the authors believe that combining this methodology with screw theory may make it possible to solve any planar mechanism; this topic will be studied in future work.

Instantaneous center of rotation

An instantaneous center of rotation is defined as a point common to two bodies in plane motion that has the same instantaneous velocity in both bodies (14). Aronhold and Kennedy independently proved that the instantaneous centers of three bodies are aligned as stated in Theorem 1. In mathema-tical terms, the Aronhold-Kennedy theorem can be expressed by Equation 1, where $\boldsymbol{\omega}_{ij}$ is the angular velocity of body j with respect to body i.

Theorem 1 (Aronhold-Kennedy theorem) *Any three bodies in plane motion will have exactly three instantaneous centers, and they will lie on the same straight line.*

$$\boldsymbol{\omega}_{ik} \times \overrightarrow{P_{ik}P_{ij}} = \boldsymbol{\omega}_{jk} \times \overrightarrow{P_{jk}P_{ij}} \qquad (1)$$

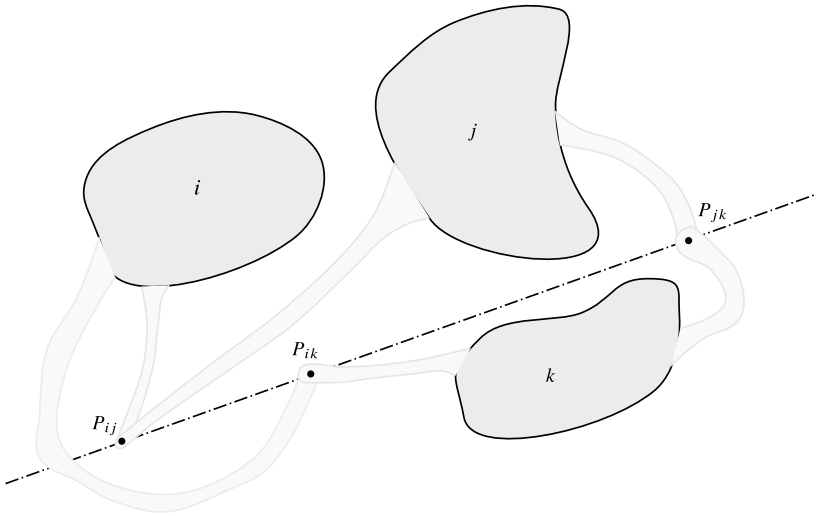

Figure 1. Graphical representation of the Aronhold-Kennedy theorem.

Source: Authors.

In practical terms, the ICR represents the point around which a body appears to rotate at a given instant, even when the body is undergoing a complex motion combining translation and rotation. This fundamental kinematic property makes it possible to significantly simplify the analysis of velocities

and accelerations in complex mechanical systems, converting general motions into instanta-neous pure rotations.

Kinematic modeling

This section presents the formulation used to determine instantaneous centers using nodal coor-dinates. For didactic purposes, the step-by-step procedure is first shown for a four-bar mechanism and is then extended to a six-bar mechanism, which is the objective of this work.

Four-bar mechanism

In this section, the constraint equations that define the kinematics of the mechanism will be deve-loped. For this purpose, the following dimensions are defined: x^0, y^0, x^0, y^0, x_A, y_A, x_B, y_B, where the first four design variables correspond to the initial coordinates of the pairs P_1 and P_2, respectively, and the remaining four variables are the coordinates of the fixed pivots A and B, see Figure 2. The dimensions can be represented in a compact form using a vector,

$$\mathbf{z} = [x_1^0\ y_1^0\ x_2^0\ y_2^0\ x_A\ y_A\ x_B\ y_B]^T \qquad (2)$$

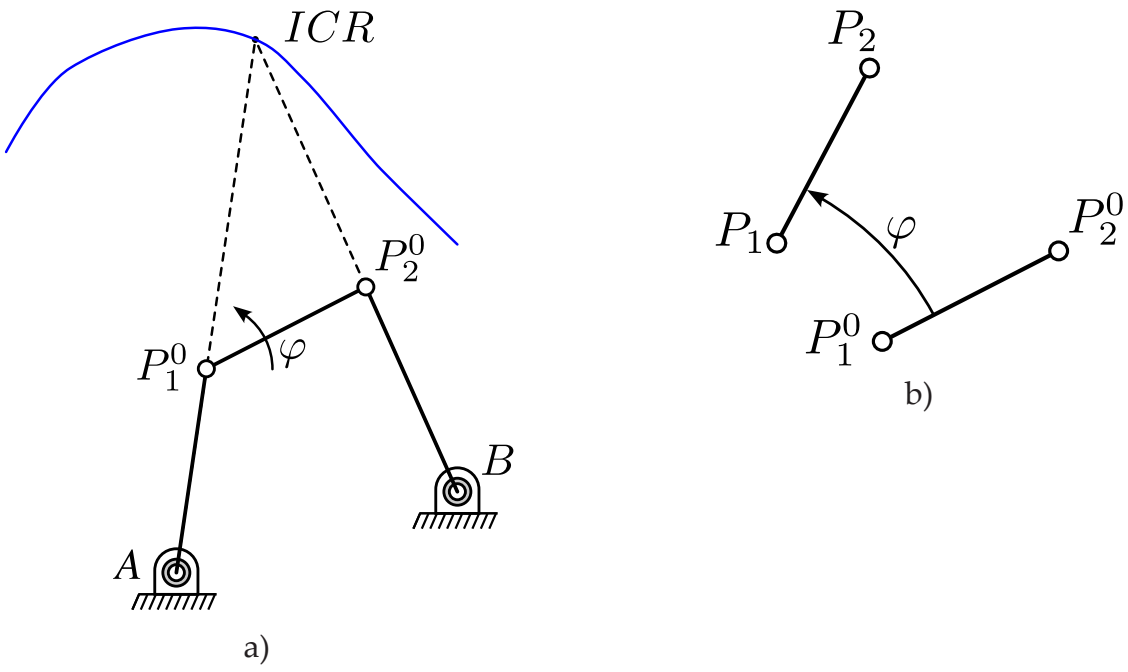

Figure 2. Kinematic representation of the four-bar mechanism.

Source: Authors.

where **z** is the vector of dimensions. To avoid ambiguity in the subsequent formulation, it is emphasized that x^0, y^0, x^0, and y^0 denote the initial coordinates of points P_1 and P_2, whereas x_1, y_1, x_2, and y_2 denote their current coordinates after the coupler rotates by the input angle (denoted here by φ).

Links AP_1 and BP_2 are rigid, so their respective distances remain constant. This can be expressed mathematically as:

$$(x_1 - x_A)^2 + (y_1 - y_A)^2 - [(x^0{}_1 - x_A/2 + (y^0{}_1 - y_A)^2] = 0 \qquad (3)$$

$$(x_2 - x_B)^2 + (y_2 - y_B)^2 - [(x^0{}_2 - x_B/2 + (y^0{}_2 - y_B)^2] = 0 \qquad (4)$$

where Equations 3 and 4 are simply circles with centers at A and B with radii d_{A1} and d_{B2}, respectively. Now note that points P_1 and P_2 are not independent since the coupling link is also rigid, and these two points are dependent on the input angle φ. Therefore, a rotation of an angle φ in the seg-ment P^0P^0 preserves the condition of rigidity, see Figure 2(b), thus, the rotation of the segment can be expressed as:

$$\begin{bmatrix}(x_2 - x_1)\\(y_2 - y_1)\end{bmatrix} = \begin{bmatrix}\cos\phi & -\sin\phi\\ \sin\phi & \cos\phi\end{bmatrix}\begin{bmatrix}(x_2^0 - x_1^0\\(y_2^0 - y_1^0\end{bmatrix} \qquad (5)$$

which can be written as follows,

$$(x_2 - x_1) - (x_2^0 - x_1^0)\cos\varphi + (y_2^0 - y_1^0)\sin\varphi = 0 \qquad (6)$$

$$(y_2 - y_1) - (x_2^0 - x_1^0)\sin\varphi - (y_2^0 - y_1^0)\cos\varphi = 0 \qquad (7)$$

Equations 3, 4, 6 and 7 represent the kinematics of the four-bar mechanism with the coupler as the input link. These constraint equations can be written compactly as follows,

$$\Phi(q, z) = \begin{bmatrix}(x_1 - x_A)^2 + (y_1 - y_A)^2 - \left[(x_1^0 - x_A)^2 + (y_1^0 - y_A)^2\right]\\ (x_2 - x_B)^2 + (y_2 - y_B)^2 - \left[(x_2^0 - x_B)^2 + (y_2^0 - y_B)^2\right]\\ (x_2 - x_1) - (x_2^0 - x_1^0)\cos\phi + (y_2^0 - y_1^0)\sin\phi\\ (y_2 - y_1) - (x_2^0 - x_1^0)\sin\phi - (y_2^0 - y_1^0)\cos\phi\end{bmatrix} = 0 \qquad (8)$$

where **q** is the vector of natural coordinates that corresponds to the coordinates of points P_1 and P_2; therefore,

$$q = \begin{bmatrix}x_1 & y_1 & x_2 & y_2\end{bmatrix}^T \qquad (9)$$

Equation 8 can be solved efficiently using the Newton-Raphson method, which has quadratic convergence provided that the initial estimate is close to the solution. This approach is adequate for simulations, but it is not sufficiently robust for mechanism optimization, because the optimization process may generate mechanism dimensions that are not physically feasible, i.e., cases in which assembly is impossible. To address this problem, the position problem can be reformulated as the minimization of the sum of squares:

$$\underset{\mathrm{q}}{\text{minimize}} \quad \frac{1}{2}\Phi(\mathrm{q},\mathrm{z})^{T}\Phi(\mathrm{q},\mathrm{z}) \qquad (10)$$

which provides an error measure when mechanism assembly is not physically possible. The resi-dual error can then be used to penalize the objective function, making gradient-based optimization methods feasible (12). The optimization problem formulated in Equation 10 can be solved using the Levenberg-Marquardt method, as shown in Algorithm 1.

Algorithm 1 Levenberg-Marquardt method

Require: $\mathbf{\Phi}_{\mathrm{q}} = \partial\mathbf{\Phi}_{\mathrm{q}}/\partial\mathbf{q}$, λ, $\mathbf{q}_0$, $\mathbf{\Phi}$

Ensure: q

for j=1 to 20 **do**
  $\Delta f \leftarrow \mathbf{\Phi}_{\mathrm{q}}^{T} \cdot \mathbf{\Phi}$;
  $\mathbf{H} \leftarrow \frac{\partial \nabla f}{\partial q}$
  if $\|\nabla f\| < \epsilon$ **then**
    break
  end if
  $(\mathbf{H} + \lambda \mathbf{I})\mathbf{s} \leftarrow -\nabla f$
  $f_p \leftarrow f(\mathbf{q} + \mathbf{s})$
  if $f_p < f$ **then**
    $\lambda \leftarrow \lambda/10$
    $\mathbf{q} \leftarrow \mathbf{q} + \mathbf{s}$
  else
    $\lambda \leftarrow \lambda \cdot 10$
  end if
end for

In Algorithm 1, **H** is the Hessian matrix, **I** is the identity matrix, λ is a scalar value, and Δf is the gradient.

Once the position kinematics of the four-bar mechanism has been solved, the instantaneous center of rotation (ICR), illustrated in Figure 2, must be determined:

$$\mathbf{r}_{AP^{ic}} \times \mathbf{r}_{AP_1} = 0 \qquad (11)$$

$$\mathbf{r}_{BP^{ic}} \times \mathbf{r}_{BP_2} = 0 \qquad (12)$$

where P^{ic} is the position of the instantaneous center of rotation between the coupler and the fixed link. The above two constraint equations can be written in expanded form as,

$$(x^{ic} - x_A)(y_1 - y_A) - (y^{ic} - y_A)(x_1 - x_A) = 0 \qquad (13)$$

$$(x^{ic} - x_B)(y_2 - y_B) - (y^{ic} - y_B)(x_2 - x_B) = 0 \qquad (14)$$

These two constraint equations can be rewritten as follows,

$$(y_1 - y_A)x^{ic} - (x_1 - x_A)y^{ic} = (y_1 - y_A)x_A - (x_1 - x_A)y_A \qquad (15)$$

$$(y_2 - y_B)x^{ic} - (x_2 - x_B)y^{ic} = (y_2 - y_B)x_B - (x_2 - x_B)y_B \qquad (16)$$

Now Equations 15 and 16 can be written in matrix form as follows,

$$\begin{bmatrix} (y_1 - y_A) & -(x_1 - x_A) \\ (y_2 - y_B) & -(x_2 - x_B) \end{bmatrix} \begin{bmatrix} x^{ic} \\ y^{ic} \end{bmatrix} = \begin{bmatrix} (y_1 - y_A)x_A - (x_1 - x_A)y_A \\ (y_2 - y_B)x_B - (x_2 - x_B)y_B \end{bmatrix} \qquad (17)$$

In order to generalize the procedures developed for the four-bar mechanism to the analysis of more complex mechanisms, Equation 17 can be rewritten as follows,

$$\mathbf{A}^{ic}(\mathbf{q})\mathbf{P}^{ic} = \mathbf{B}^{ic}(\mathbf{q}) \qquad (18)$$

where $\mathbf{A}^{ic}$ is the coefficient matrix and $\mathbf{B}^{ic}$ is the resultant vector. Equation 18 is referred to as the instantaneous-center equation. In the following section, where a six-bar mechanism is analyzed, it is shown that the instantaneous-center equation is generally nonlinear.

Six-bar mechanism

In this section, the method proposed for the four-bar mechanism is generalized to the kinematic study of six-bar mechanisms, as shown in Figure 3. This mechanism is defined by the following dimensions or design variables:

$$Z = [x_1^0 \; y_1^0 \; x_2^0 \; y_2^0 \; x_3^0 \; y_3^0 \; x_4^0 \; y_4^0 \; x_5^0 \; x_5^0 \; x_A \; y_A \; x_B \; y_B]^T \qquad (19)$$

The constraint equations that describe the positional kinematics of the mechanism are now defined. Distance equations can be established for the segments AP_1, P_1P_2, BP_2, P_1P_3, P_2P_3, P_2P_5, BP_5,

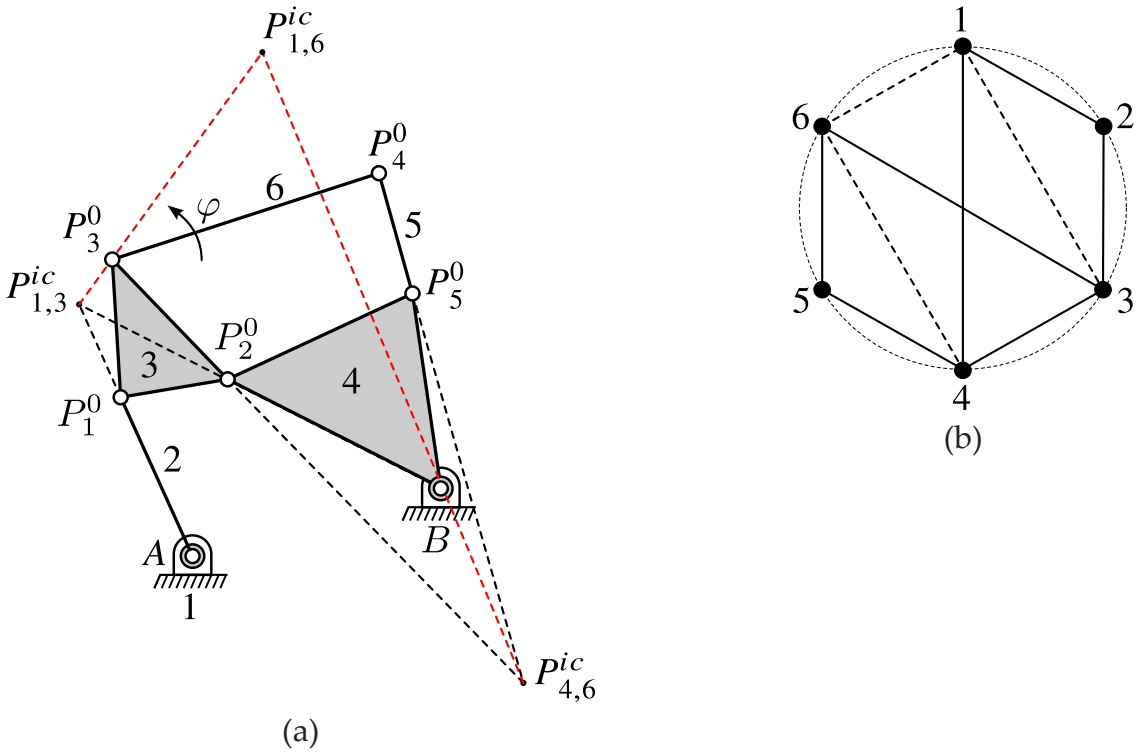

Figure 3. Kinematic diagram and location of the ICRs of the six-bar mechanism using Kennedy's theorem.

Source: Authors.

and P_4P_5. Two additional constraint equations are then defined by applying a rotation φ to the segment P_3P_4. These constraints are grouped in the constraint vector shown in Equation 21, where the vector of natural coordinates is:

$$q = [x_1 \; y_1 \; x_2 \; y_2 \; x_3 \; y_3 \; x_4 \; y_4 \; x_5 \; y_5]^T \qquad (20)$$

$$\Phi(q,z)=\begin{bmatrix}(x_1-x_A)^2+(y_1-y_A)^2-\left[(x_1^0-x_A)^2+(y_1^0-y_A)^2\right]\\(x_2-x_B)^2+(y_2-y_B)^2-\left[(x_2^0-x_B)^2+(y_2^0-y_B)^2\right]\\(x_2-x_1)^2+(y_2-y_1)^2-\left[(x_2^0-x_1^0)^2+(y_2^0-y_1^0)^2\right]\\(x_3-x_1)^2+(y_3-y_1)^2-\left[(x_3^0-x_1^0)^2+(y_3^0-y_1^0)^2\right]\\(x_3-x_2)^2+(y_3-y_2)^2-\left[(x_3^0-x_2^0)^2+(y_3^0-y_2^0)^2\right]\\(x_5-x_2)^2+(y_5-y_2)^2-\left[(x_5^0-x_2^0)^2+(y_5^0-y_2^0)^2\right]\\(x_5-x_B)^2+(y_5-y_B)^2-\left[(x_5^0-x_B)^2+(y_5^0-y_B)^2\right]\\(x_5-x_4)^2+(y_5-y_4)^2-\left[(x_5^0-x_4^0)^2+(y_5^0-y_4^0)^2\right]\\(x_4-x_3-(x_4^0-x_3^0)\cos\phi+(y_4^0-y_3^0)\sin\phi\\(y_4-y_3)-(x_4^0-x_3^0)\sin\phi-(y_4^0-y_3^0)\cos\phi\end{bmatrix}=0 \qquad (21)$$

For the mechanism under analysis, the centers of rotation can be determined graphically using Kennedy's theorem (14), which states that the instantaneous centers of three bodies are aligned. For more complex mechanisms, velocity analysis can be performed using natural coordinates (9) or screw theory, which enables systematic determination of all instantaneous centers without calculating derivatives (13).

The relationship between the instantaneous centers can be written mathematically by means of the constraint vector:

$$\mathbf{\Phi}^{ic}(\mathbf{q},\mathbf{q}^{ic})=\mathbf{0} \qquad (22)$$

where $\mathbf{\Phi}^{ic}$ is the vector of instantaneous-center constraints and $\mathbf{q}^{ic}$ is the vector of instantaneous centers. For the six-bar mechanism shown in Figure 3, Equation 22 can be written as:

$$\Phi^{ic}\left(q,q^{ic}\right)=\begin{bmatrix}\mathbf{r}_{AP_{1,3}^{ic}}\times\mathbf{r}_{AP_1}\\\mathbf{r}_{BP_{1,3}^{ic}}\times\mathbf{r}_{BP_2}\\\mathbf{r}_{P_4P_{4,6}^{ic}}\times\mathbf{r}_{P_4P_5}\\\mathbf{r}_{P_3P_{4,6}^{ic}}\times\mathbf{r}_{P_3P_2}\\\mathbf{r}_{BP_{4,6}^{ic}}\times\mathbf{r}_{BP_{1,6}^{ic}}\\\mathbf{r}_{P_3P_{1,3}^{ic}}\times\mathbf{r}_{P_3P_{1,6}^{ic}}\end{bmatrix}=0 \qquad (23)$$

In this case, the equation was found to be nonlinear with respect to the coordinates of the ins-tantaneous centers. However, the system can be decoupled into two linear systems: one with four equations and four unknowns, Equation 24, and another with two equations and two unknowns, Equation 25. Whether the general system can always be expressed as a set of linear systems remains unknown; addressing this question would require the analysis of additional systems.

$$\begin{bmatrix} (y_1 - y_A) & -(x_1 - x_A) & 0 & 0 \\ (y_2 - y_B) & -(x_2 - x_B) & 0 & 0 \\ 0 & 0 & (y_5 - y_4) & -(x_5 - x_4) \\ 0 & 0 & (y_2 - y_3) & -(x_2 - x_3) \end{bmatrix} \begin{bmatrix} x_{P_{13}} \\ y_{P_{13}} \\ x_{P_{46}} \\ y_{P_{46}} \end{bmatrix} = \begin{bmatrix} x_A (y_1 - y_A) + y_A (x_1 - x_A) \\ x_B (y_2 - y_B) + y_B (x_2 - x_B) \\ x_4 (y_5 - y_4) + y_4 (x_5 - x_4) \\ x_3 (y_2 - y_3) + y_3 (x_2 - x_3) \end{bmatrix} \quad (24)$$

$$\begin{bmatrix} -(y_{P_{46}} - y_B) & (x_{P_{46}} - x_B) \\ -(y_{P_{13}} - y_3) & (x_{P_{13}} - x_3) \end{bmatrix} \begin{bmatrix} x_{P_{16}} \\ y_{P_{16}} \end{bmatrix} = \begin{bmatrix} y_B (x_{P_{46}} - x_B) - x_B (y_{P_{46}} - y_B) \\ y_3 (x_{P_{13}} - x_3) - x_3 (y_{P_{13}} - y_3) \end{bmatrix} \quad (25)$$

Results

This section demonstrates the implementation of the proposed procedure for arbitrary dimen-sions of both a four-bar mechanism and a six-bar mechanism. In practical problems, the instantaneous center of rotation of a particular link with respect to the fixed link is often of interest. Therefore, only instantaneous centers of practical interest are analyzed here. The proposed model was imple-mented in MATLAB, and its results were verified using GIM (Geometrical Interactive Method). Figures 4 and 5 provide a graphical comparison between the results obtained with the proposed model and those obtained with GIM for the four-bar and six-bar mechanisms, respectively. For both mecha-nisms, the maximum absolute error and RMSE were zero within the numerical precision adopted in both programs. For reproducibility, the source codes and simulation files were deposited in Zenodo for the four-bar mechanism at (15) and for the six-bar mechanism at (16).

Table 1 shows the nodal dimensions of the four-bar mechanism, where all dimensions are expres-sed in units of length. Because this is an illustrative example, the units are not specified. Figure 4(a) shows, in red, the trajectory of the instantaneous center of the coupler with respect to the fixed link. Figure 4(b) illustrates a possible application of this instantaneous center calculation. This application is relevant because the trajectory of the instantaneous center of rotation is an important kinematic indicator in the analysis and design of knee prosthesis mechanisms, where the relative motion between the thigh and shank must be accurately reproduced.

Table 1. *Nodal dimensions of the four-bar mechanism.*

Dimensions	x_1^0	y_1^0	x_2^0	y_2^0	x_A	y_A	x_B	y_B
Values	0	2.5	2	2.5	0	0	3	0

Source: Authors.

Table 2 shows the nodal dimensions of the six-bar mechanism, where all dimensions are expressed in units of length. Figure 5(a) shows, in red, the trajectory of the instantaneous center of link 3 relative to the fixed link; in green, the instantaneous center of link 6 relative to link 4; and in blue, the instantaneous center of link 6 relative to fixed link 1. A possible application of this instantaneous center calculation is illustrated in Figure 5(b).

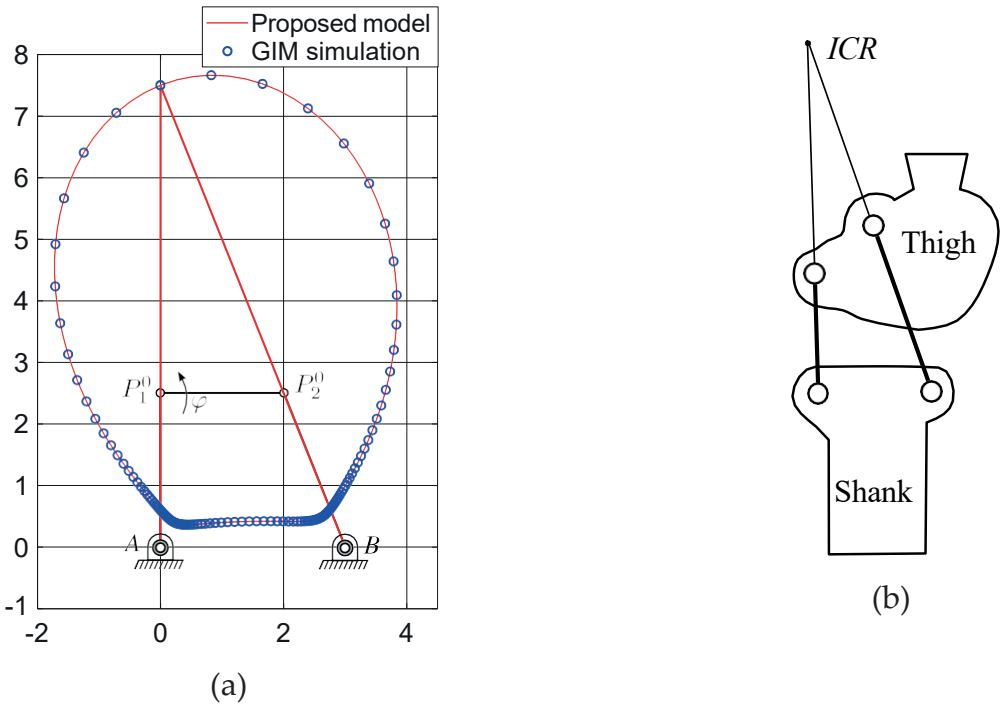

Figure 4. Comparison between the results obtained with the proposed MATLAB implementation and GIM (Geometrical Interactive Method) for the four-bar mechanism. (a) Trajectory of the instantaneous center of rotation of the coupler relative to the fixed link. (b) Example of application to the kinematic analysis of a knee prosthesis.

Source: Authors.

Conclusions

This study developed and validated an analytical method for determining the instantaneous center of rotation (ICR) in planar mechanisms, specifically in a six-bar linkage, using nodal coordinates and the Aronhold-Kennedy theorem. The proposed methodology is based on formulating kinematic constraint equations as a nonlinear system, which is solved robustly using the Levenberg-Marquardt method. The results show that this approach enables precise identification of ICRs of practical interest and can be applied to arbitrary geometries, thereby avoiding reliance on traditional graphical methods that often fail in complex or indeterminate mechanisms. In addition, it was shown that, under certain conditions, the nonlinear system can be rewritten as a set of linear subsystems, opening the door to more efficient computational implementations.

Table 2. *Nodal dimensions of the six-bar mechanism.*

Dimensions	Values	Dimensions	Values
x_1^0	-5.820789	y_1^0	13.05212
x_2^0	2.471042	y_2^0	17.23752
x_3^0	-3.451695	y_3^0	27.5036
x_4^0	5.071548	y_4^0	33.37934
x_5^0	25.37229	y_5^0	20.55425
x_A	0	y_A	0
x_B	28.05727	y_B	4.760285

Source: Authors.

This approach has strong potential for incorporation into mechanism synthesis and optimization, and it provides a solid foundation for future research in multibody system dynamics, particularly when combined with geometric frameworks such as screw theory.

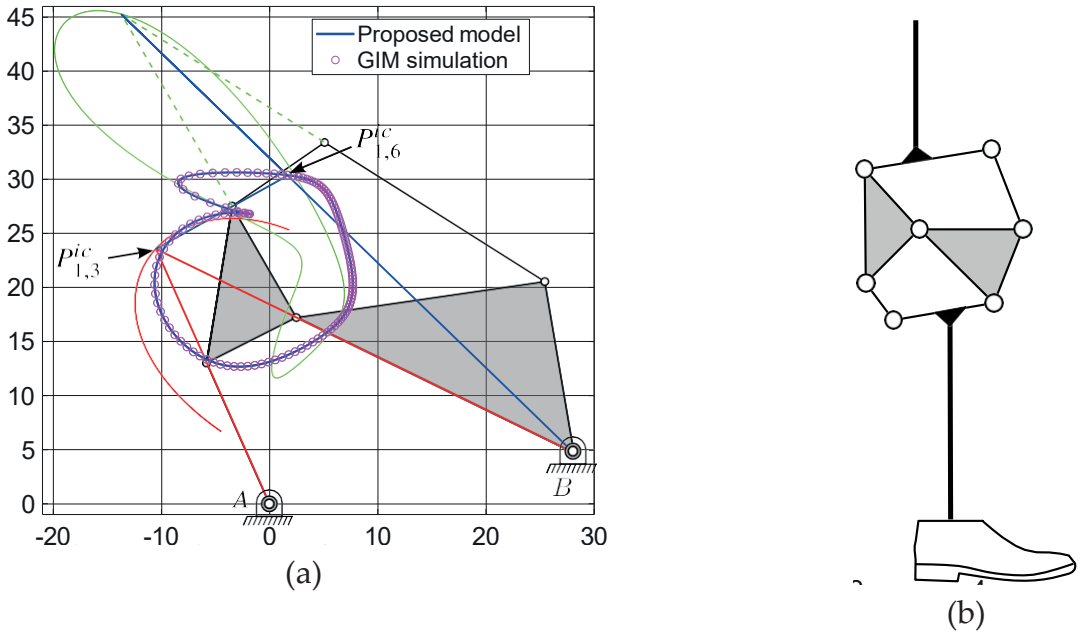

Figure 5. Comparison between the results obtained with the proposed MATLAB implementation and GIM (Geometrical Interactive Method) for the six-bar mechanism. (a) Trajectories of the instantaneous centers of rotation: link 3 relative to the fixed link, link 6 relative to link 4, and link 6 relative to the fixed link. (b) Example of application of the computed instantaneous centers.

Source: Authors.

Acknowledgments

The authors would like to thank the Mechanical Engineering Research Group of the University of Pamplona (GIMUP) for their support and valuable contributions to this work.

This work was partially supported by ANEEL and Celesc under R&D projects 5697-0923/2023 and 5697-1123/2023; FINEP under R&D project 0378/2023; Embraer under project GDT0045-2024; CAPES under Finance Code 001; and CNPq under grant 312980/2025-6, Brazil.

References

[1] S. Zarkandi, "Application of mechanical advantage and instant centers on singularity analysis of single-DOF planar mechanisms," *J. Mech. Eng.*, vol. 41, no. 1, pp. 50–57, 2010. https://doi.org/10.3329/jme.v41i1.5362 ↑ 2, 3

[2] P. A. Simionescu, I. Talpasanu, and R. di Gregorio, "Instant-center based force transmissivity analysis in planar mechanisms," *J. Mech. Des.*, vol. 132, no. 6, pp. 061003–1–061003–9, 2010. https://doi.org/10.1115/1.4001094 ↑ 2, 3

[3] L. Nie, H. Ding, K.-L. Ting, and A. Kecskeméthy, "Instant center identification of single-loop multi-DOF planar linkage using virtual link," *Appl. Sci.*, vol. 11, no. 10, p. 4463, 2021. https://doi.org/10.3390/app11104463 ↑ 3

[4] J. I. Valderrama-Rodríguez, J. M. Rico, J. J. Cervantes-Sánchez, and R. García-García, "A screw theory approach to computing the instantaneous rotation centers of indeterminate planar linkages," *Robotics*, vol. 11, no. 1, p. 6, 2021. https://doi.org/10.3390/robotics11010006 ↑ 3

[5] R. Di Gregorio, "An algorithm for analytically calculating the positions of the secondary instant centers of indeterminate linkages," *J. Mech. Des.*, vol. 130, no. 4, p. 042302, 2008. https://doi.org/10.1115/1.2839008 ↑ 3

[6] Y. P. Chang and I. Her, "A virtual cam method for locating instant centers of kinematically indeterminate linkages," *J. Mech. Des.*, vol. 130, no. 6, p. 062301, 2008. https://doi.org/10.1115/1.2900720 ↑ 3

[7] J. I. Valderrama-Rodríguez, J. M. Rico, and J. J. Cervantes-Sánchez, "A general method for the determi-nation of the instantaneous screw axes of one-degree-of-freedom spatial mechanisms," *Mech. Sci.*, vol. 11, no. 1, pp. 91–99, 2020. https://doi.org/10.5194/ms-11-91-2020 ↑ 3

[8] J. G. De Jalón, J. Unda, and A. Avello, "Natural coordinates for the computer analysis of multibody sys-tems," *Comput. Methods Appl. Mech. Eng.*, vol. 56, no. 3, pp. 309–327, 1986. https://doi.org/10.1016/0045-7825(86)90044-7 ↑ 4

[9] J. G. De Jalón and E. Bayo, *Kinematic and Dynamic Simulation of Multibody Systems*. Berlin, Germany: Springer-Verlag, 1994. ↑ 4, 11

[10] N. N. Romero, "Contributions to the kinematics and balancing of mechanisms," Ph.D. dissertation, 2023. ↑ 4

[11] R. Sancibrian, E. G. Sarabia, A. Sedano, and J. M. Blanco, "A general method for the optimal synthesis of mechanisms using prescribed instant center positions," *Appl. Math. Model.*, vol. 40, no. 3, pp. 2206–2222, 2016. https://doi.org/10.1016/j.apm.2015.09.032 ↑ 4

[12] J.-F. F. Collard, "Geometrical and kinematic optimization of closed-loop multibody systems," Ph.D. dis-sertation, Université Catholique de Louvain, 2007. ↑ 8

[13] H. R. Cazangi, "Aplicação do método de Davies para análise cinemática e estática de mecanismos com múltiplos graus de liberdade," M.S. thesis, 2008. ↑ 11

[14] R. L. Norton, *Design of Machinery: An Introduction to the Synthesis and Analysis of Mechanisms and Machines*. New York, NY, USA: McGraw-Hill Higher Education, 2003. ↑ 4, 11

[15] N. N. Romero Nuñez, "Simulation of a four-bar mechanism in MATLAB and GIM," *Zenodo*, 2026. https://doi.org/10.5281/zenodo.19378994 ↑ 12

[16] N. N. Romero Nuñez, "Simulation of a six-bar mechanism in MATLAB and GIM," *Zenodo*, 2026. https://doi.org/10.5281/zenodo.19379264 ↑ 12

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.24200

INVESTIGACIÓN

Petri Net Modeling of a Teleoperated Laboratory for Mechanical Ventilation Training

Modelado con Redes de Petri de un Laboratorio Teleoperado para entrenamiento en Ventilación Mecánica

Andrés Mauricio Valencia [1]

Fecha de Recepción: 12 de octubre de 2025 **Fecha de Aceptación**: 28 de abril de 2026

Cómo citar: A.M. Valencia, «Petri Net Modeling of a Teleoperated Laboratory for Mechanical Ventilation Training», *Tecnura*, vol. 30, n.° 88, jun. 2026. 19–37. https://doi.org/10.14483/22487638.24200

Abstract

Pulmonary pathologies persist as leading contributors to global morbidity and mortality. This scenario was further intensified following the advent and rapid dissemination of COVID-19, underscoring the critical necessity for technological advancements in clinical patient oversight, especially within the domain of mechanical respiratory assistance. However, the integration of cyber-physical systems with remote instructional platforms and virtually accessible laboratories dedicated to the training of medical professionals in ventilator operation, remains inadequately investigated. To bridge this gap, this work delineates the architecture and engineering particulars of an e-learning ecosystem that seamlessly integrates electromechanical components and computational applications with pedagogical strategies. The proposed model uses Colored petri Nets as a rigorous formalism for representing and emulating the intricate dynamic processes inherent to the system.

Keywords: Mechanical Ventilation, Virtual Learning Environments, Teleoperated Equipment, Cyber-Physical Systems, Colored Petri Nets, Simulation and Modeling, Remote Laboratories, Healthcare Professional Training

Resumen

Las patologías pulmonares se mantienen entre las principales causas de morbilidad y mortalidad a nivel mundial. Esta situación se vio agravada con la aparición y diseminación del COVID-19, evidenciando la necesidad crítica de avances tecnológicos para la supervisión clínica, particularmente en el ámbito de la asistencia respiratoria mecánica. No obstante, la integración de sistemas ciberfísicos con plataformas de instrucción remota y laboratorios de acceso virtual, dedicados a la formación de profesionales médicos en el manejo de ventiladores, ha sido escasamente explorada. Para abordar esta brecha, este trabajo presenta el diseño y los detalles de ingeniería de un ecosistema de aprendizaje digital que integra de manera armoniosa componentes electromecánicos y aplicaciones computacionales con estrategias pedagógicas. El modelo propuesto utiliza Redes de Petri Coloreadas como un formalismo riguroso para representar y emular los complejos procesos dinámicos inherentes al sistema.

1 Docente de la Escuela de Ingeniería de sistemas y Ciencias de la Computación de la Universidad del Valle. Miembro del grupo de investigación BONOVO, GUIA. ROR Email: andres.valencia.restrepo@correounivalle.edu.co

Palabras Clave: Ventilación Mecánica, Entornos Virtuales de Aprendizaje, Equipos Teleoperados, Sistemas Ciberfísicos, Redes de Petri Coloreadas, Simulación y Modelado, Laboratorios Remotos, Formación de Profesionales de la salud.

Introduction

Ventilation, an innate physiological process critical for hemodynamic gas exchange (O_2 and CO_2), is typically performed autonomously [1]. Despite this, pulmonary disorders continue to constitute a predominant cause of global mortality and impairment [2]. This panorama has been aggravated by diverse factors, including pathological and ecological concerns [3], [4]. Specifically, the COVID-19 pandemic precipitated a considerable burden, manifesting as a clinical spectrum linked to SARS-CoV-2 infection. Its presentation spans from mild respiratory afflictions to severe interstitial pneumonitis and acute respiratory distress syndrome (ARDS) [5], thereby introducing novel complexities for clinical practitioners.

The escalation in fatalities and number of cases was propelled by multiple determinants. These encompassed a constrained inventory of apparatus for managing critically ill individuals, the hazard of pathogen transmission among clinical staff, cross-contamination originating from infected personnel, and logistical complications in the distribution of mechanical ventilatory support. On July 13, 2020, Bogotá, Colombia's capital, documented an intensive care unit (ICU) utilization rate of 97.3%, wherein 71.8% of occupied beds were allocated to COVID-19 patients during that period [3]. Concurrently, the city of Cali accounted for 1,780 fatalities out of a national total of 28,803 deaths associated with COVID-19 [4]. Consequently, mitigating the exposure of clinical staff to infected individuals is paramount for diminishing transmission risk, rendering the investigation of all viable methodologies an imperative objective.

Implementing digital transformation paradigms offers a pathway to diminish clinician exposure within both instructional and therapeutic contexts. Although numerous academic and commercial pulmonary simulators have been engineered [6]–[15], and the pandemic has accelerated the development of mechanical ventilators [16]–[28], a scarcity of information persists regarding cyber-physical structures that facilitate remote actuation. For instance, reference [29] proposed a taxonomy that categorizes ventilation initiatives across ten attributes, organized by constructs of manufacturability, flexibility, and expandability. As noted in [30], the engineering of such devices is directed by the confluence of sophisticated technologies, frequently characterized as "intelligent," although remote control and surveillance functionalities have been marginally addressed. Notwithstanding, [31] details a mechanical ventilator incorporating internet-based telemonitoring capacities, and [32] outlines a virtual simulation environment conceived as an autodidactic instrument for novice medical staff has been outlined [32]. While [33] conceded that further investigation is requisite before telemonitoring can be deemed a substantive enhancement in patient management, its application within clinical training milieus is endorsed.

Embracing a proactive stance, [34] introduced a foundational infrastructure intended to augment synergy among medical practitioners, technological suites, and digital informatics, thereby promoting the transition to cognizant domiciliary hospitalization. The uniformity and efficacy of integration and orchestration across disparate components and data streams, the adoption of stringent formal modeling methodologies—such as Colored Petri Nets (CPNs)—is recommended. As an example, [35] demonstrates how patient statuses and the correlations among clinical interventions and assets can be depicted inside a cloud-centric healthcare network utilizing CPN Tools. Correspondingly, [36] proposes a Petri net schema for a decentralized telemedicine system based on SOA and contemporary telecommunication protocols. In a cognate manner, [37] elaborates a mechanism enabling the remote oversight of rehabilitative protocols via teleoperated instrumentation. Furthermore, Colored Petri Nets were deployed in [38] to authenticate a decentralized configuration for locomotion assessment and in [39] to institute a security-oriented modeling architecture for digital learning infrastructures.

Within this conceptual milieu, the present investigation delineates an instructional platform that facilitates the actuation and monitoring of mechanical ventilation through digital emulation and online-enabled technologies. Owing to the event-driven dynamics intrinsic to the proposed system, its architecture is formally abstracted using a Colored Petri Net representation to meticulously encapsulate its operational logic.

Methodological Framework

This investigation was based on an adaptive methodological framework, conceptually grounded in the iterative cycles of the spiral development paradigm (Figure 1). The ensuing elaboration delineates the distinct phases constituting this research approach.

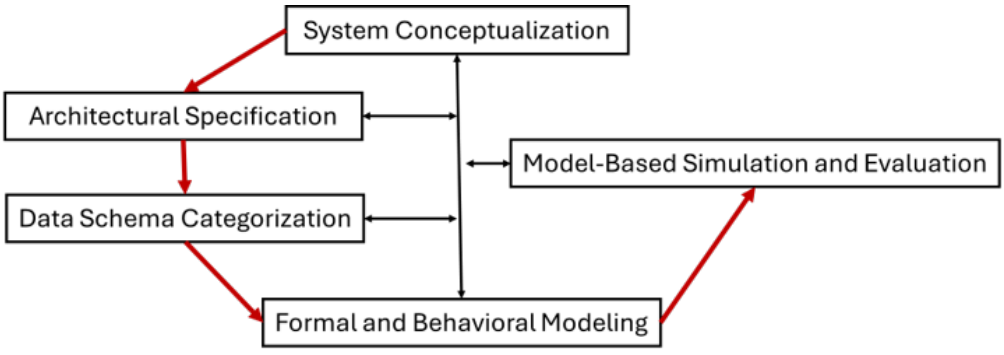

Figure 1. Methodological framework.

Source: own elaboration.

System Conceptualization:

The initial phase is dedicated to establishing a foundational understanding of the target system. This involves a meticulous analysis of its operational principles to identify core functions, primary architectural constituents, and contextual boundaries. The culmination of this stage yields a precise characterization of all system elements, facilitating a clear understanding of the synergies between physical and logical entities that enable the execution of designated processes.

Architectural Specification:

This stage focuses on formalizing the operational architecture of the system, leveraging the insights acquired from the preceding phase. The methodology advocates for the application of high-level structural schematics [40], which provide a holistic visualization of the system's topology and the interconnectivity between its central and peripheral components. The procedure initiates with the identification of principal system actors. Each entity is delineated by its fundamental purpose and its interaction protocols with other elements, maintaining a conceptual perspective devoid of implementation specifics. Completion of this phase yields a comprehensive layout blueprint of the system, highlighting key agents, auxiliary modules, and their functional interdependencies.

Data Schema Categorization:

Building upon the architectural schematics, an exhaustive inventory of critical system variables is compiled. The process begins by enumerating local variables, which are confined to separate functional units or modules. This is followed by the global variable specification, which facilitate data exchange across multiple operational segments. Performing this classification early in the development lifecycle is criticalbecause the resultant schema forms the basis for establishing data relationships in the final model, governing the information flow and transactional logic between system entities.

Formal and Behavioral Modeling:

In this phase, the system's operational specifications are refined through an evolved set of architectural diagrams. These representations are enriched with detailed descriptions of the dynamic behavior of the system, incorporating the data schema defined previously. The consolidation of this information guides the design of discrete functional modulesengineered to ensure robust performance of the simulated environment. The resulting diagrams are instrumental, as they supply the foundational input for constructing Colored Petri Net models, which validate the system's holistic functionality by defining its structural and dataflow properties.

Model-Based Simulation and Evaluation:

A suite of simulation scenarios is constructed by leveraging the outputs from all prior stages, each accompanied by specific observation criteria and performance indicatorsevaluation. Every scenario is architected in accordance with discrete analytical objectives, which may include evaluating resource utilization, verifying process concurrency, or appraising overall systemic throughputevaluation.

Results

Architectural Synopsis of the Remote Mechanical Ventilation Training Platform

The implemented cyber-physical framework for remote mechanical ventilation instruction was engineered to deliver experiential skill development via teleoperated interfaces (Figure 2). This solution is particularly advantageous for healthcare professionals and trainees facing geographical or infrastructural constraints that hinder access to conventional hands-on training. The platform's architecture is structured to cultivate the core competencies necessary for the adept clinical management of mechanical ventilation systems.

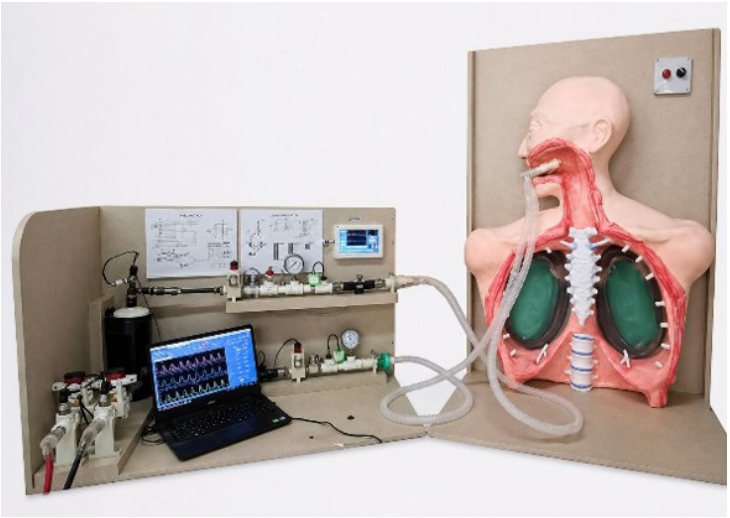

Figure 2. Mechanical Ventilator (MV) and Patient Emulator (PE)

Source: own elaboration.

A dedicated mechanical ventilation training laboratory was engineered to fulfill this objective, comprising two fundamental units: a ventilator simulator and a computational patient model. These entities are unified within a teleoperation infrastructure, permitting comprehensive command and monitoring via distinct human-machine interfaces (HMIs)—one allocated for the instructor and another for the student cohort. This split access model delineates user privileges and streamlines asset allocation, positioning the instructor as the system administrator with the authority to define and modulate the operational permissions granted to learners.

Trainees interact with the platform through their assigned interfaces, connecting via personal computing equipment. Initially, participants are assigned a read-only mode that is elevated to an active control state upon receiving explicit authorization from the instructor. This transition enables real-time adjustment of ventilator operational parameters from the student terminal.

Furthermore, the cyber-physical system incorporates a comprehensive data logging mechanismthat archives all operational information produced during instructional sessions within a centralized repository. This capability supports post-session auditing and analytical review, while also permitting the detailed tracing of user performance, documenting both appropriate and incorrect interventions. The databank captures three primary data classifications:

- **Control Parameters**: Configurable settings modified by the trainee to govern the operational modes of the ventilator simulator and the physiological patient model.

- **Clinical Contextualization Data**: The instructor supplied supplementary information to frame the patient emulator's state within a plausible medical narrative. While this data does not directly influence the emulator's dynamics, it serves to heighten the simulation's fidelity.

- **Apparatus Telemetry Data**: Live sensor readings—encompassing pressure, volumetric flow, and oxygen concentration—alongside the status of actuation components (e.g., Vacuum pumps, proportional solenoids, and binary actuators) integrated into the physical laboratory apparatus.

Functional Architecture of the Remote Ventilator Training Platform

The implemented communication structure facilitates synchronous interaction between a single instructor and multiple trainees, all interfaced concurrently with the ventilator simulator and the patient model. The system's functional topology, illustrated in Figure 3, delineates the principal data pathways and the interconnectivity between its constituent modules.

Core architectural constituents:

- **Instructor Command Console (Figure 4)**: This interface provides a supervisory control environment, facilitating direct instructor-student communication and full command over the physical apparatus—namely, the mechanical ventilator and patient emulator. It delivers exhaustive telemetry on equipment status and enables the dynamic allocation or revocation of trainee operational privileges.

- **Trainee Operational Terminal (Figure 5):** A digital simulation environment that facilitates mediated interaction with the ventilator system. All operational commands issued by the trainee are routed through and require validation by the instructor's console, ensuring supervised execution.

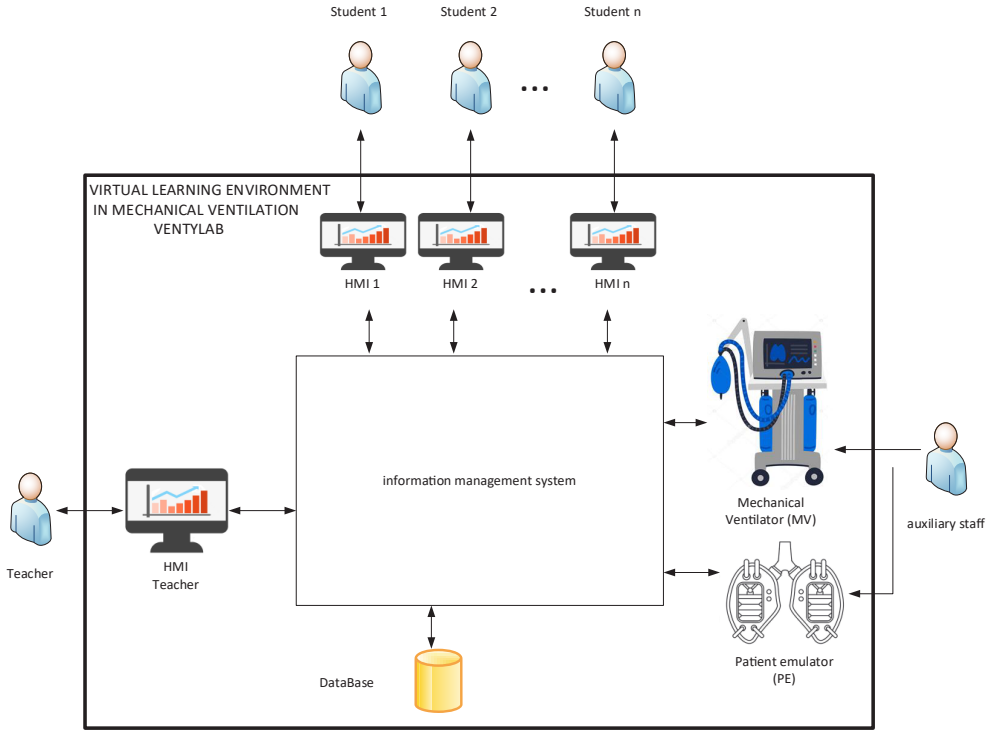

Figure 3. Characters involved in the information system.

Source: own elaboration

Figure 4. HMI Instructor.

Source: own elaboration

Figure 5. HMI Student.

Source: own elaboration

- **Mechanical Ventilator (MV):** This is a clinical-grade apparatus engineered to provide full or partial respiratory support for patients with compromised pulmonary function. Its operational principle involves the automated delivery of a precisely blended respiratory gas (comprising medical air and oxygen) to the patient's airways.

- **Patient emulator (PE):** A hardware unit that interfaces directly with the mechanical ventilator to simulate the biomechanical properties of the human respiratory system. Through the calibration of physiological parameters—including pulmonary compliance, tracheobronchial resistance, and circuit leakage—it can replicate a diverse spectrum of pathological pulmonary states. The design and implementation of this simulator are detailed in [41].

Variable Specification for the Remote Mechanical Ventilation Training Platform

Each entity delineated in Figure 2 is associated with a distinct set of operational variables, which are characterized as follows.

Trainee Terminal:

This interface relays ventilator configuration parameters to the central communication node. This data stream is formally represented by the variable ve(n), where the index (n) denotes the specific trainee initiating the parameter adjustment. Table 1 provides a comprehensive specification of these variables.

Table 1. *Operational variables of the Cyber-Physical System.*

Variable	Values	Description
IP	1…5	The IP address is used to facilitate the structured and secure transfer of data between devices.
sid(n)	sid(1), sid(2), …, sid(n)	Unique identifier for each student participant in the training scenario.
vpe	vpe1, vpe2, vpe3	Configuration parameters defined by the instructor for the patient emulator.
set up (data)	set up("mv1"), set up("mv2"), set up("mv3")	Configuration parameters assigned to each mechanical ventilator emulator instance is conducted.
Variables (data)	variables("vmv1"), variables("vmv2"), variables("vmv3")	The mechanical ventilator emulator generates operational variables during simulation and training.

Functional and Operational Modeling of the Remote Mechanical Ventilation Training Platform

Following the systematic characterization of the principal agents of the system and their associated operational variables, the subsequent phase involves a granular analysis of its core functionalities. This is accomplished by developing an enhanced architectural schematic that elaborates upon the initial conceptual diagram. The refined representation, presented in Figure 3, explicitly delineates the specific processes enabled by the data management subsystem within the cyber-physical architecture.

A detailed assessment of Figure 3 indicates that the information management subsystem provides comprehensive support for the following operational capacities:

a. **Real-Time Telemetry and Visualization:** The framework ensures the continuous acquisition and instantaneous graphical representation of operational telemetry from both the ventilator simulator and pulmonary emulator, presenting this data within individualized trainee consoles.

b. **Participant Connection State Supervision:** The instructor's console incorporates functionality for tracking the connection status and activity of all active trainees, providing continuous oversight throughout instructional exercises.

c. **Privilege-Based Resource Allocation:** The system enables the instructor to dynamically assign equipment control privileges to specific trainees, facilitating guided interaction with the ventilator simulator while preserving the operational security.

d. **Direct Instructor-Initiated Parameterization:** The architecture permits the instructor to directly configure operational parameters of both the mechanical ventilator and patient emulator, enabling the precise replication of complex clinical presentations.

e. Configuration Parameter Archival: All parameter sets applied to the ventilator simulator and patient module during training sessions are systematically recorded in a secured database, enabling post-session evaluation and performance review.

f. Operational Response Data Capture: The system persistently logs dynamic performance metrics generated during simulator operation, creating a comprehensive dataset for subsequent trainee competency assessment and skill progression analysis.

This rigorous functional modeling ensures that the cyber-physical system satisfies the exacting requirements of remote clinical ventilation training, delivering a resilient and scalable instructional framework.

The implemented communication architecture thereby establishes the necessary infrastructure for deploying a distributed laboratory for mechanical ventilation instruction, incorporating an integrated ventilator simulator and patient emulator to create an authentic clinical training environment. With the system's functional specifications and component interactions fully defined, the development of formal models using Petri net formalism can be commenced.

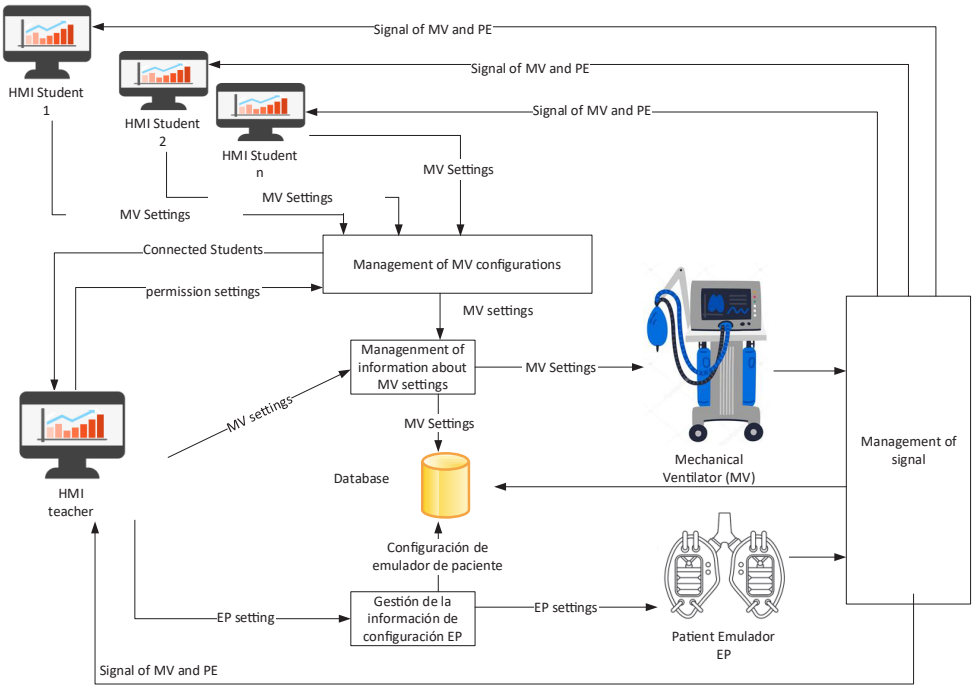

Figure 6. Comprehensive Infrastructure Diagram of the VentyLab Information Management Framework.

Source: own elaboration

Simulation Framework Employing Colored Petri Nets

A computational model was implemented to emulate the dynamic behavior of the communication infrastructure underpinning the teleoperated mechanical ventilation training system. This model is derived from the architectural topology presented in Figure 1 and incorporates the specified system variables with their associated operational logic. The formal representation was constructed using Colored Petri Nets, which provide a rigorous, event-driven methodology for capturing the system's concurrent processes and state-dependent interactions, as depicted in Figure 7.

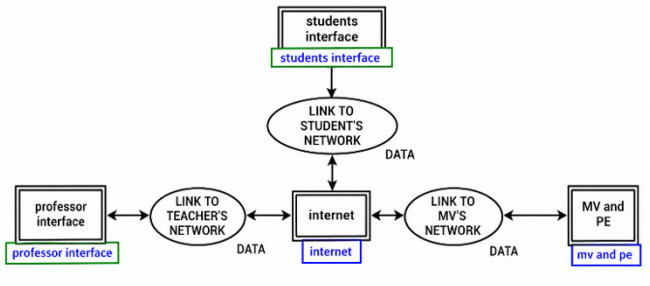

Figure 7. Model in petri nets of the interactions between system actors.

Source: own elaboration

The formulated model is architected around three principal transitions—denoted by double-bordered rectangles—which consolidate the fundamental subnets representing the Professor Interface, the Communication Network, and the integrated Mechanical Ventilator–Patient Emulator (MV–PE) unit, in addition to the Student Interfaces.

The macro-transition designated as "Professor Interface" encapsulates the subnet corresponding to the instructor's control station. This subsystem enables the professor to monitor the roster of active student sessions and grant individual permissions for remote operation of the laboratory equipment. A critical system constraint dictates that configuration and operational control of the mechanical ventilator and patient emulator are exclusively allocated to a single user at any given time, whether the professor or a designated student.

As illustrated in Figure 8, the "Professor Interface" subnet depicts a simulated state wherein three student sessions—identified as sid(1), sid(2), and sid(3)—maintain concurrent connections to the platform. Within this operational context, the professor possesses the capability to delegate specific control privileges to individual students, permitting them to modify ventilator parameters in accordance with a pre-established clinical scenario (represented by the vpe variable for the patient emulator). Conversely, the professor retains the option to directly configure the ventilator and emulator settings via the dedicated "Set up MV and PE" subnet.

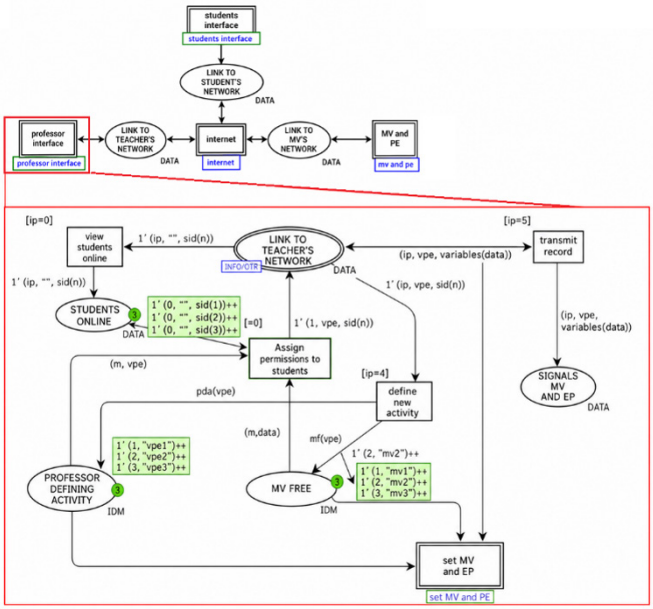

Figure 8. Subnet "professor interface"

Source: own elaboration

The macro-transition designated as "Internet," illustrated in Figure 9, orchestrates the bidirectional exchange of data between the instructional staff, trainees, and the physical hardware components. Within this architecture, control permissions issued by the professor are propagated via the communication network to individual student interfaces, maintaining synchronized state management across the distributed cyber-physical system.

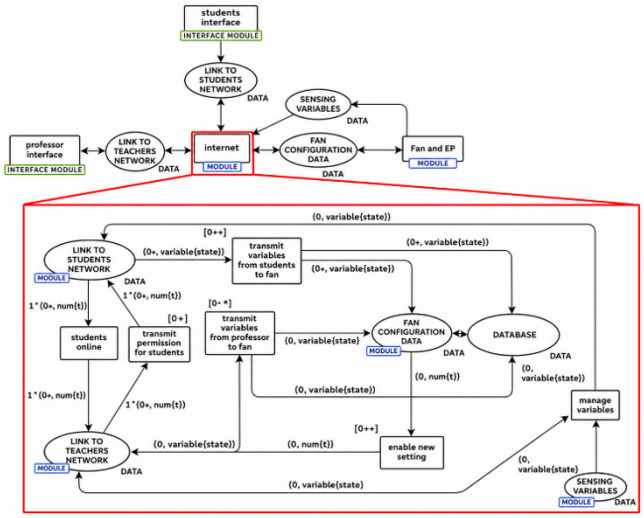

Figure 9. Subnet Internet.

Source: own elaboration

Upon authorization, each trainee configures the mechanical ventilator's operational parameters (represented by the token ip=3). These calibrated values are subsequently transmitted via the communication network to the physical laboratory apparatus, as delineated in Figure 10.

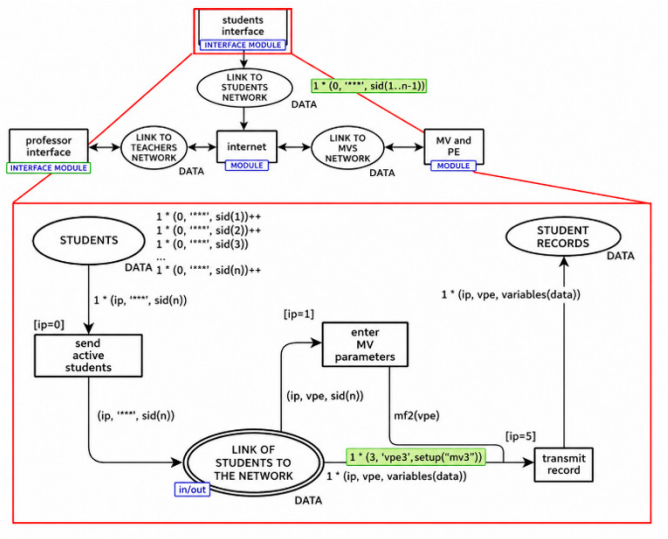

Figure 10. Subnet students interface.

Source: own elaboration

Furthermore, the Student Interface subnet aggregates the variable data streams generated by both the mechanical ventilator and the patient emulator. This functionality ensures all connected trainees can monitor the operational outputs and performance metrics of the ventilator system in real time.

The "MV and PE" subnet processes configuration data originating either from the instructor—when establishing a representative clinical scenario—or from authorized students during training exercises. This initialization phase, parameterized by directives such as set up (mv3), defines the simulated clinical case through variables modeling pulmonary respiratory mechanics, specifically pulmonary compliance and airway resistance.

This input data drives the configuration of the ventilator emulator. The resultant response variables produced by the emulator (e.g., "vmv1", "vmv2", "vmv3") are subsequently broadcast to both the instructor and student interfaces for analytical review, as illustrated in Figures 11 and 12.

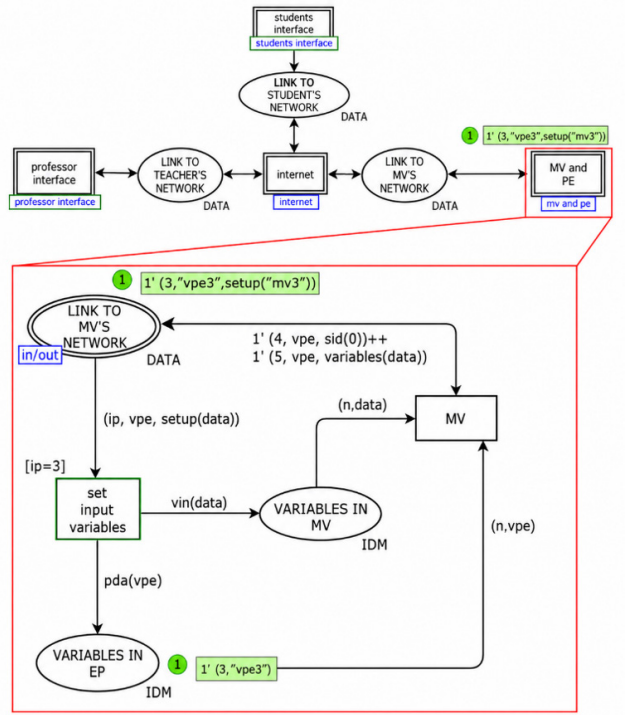

Figure 11. Subnet "MV and PE": Data Input to the Patient Emulator.

Source: own elaboration

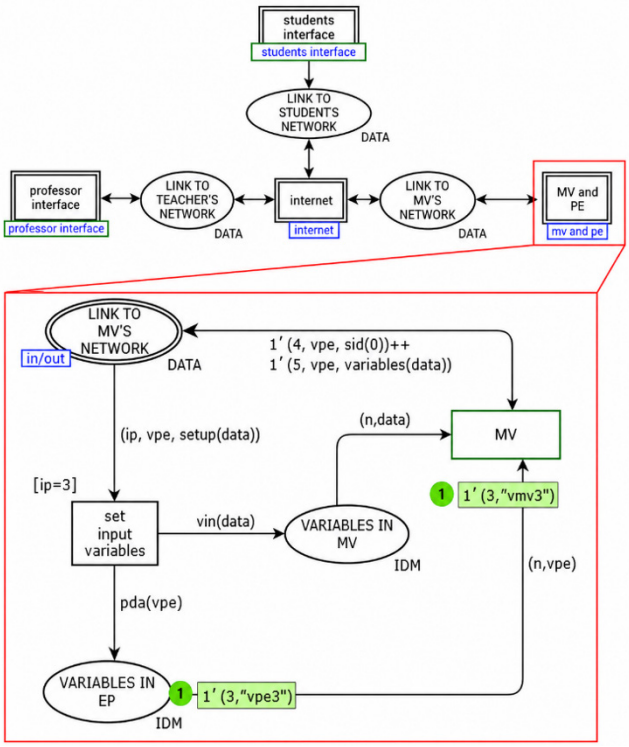

Figure 12. Subnet "MV and EP", EP's response.

Source: own elaboration

Discussion of Results

The constructed model, based on the proposed modular architecture, demonstrates a robust framework for analyzing dynamic interactions within the training ecosystem—specifically between instructional interfaces and physical simulation devices. This methodology accurately replicates operational conditions encountered in clinical mechanical ventilation scenarios.

The application of Colored Petri Nets afforded a detailed yet integrated representation of system functionality. This abstraction level enables precise identification of subsystem interdependencies, supporting both operational visualization and prediction of potential system constraints. The explicit modeling of permission structures, data acquisition pathways, and equipment responses facilitates the simulation of diverse clinical presentations, thereby enhancing training realism and educational effectiveness.

The architecture's modular nature provides significant adaptability. Modifications to specific components—such as trainee interaction protocols or device response algorithms—can be implemented without disrupting overall system integrity. This flexibility is particularly valuable in medical education, where evolving clinical demands require responsive training methodologies.

The implementation of bidirectional data exchange between interfaces and physical simulators enables real-time performance feedback for both instructors and trainees. This capability not only improves simulation fidelity but also supports comprehensive competency assessment during remote training sessions.

Future Work:

While the proposed model demonstrates a robust architectural and formal representation of the teleoperated training system, several avenues remain open for future development. From a technical perspective, it is essential to conduct stress and scalability tests of the communication network to evaluate system performance under high concurrency conditions, including latency analysis and maximum supported number of simultaneous users. These experiments would provide quantitative insights into the operational limits of the platform in real-world deployment scenarios.

Additionally, future work should incorporate a pedagogical validation of the system through controlled pilot studies involving medical trainees. Such studies would enable the assessment of learning outcomes, user interaction patterns, and the effectiveness of the platform in improving clinical decision-making skills in mechanical ventilation. The integration of learning analytics could further support the objective measurement of user performance and skill acquisition over time.

Conclusions

This research establishes a methodologically rigorous framework that integrates remote laboratory capabilities with digital learning environments through advanced information technologies. The cyber-physical model, developed using Colored Petri Nets, ensures precise specification of both architectural components and dynamic interactions between human operators and physical simulation devices.

Through systematic identification and modeling of operational parameters, the framework accurately represents all aspects of remote ventilation training—including instructional supervision, controlled trainee access, and clinical scenario emulation through parameterized respiratory mechanics.

The proposed architecture enhances system adaptability and scalability, providing a foundation for continuous refinement in response to evolving educational requirements and clinical protocols. This work holds immediate relevance for advancing clinical training in mechanical ventilation—particularly crucial in pandemic contexts and future scenarios requiring decentralized educational solutions.

In summary, this investigation establishes a comprehensive technical model that bridges theoretical simulation and practical application in medical education, creating new possibilities for high-fidelity remote training systems while strengthening clinical preparedness in ventilator management.

Acknowledgments

The author acknowledges Universidad del Valle for the financial support that enabled this research.

References

[1] J. D. Allen, "Human physiology - the basis of medicine," *Ulster Med. J.*, vol. 77, no. 3, p. 216, Sep. 2008. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2604485/

[2] Forum of International Respiratory Societies and European Respiratory Society, *The Global Impact of Respiratory Disease*. Sheffield, UK: European Respiratory Society, 2017, ISBN: 978-1-84984-087-3. [3] Global Asthma Network, *The Global Asthma Report 2014*. Auckland, New Zealand: Global Asthma Network, 2014, ISBN: 978-0-473-29125-9.

[4] P. G. J. Burney, J. Patel, R. Newson *et al.*, "Global and regional trends in COPD mortality, 1990–2010," *Eur. Respir. J.*, vol. 45, no. 5, pp. 1239–1247, May 2015. https://doi.org/10.1183/09031936.00142414

[5] N. Petrosillo, G. Viceconte, O. Ergonul *et al.*, "COVID-19, SARS and MERS: Are they closely related?" *Clin. Microbiol. Infect.*, vol. 26, no. 6, pp. 729–734, Jun. 2020. https://doi.org/10.1016/j.cmi.2020.03.026[6] N. Karamolegkos *et al.*, "Patient emulator: A tool for testing mechanical ventilation therapies," in *Proc. 38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, IEEE, 2016. https://doi.org/10.1109/EMBC.2016.7591683

[7] G. Avendaño, F. Toncio, and P. Fuentes, "Design and construction of a real simulator for calibrating lung servo-ventilators," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. (EMBS)*, IEEE, 2010. https://doi.org/10.1109/IEMBS.2010.5626175

[8] AQAI, "TestChest lung simulator," AQAI GmbH. [Online]. Available: https://www.aqai.eu/en/products-service/development/testchest.php

[9] Michigan Instruments, "Lung simulators," Michigan Instruments. [Online]. Available: https://www.michiganinstruments.com/lung-simulators/

[10] R. Pasteka *et al.*, "Electro-mechanical lung simulator using polymer and organic human lung equivalents for realistic breathing simulation," *Sci. Rep.*, vol. 9, no. 1, art. 19778, pp. 1–12, 2019. https://doi.org/10.1038/s41598-019-56176-6

[11] S. Heili-Frades, G. Peces-Barba, and M. J. Rodríguez-Nieto, "Design of a lung simulator for teaching lung mechanics in mechanical ventilation," *Arch. Bronconeumol. (Engl. Ed.)*, vol. 43, no. 12, pp. 674–679, 2007. https://doi.org/10.1016/S1579-2129(07)60154-2

[12] MA Horvath *et al.* , "Un simulador respiratorio robótico blando organosintético", *APL Bioengineering* , vol. 4, n.º 2, pág. 026108, junio de 2020, https://doi.org/10.1063/1.5140760

[13] Laerdal Medical, "ASL 5000 lung solution," Laerdal Medical. [Online]. Available: https://laerdal.com/de/information/shortcuts-and-redirects/ASL5000-LungSolution/

[14] R. Paštěka and M. Forjan, "Actively breathing mechanical lung simulator development and preliminary measurements," in *EMBEC & NBC 2017*, Singapore: Springer, 2017, pp. 751–754. https://doi.org/10.1007/978-981-10-5122-7_188

[15] F. Bautsch, G. Männel, and P. Rostalski, "Development of a novel low-cost lung function simulator," *Curr. Dir. Biomed. Eng.*, vol. 5, no. 1, pp. 557–560, 2019. https://doi.org/10.1515/cdbme-2019-0140

[16] S. Heili-Frades, G. Peces-Barba, and M. J. Rodríguez-Nieto, "Diseño de un simulador de pulmón para el aprendizaje de la mecánica pulmonar en ventilación mecánica," *Arch. Bronconeumol.*, vol. 43, no. 12, pp. 674–679, 2007. https://doi.org/10.1157/13112966 [17] H. S. Johar and K. Yadav, "DRDO's portable low-cost ventilator: 'DEVEN'," *Trans. Indian Natl. Acad. Eng.*, vol. 5, no. 2, pp. 365–371, 2020. https://doi.org/10.1007/s41403-020-00143-5

[18] J. Saiful *et al.*, "Design and implementation of ventilator for breathing apparatus," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 990, no. 1, art. 012007, 2020. https://doi.org/10.1088/1757-899X/990/1/012007

[19] B. El Majid *et al.*, "Preliminary design of an innovative, simple, and easy-to-build portable ventilator for COVID-19 patients," *Euro-Mediterr. J. Environ. Integr.*, vol. 5, art. 57, pp. 1–4, 2020. https://doi.org/10.1007/s41207-020-00163-1

[20] J. M. Knorr *et al.*, "Design and performance testing of a novel emergency ventilator for in-hospital use," *Can. J. Respir. Ther.*, vol. 56, art. 42, 2020. https://doi.org/10.29390/cjrt-2020-023

[21] A. Darwood *et al.*, "The design and evaluation of a novel low-cost portable ventilator," *Anaesthesia*, vol. 74, no. 11, pp. 1406–1415, 2019. https://doi.org/10.1111/anae.14726

[22] A. Vasan *et al.*, "MADVent: A low-cost ventilator for patients with COVID-19," *Med. Devices Sens.*, vol. 3, no. 4, art. e10106, 2020. https://doi.org/10.1002/mds3.10106

[23] F. J. Vivas Fernández *et al.*, "ResUHUrge: A low cost and fully functional ventilator indicated for application in COVID-19 patients," *Sensors*, vol. 20, no. 23, art. 6774, 2020. https://doi.org/10.3390/s20236774

[24] J. Tharion *et al.*, "Rapid manufacturable ventilator for respiratory emergencies of COVID-19 disease," *Trans. Indian Natl. Acad. Eng.*, vol. 5, pp. 373–378, 2020. https://doi.org/10.1007/s41403-020-00118-6 [25] A. Petsiuk *et al.*, "Partially RepRapable automated open source bag valve mask-based ventilator," *HardwareX*, vol. 8, art. e00131, 2020. https://doi.org/10.1016/j.ohx.2020.e00131.

[26] S. H. Sojar *et al.*, "Titration of parameters in shared ventilation with a portable ventilator," *Respir. Care*, vol. 66, no. 5, pp. 758–768, 2021. https://doi.org/10.4187/respcare.08446

[27] C. Galbiati *et al.*, "Mechanical Ventilator Milano (MVM): A novel mechanical ventilator designed for mass scale production in response to the COVID-19 pandemics," *medRxiv*, preprint, 2020. https://doi.org/10.1101/2020.03.24.20042234

[28] J. Živčák *et al.*, "A portable BVM-based emergency mechanical ventilator," in *Proc. 19th IEEE World Symp. Appl. Mach. Intell. Informatics (SAMI)*, IEEE, 2021. https://doi.org/10.1109/SAMI50585.2021.9378620 [29] S. M. Mirvakili, D. Sim, and R. Langer, "Inverse pneumatic artificial muscles for application in low-cost ventilators," *Adv. Intell. Syst.*, vol. 3, no. 1, art. 2000200, 2021. https://doi.org/10.1002/aisy.202000200

[30] S. Mora, F. Duarte, and C. Ratti, "Can open source hardware mechanical ventilator (OSH-MVs) initiatives help cope with the COVID-19 health crisis? Taxonomy and state of the art," *HardwareX*, vol. 8, art. e00150, 2020. https://doi.org/10.1016/j.ohx.2020.e00150

[31] R. M. Kacmarek, "The mechanical ventilator: Past, present, and future," *Respir. Care*, vol. 56, no. 8, pp. 1170–1180, 2011. https://doi.org/10.4187/respcare.01420

[32] J. Chang *et al.*, "Masi: A mechanical ventilator based on a manual resuscitator with telemedicine capabilities for patients with ARDS during the COVID-19 crisis," *HardwareX*, vol. 9, art. e00187, 2021. https://doi.org/10.1016/j.ohx.2021.e00187

[33] A. Takeuchi *et al.*, "Interactive simulation system for artificial ventilation on the internet: Virtual ventilator," *J. Clin. Monit. Comput.*, vol. 18, no. 5, pp. 353–363, 2004. https://doi.org/10.1007/s10877-005-6268-0

[34] N. Ambrosino *et al.*, "Tele-monitoring of ventilator-dependent patients: A European Respiratory Society Statement," *Eur. Respir. J.*, vol. 48, no. 3, pp. 648–663, 2016. https://doi.org/10.1183/13993003.01721-2015

[35] Y. Li *et al.*, "A Petri net based model for a cloud healthcare system," in *Proc. Chinese Control and Decision Conf. (CCDC)*, IEEE, 2018. https://doi.org/10.1109/CCDC.2018.8407805 [36] S. Mtibaa and M. Tagina, "An automated Petri-net based approach for change management in distributed telemedicine environment," arXiv preprint arXiv:1210.6076, 2012. [Online]. Available: https://arxiv.org/abs/1210.6076

[37] I. Ruiz, J. Contreras, and J. Garcia, "Towards a physical rehabilitation system using a telemedicine approach," *Comput. Methods Biomech. Biomed. Eng.: Imaging Vis.*, vol. 9, no. 4, pp. 354–363, 2020. https://doi.org/10.1080/21681163.2020.1795929

[38] F. J. Mejia, J. I. Garcia, and C. E. Hurtado, "Model-based design of body motion sensing technology using systems modeling language and coloured Petri nets," in *Proc. IEEE Int. Conf. E-health Netw. Appl. Serv. (HealthCom)*, IEEE, 2019. https://doi.org/10.1109/HealthCom46333.2019.9009430

[39] K. Collante, "Guía completa para crear tu diagrama de infraestructura," Hackmetrix Blog, Aug. 19, 2021. Accessed: Nov. 19, 2021. [Online]. Available: https://blog.hackmetrix.com/como-hacer-un-diagrama-de-infraestructura/

[40] J. M. Rosen *et al.*, "Telehealth's new horizon: Providing smart hospital-level care in the home," *Telemed. e-Health*, vol. 27, no. 11, pp. 1215–1224, 2021. https://doi.org/10.1089/tmj.2020.0448

[41] A. M. Valencia, I. Ruiz, J. I. García, and A. Galvis, "Design of a patient simulator for clinicians training in mechanical ventilation: SimVep," *J. Med. Eng. Technol.*, vol. 49, no. 3, pp. 79–92, 2025. https://doi.org/10.1080/03091902.2025.2484672

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.24849

INVESTIGACIÓN

Metrics for the evaluation of documentation format in agile software projects

Métricas para la evaluación del formato de la documentación en proyectos de software ágil

Juan Carlos Narváez [1] y César Jesús Pardo Calvache [2]

Fecha de Recepción: 12 de noviembre de 2025 **Fecha de Aceptación**: 24 de febrero de 2026

Cómo citar: J.C. Narváez, C.J. PArdo Calvacho, «Metrics for evaluation of documentation format in agile software projects», *Tecnura*, vol. 30, n.° 88, jun. 2026. 38–57. https://doi.org/10.14483/22487638.24849

Abstract

Objective: This paper proposes a metrics model for assessing and making documentation debt visible in agile software development, with a specific focus on the Format dimension.
Methodology: Based on a systematic literature review, the study identified critical risks and applied the Goal-Question-Metric (GQM) paradigm to design indicators. Both subjective metrics, based on perception, and objective metrics, based on structural analysis, were defined to evaluate attributes such as readability, conciseness, and clarity.
Results: A five-dimensional architecture was defined (Structure, Format, Usability, Correlation, and Auditability) and specific metrics were developed for the Format dimension, addressing readability, conciseness, and clarity. These metrics integrate subjective user evaluation with objective structural complexity indicators—such as Average Words per Sentence (PPO)—to quantify risks associated with code misunderstanding and communication failures.
Conclusions: Format deficiencies can give rise to serious risks, including communication failures. The combined use of subjective and objective metrics is essential for a holistic diagnosis, transforming documentation quality into a measurable engineering attribute that can be managed proactively
Keywords: Documentation Debt, Metrics, Agile software development, Technical Debt, Software Quality

Resumen

Objetivo: este trabajo propone un modelo de métricas para evaluar y visibilizar la deuda de la documentación en el desarrollo ágil de software, enfocándose específicamente en la dimensión de Formato.
Métodología: a partir de una revisión sistemática de literatura, se identificaron riesgos críticos y se aplicó el paradigma Goal-Question-Metric (GQM) para diseñar indicadores. Se definieron métricas subjetivas (basadas en percepción) y objetivas (análisis estructural) para evaluar atributos como legibilidad, concisión y claridad.

1 Magister en computación. Docente en la Universidad del Cauca. Email: juanarvaez@unicauca.edu.co
2 PhD. en Informática. Docente en la Universidad del Cauca. Email: cpardo@unicauca.edu.co

Resultados: se definió una arquitectura de cinco dimensiones (Estructura, Formato, Usabilidad, Correlación y Auditabilidad) y se desarrollaron métricas específicas para el Formato, abordando la Legibilidad, Concisión y Claridad. Estas métricas integran la evaluación subjetiva del usuario con indicadores objetivos de complejidad estructural, como el Promedio de Palabras por Oración (PPO), para cuantificar riesgos asociados a la incomprensión del código y fallas de comunicación.
Conclusiones: las deficiencias de formato son causantes de riesgos graves como fallas de comunicación. La sinergia entre métricas subjetivas y objetivas es indispensable para un diagnóstico holístico, transformando la calidad documental en un atributo de ingeniería medible para su gestión proactiva.
Palabras clave: Deuda de la Documentación, Métricas, Desarrollo Ágil de Software, Deuda Técnica, Calidad de Software

Introduction

High-quality documentation is widely regarded as a strategic resource in software engineering because it is essential for understanding a system holistically and maintaining it over the long term [1, 2]. However, there is a clear gap between its recognized importance and its practical implementation: producing pragmatic and effective documentation remains a persistent challenge in the field [3]. This problem is exacerbated in the context of agile approaches where, despite their aim of improving value delivery in short development cycles [4], the principle of documenting only what is necessary is often misinterpreted as a justification for relegating software documentation to a secondary role [5, 6, 7].

Far from being a harmless omission, this practice creates an insidious type of technical debt known as documentation debt [8]. This concept does not simply refer to a lack of text, but to an ecosystem of deficient information characterized characterized by scarce, inconsistent, or outdated artifacts. The fundamental problem with this type of technical debt is its invisible nature: it accumulates silently until its consequences become prohibitively expensive [4, 8].

The progressive accumulation of technical debt in software documentation increases the likelihood of risks that compromise project viability, maintenance costs, the efficiency of onboarding new team members, and overall software quality [9]. As a result, the personnel involved in building a software system remain trapped in a cycle of reactive management, facing negative consequences only once they have reached a critical state. This research is therefore motivated by the need for a formal mechanism that allows the level of technical debt in software documentation to be visualized, measured, and controlled.

This paper responds to that need by proposing a structured metrics model designed to quantify the likelihood of risks associated with software documentation. The model seeks to transform an abstract and subjective problem—such as poor documentation—into concrete and actionable indicators. It addresses Documentation Debt from five fundamental dimensions: Structure, Format, Usability, Correlation, and Auditability. This allows organizations not only to identify weaknesses but also to justify the

allocation of resources and proactively manage the quality of their knowledge assets. This article introduces the general architecture of the model and, as an initial result, details the set of metrics designed for the Format dimension [10].

The remainder of the article is organized as follows. Section 2 describes the five dimensions of documentation and their characteristics. Section 3 presents the methodology followed for the construction of the model. Section 4 presents the metrics of the Format dimension. Section 5 discusses the results. Section 6 presents the conclusions and future work.

Dimensions and Characteristics of Documentation

To evaluate documentation debt systematically, a hierarchical model is proposed that organizes documentation quality into two levels: **Dimensions**, which represent the main evaluation perspectives for a documentation artifact, and **Characteristics**, which correspond to the specific and measurable attributes within each dimension.

As shown in Figure 1, the model comprises five dimensions—Structure, Format, Usability, Correlation, and Auditability—which group a total of seventeen quality characteristics, providing a comprehensive basis for diagnosing documentation quality and identifying areas in which debt may accumulate.

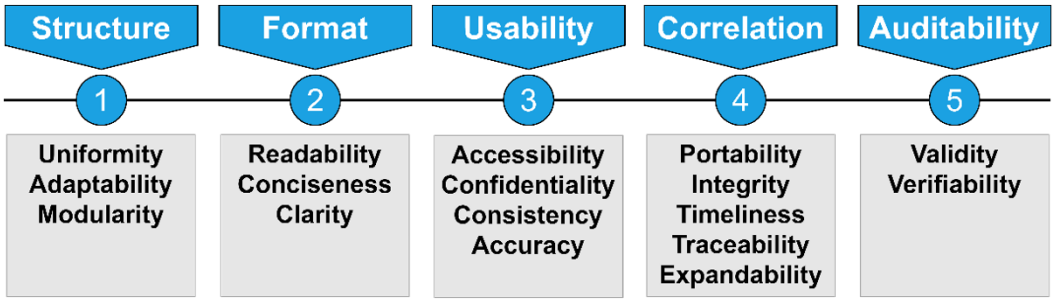

Figure 1. Dimensions and characteristics of software documentation

Source: own elaboration.

The dimensions and characteristics associated with each are described below.

Structure

Following Koznov [11], this dimension focuses on the logical distribution of documentation content to enable effective understanding and use. Each component—indexes, chapters, glossary, images, tables, error descriptions and solutions, usage instructions, and references—must have a specific purpose

and be coherently related, either internally (with parts of the same artifact) or externally (with other artifacts), to maintain the overall meaning of the document. Its characteristics are:

- **Uniformity:** Consistency of the information within the artifact, ensuring that there are no conflicts, contradictions, or duplications, and maintaining coherence in its format, structure, storage, and updating [11, 12].

- **Adaptability:** The artifact's ability to evolve and remain relevant as the needs and requirements of the project change [13].

- **Modularity:** The capacity to divide an artifact into independent, cohesive sections with specific objectives, facilitating the understanding of specific system details without requiring review of the entire document [1].

Format

The Format dimension focuses on the visual presentation, language, and grammar of the content. Although its deficiencies may go unnoticed in the short term thanks to the team's tacit knowledge, they seriously affect the future understanding of the information in the long term [1, 10]. The characteristics of this dimension are:

- **Readability:** The ease of reading an artifact, which can be hindered by abstract, overly technical, or overloaded information, or by the presence of typographical errors. This characteristic evaluates the effort required by the reader to access the information and achieve the purpose for which the document was created [14].

- **Conciseness:** The ability to use only the information strictly necessary to explain the system without sacrificing accuracy. The presence of useless or redundant sections makes the document cumbersome and incomprehensible [1].

- **Clarity:** The ability of content to be understandable and intelligible without generating doubts. It requires appropriate language and simple wording that allows information to be found quickly without the need to re-read, adapting the structure and visual design to the user's needs [1].

Usability

The Usability dimension assesses how easily a reader can obtain the information necessary to meet their immediate objectives. This perspective analyzes the effective use of documentation, considering factors such as navigation, format, structure, and preservation mechanisms that condition access [15]. Its characteristics are:

- **Accessibility:** The ability of the documentation to be located and operational when needed, allowing for its retrieval and reading according to the user's availability and access level [12].

- **Confidentiality:** Based on the ISO 27001 standard, this ensures that documentation is available only to authorized personnel or processes, requiring visible classification of artifacts —such as public, internal, or restricted.

- **Consistency:** The ability of documentation to avoid discrepancies between its content and the actual operation of the system. It depends on the uniformity and integrity of the content and is evaluated through elements such as the level of formality, semantics, visual content, and organization [12, 16, 17].

- **Accuracy:** The ability of the artifact to convey accurate and unambiguous information that faithfully reflects the actual state of the system, given that inaccurate documentation can be more harmful than its absence [15, 18].

Correlation

The Correlation dimension refers to the correspondence required between the software system and its documentation. Its main objective is to ensure consistency between recorded information and the actual behavior of the system, keeping artifacts up to date whenever changes occur. Its characteristics are:

- **Portability:** The quality that allows documentation to be transferred efficiently between different technological or operational environments, using standard formats that ensure independence and interoperability [12].

- **Integrity:** The degree to which the documentation remains correct and complete after changes to the system, retaining sufficient information to support development, maintenance, and use tasks [12].

- **Timeliness:** The degree to which documentation remains current throughout the software lifecycle, depending on adequate traceability to ensure the simultaneous evolution of the system and its documents [12].

- **Traceability:** The record of the artifact's evolution, allowing identification of the context of changes—where, when, who, and why. This facilitates tracking of modifications to maintain consistency with the system and understand dependencies between artifacts [16].

- **Expandability:** The ability to add or modify information in an artifact—increasing its size or scope—without negatively affecting other characteristics, which is essential for system evolution and maintenance [15].

Auditability

The Auditability dimension involves inspecting and verifying documentation with respect to software behavior and established review criteria. Documentation must serve as eliable evidence of the procedures, actions, and decisions taken during development. Its characteristics are:

- **Validity:** The ability to prove the authenticity, veracity, legality, and reliability of information through mechanisms such as signatures and seals, allowing agreements to be formalized and the relevance of the content to be certified [1, 16].

- **Verifiability:** The ability to corroborate whether the documentation provides accurate and reliable information, avoiding conflicts with other artifacts. It relies on readability and structure to ensure effective review, since incorrect or unverified information can lead to errors [1, 16].

Model construction methodology

The construction of the model began by consolidating empirical evidence through systematic literature mapping and causal analysis of documentation debt [19]. This process made it possible to derive and formulate the associated risks, design the overall architecture, and define the metrics under the Goal-Question-Metric (GQM) paradigm.

Risk definition process

To ensure that the model addresses significant Documentation Debt issues in agile software development, a formal risk identification process was carried out in three phases.

Phase 1 (Empirical Evidence Collection) consolidated the findings of a systematic literature mapping on documentation debt in agile software development conducted in 2022 [20], which provided the knowledge base for designing the metrics model.

Phase 2 (Causal Analysis), involved the extraction and analysis of the most frequently reported factors and consequences in the literature. A total of 45 causes and 42 effects of documentation debt were identified, which were then refined to remove redundancies and consolidate the main concepts.

Phase 3 (Synthesis and Risk Formulation), used the refined causes and effects to formulate 15 specific documentation risks. Each risk was formulated following a structure inspired by the ISO 31000 standard, detailing four elements: the affected actor, the nature of the risk, its root cause, and the potential impact.

Table 1 presents the risks defined during this process according to the following format:

For (who is affected by the risk) + **there is a risk** (specification of the risk) + **due to** (one or more causes of the risk) + **this may** (the consequences of the risk materializing)

Table 1. *Documentation risks in agile software development*

Id	Risk description
R1	For development and maintenance teams, there is a risk of misunderstanding the source code in the future, due to a lack of code comments and technical documentation that is scarce, incomprehensible, outdated, or non-existent. This may affect the maintainability and modifiability of the system, teamwork, knowledge transfer, and problem solving.
R2	For administrators and end users, there is a risk that the system will be highly vulnerable because its documentation does not correctly describe its architecture, design, functionalities, and restrictions. This may hinder the understanding of risks and threats, impede the implementation or improvement of security practices, and increase the complexity of incident management and response.
R3	For the company, there is a risk that the system will be very difficult to maintain in the future because its documentation does not support an adequate understanding of its operation, architecture, design, and the decisions made during its construction. This may affect code refactoring, decrease consistency in system development, hinder the traceability of changes, and increase the effort required to identify, understand, and resolve incidents.
R4	For the company, there is a risk that the system will be of poor quality because its documentation does not provide clear and accurate information for understanding its design, architecture, and operation. This may hinder quality control, scalability and maintainability, knowledge transfer to new staff, and increase dependence on the personnel who originally participated in its development. It may also cause dissatisfaction among stakeholders and damage the company's business relationships, reducing competitiveness.
R5	For the company, there is a risk of rework during system development because the documentation is confusing, incomplete, inconsistent, or outdated. This may lead to misunderstandings in the interpretation of requirements, increase the likelihood of errors, and cause important information to be omitted during design or implementation, resulting in rework and delivery delays.
R6	The company faces the risk of progressively accumulating unmanageable levels of technical debt due to unclear documentation, the absence of best practices and standards, a lack of details on dependencies and risks, and non-existent or outdated design and architecture documentation. This may lead to low-quality software resulting from rushed or incorrect decisions.
R7	The company faces the risk of having informal development and quality control processes because the guidelines to be followed at each stage are not clearly documented. This may lead to a lack of uniformity and consistency in the execution, monitoring, and control of processes, and increase the likelihood of losing valuable knowledge, as processes are executed based on intuition rather than documented guidelines.
R8	The company faces the risk of not improving its processes because the documentation does not adequately record how they should be executed to be efficient, consistent, and improve the quality of operations. This may affect the visibility of processes, limit analysis and performance measurement, increase uncertainty, and constrain the capacity for continuous improvement.
R9	For the deployment team, there is a risk that the system cannot be correctly implemented in their environment because the documentation lacks precise information on its operation and how it should be installed, configured, and used. This may affect implementation planning, lead to errors or omissions during the process, and hinder the functioning of the system after deployment
R10	For the company, there is a risk of losing the knowledge acquired by the development team due to poor, incomplete, or non-existent documentation of design decisions, functionalities, configuration, integrations, requirements management, problem solutions, and lessons learned. This may increase dependence on the tacit knowledge of certain team members and reduce team productivity
R11	The development team faces the risk of implementing system requirements incorrectly due to ambiguous documentation. This may lead to requirements being misinterpreted, inconsistent, or contradictory, causing confusion during system construction and increasing the likelihood of omitting important details in functionalities, constraints, business rules, or non-functional requirements.
R12	For the company, there is a risk of not effectively integrating new staff, because the documentation does not support an adequate understanding of the system, its status, its operation, the requirements it must meet, its design, and its architecture. This may delay the adaptation of new personnel and their ability to fully contribute to the team's objectives.

Id	Risk description
R13	For the quality team, there is a risk that it will be very difficult to determine how to test the system because the documentation presents incomplete information on requirements and does not clearly explain the acceptance criteria. This may lead to test cases that do not cover all relevant scenarios, inadequate defect management, and loss of traceability.
R14	The company faces the risk of losing the ability to adequately track the evolution and changes made over time to documentation artifacts due to the deficiency or absence of version control. This may affect version history management, make it difficult to understand the context of modifications, and lead to confusion and loss of information
R15	For the development team, there is a risk of communication problems arising because the documentation is ambiguous, unclear, or outdated in its description of the system, its functionalities, and its conditions of use. This may lead to misinterpretations, misunderstandings, and confusion in internal and external communications, affecting collaboration and problem-solving.

Source: own elaboration.

To contextualize the metrics, risks R1, R4, and R15 were selected due to their high relevance to the Format dimension. These risks address issues such as code comprehension, low system quality, and communication failures, which directly affect the clarity, readability, and accuracy of the documentation. This selection allowed specific indicators to be defined to measure their impact on software viability.

Risk and dimension mapping

Once the risks had been identified, the next step was to establish their relationship with the dimensions to validate the conceptual coverage of the model and understand the multidimensional nature of the risks. Three steps were taken:

First, **a critical analysis and semantic deconstruction of each risk** was performed to extract its components: the affected actors (those who suffer the consequences), the nature of the risk (the central negative event), the root causes (identifying adjectives that denote documentary deficiencies such as "ambiguous" or "scarce"), and the potential impact. The objective was to obtain a set of concrete descriptors that directly relate each risk to specific failures or deficiencies in the documentation artifacts.

Second, **the link between each risk and the documentation quality characteristics was established** by comparing the previously extracted descriptors with the definitions in the model. The fundamental criterion was the existence of a direct correspondence between the problem described in the risk (cause or impact) and the specific quality attribute.

Third, **the affected characteristics were grouped into the corresponding dimensions** of the model. The criterion established was to associate a risk with a dimension if it affected at least one of its characteristics, producing a multidimensional impact profile for each risk. For example, risk R1 was associated with four dimensions, while R3 covered all five.

Table 2 presents the resulting mapping matrix, which summarizes the interrelationship between risks and the dimensions of the model.

Table 2. *Mapping of risks to documentation with the dimensions of the model.*

Risk	Structure	Format	Usability	Correlation	Auditability
R1	X	X	X	X	
R2		X	X		X
R3	X	X	X	X	X
R4		X	X		X
R5		X	X	X	X
R6	X	X	X	X	
R7	X	X	X	X	X
R8		X	X		
R9			X	X	X
R10	X		X	X	X
R11	X	X	X		X
R12		X	X		
R13	X	X	X	X	X
R14	X		X	X	X
R15	X	X	X		
Total	9	12	15	9	10

Source: own elaboration.

To illustrate the mapping process described above, the analysis performed for risk R1 is detailed below:

Definition of risk R1 (see Table 1): For development and maintenance teams, there is a risk of misunderstanding the system's source code in the future, because it has no comments to support the explanation of its intent and the technical documentation is scarce, incomprehensible, outdated, or non-existent. This may affect the maintainability and modifiability of the system, teamwork, knowledge transfer to new staff, and problem solving.

In this first step, the **causes** were identified (scarce, incomprehensible, outdated, or nonexistent documentation), the **central problem** was defined (the inability to correctly understand the source code), and the **impact** was determined (negative effects on system maintainability and knowledge transfer).

In the second step, direct links were established between the textual components of R1 and the quality characteristics. Phrases such as "failure to understand correctly" or "incomprehensible" indicate difficulty assimilating information, related to **Clarity** and **Readability**. Words such as scarce or non-existent correspond to a deficiency in **Integrity**, while outdated indicates failures in **Timeliness** and **Accuracy**.

Incomprehensibility was associated with a lack of Uniformity, and difficulties in maintainability or knowledge transfer were identified as **Modularity** problems.

In the third step, the identified characteristics were grouped with their respective dimensions. Uniformity and Modularity belong to the Structure dimension; Clarity and Readability correspond to Format; Accuracy is located in Usability; and Integrity and Timeliness are part of Correlation.

As a result, risk R1 would impact on the Structure, Format, Usability, and Correlation dimensions, as shown in Table 2.

The analysis of risk distribution (Table 2) was decisive in defining the scope of the research. Although the Usability dimension emerged as the most cross-cutting—impacted by all 15 risks—the initial study was strategically focused on the Format dimension, based on several considerations.

The Format dimension is critical, as it is the second most affected, directly linked to 12 of the 15 identified risks. Risks such as source code misunderstanding (R1), low system quality (R4), and critical communication failures (R15) are strongly associated with the presentation and language of the documentation. This suggests that improving Readability, Conciseness, and Clarity can substantially help mitigate serious project risks.

Beyond its frequency of impact, the Format dimension is foundational to documentation quality: if documentation lacks Readability or Clarity, it fails to fulfill its communicative purpose, regardless of its visual structure. Therefore, addressing format deficiencies is an indispensable step toward enabling and enhancing quality across the rest of the model.

Furthermore, the Format dimension allows for direct identification of problems and the implementation of concrete corrective measures. Problems in this area are tangible and observable, manifesting in specific elements such as excessively long sentences or the absence of visual aids. This advantage is reflected in the metrics developed (Section 4), which integrate objective indicators derived from linguistic and structural analysis (IFKE, IEC, IPP, PPO, PFO, ICP) with subjective assessments of user perception (PLD, PCD, PCLD). This combination provides a robust diagnosis that not only detects whether a problem exists but also identifies its structural causes, facilitating the implementation of specific and measurable improvements.

In conclusion, given the criticality, foundational role, and diagnostic tangibility of the Format dimension, this article focuses on the specification and discussion of its metrics. This approach seeks to establish a coherent methodology and provide concrete results that serve as a starting point for future research on the remaining dimensions.

General architecture of the model and use of GQM

Once the risks were established, the relational architecture of the model was designed (Figure 3), incorporating the dimensions and characteristics described above. Under the Goal-Question-Metric (GQM) paradigm [21] (Figure 2), each characteristic is associated with a group of specific metrics: metrics for **direct measurement** of objective attributes and metrics for **subjective perception** through surveys.

The GQM paradigm ensures that metrics are not arbitrary, but rather aligned with measurement objectives and the questions that evaluate their achievement. It operates at three levels:

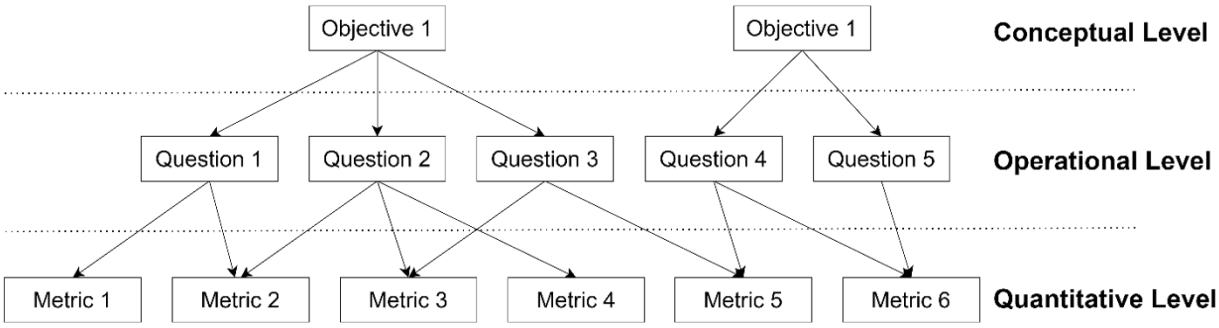

Figure 2. Basic structure of the GQM paradigm

Source: Basili et al. [21].

Conceptual Level (Goal): Defines clear and strategically aligned measurement objectives, specifying their purpose, perspective, object of analysis, and context.

Operational Level (Questions): Breaks down each objective into specific questions that characterize the object of study and suggests the information needed to determine whether the goal is being achieved.

Quantitative Level (Metric): Defines specific metrics to answer these questions. They can be objective —such as lines of code— or subjective —level of satisfaction— and must be clearly linked to the operational questions.

The five dimensions that make up the architecture are: (i) Structure, which focuses on the logical organization and distribution of content; (ii) Format, which evaluates the visual presentation, language, and grammar used; (iii) Usability, which measures the ease with which the reader can extract the information necessary for their objectives; (iv) Correlation, which examines the consistency and timeliness of the documentation with respect to the system it describes; and (v) Auditability, which determines the artifact's ability to be systematically inspected and verified as a reliable record.

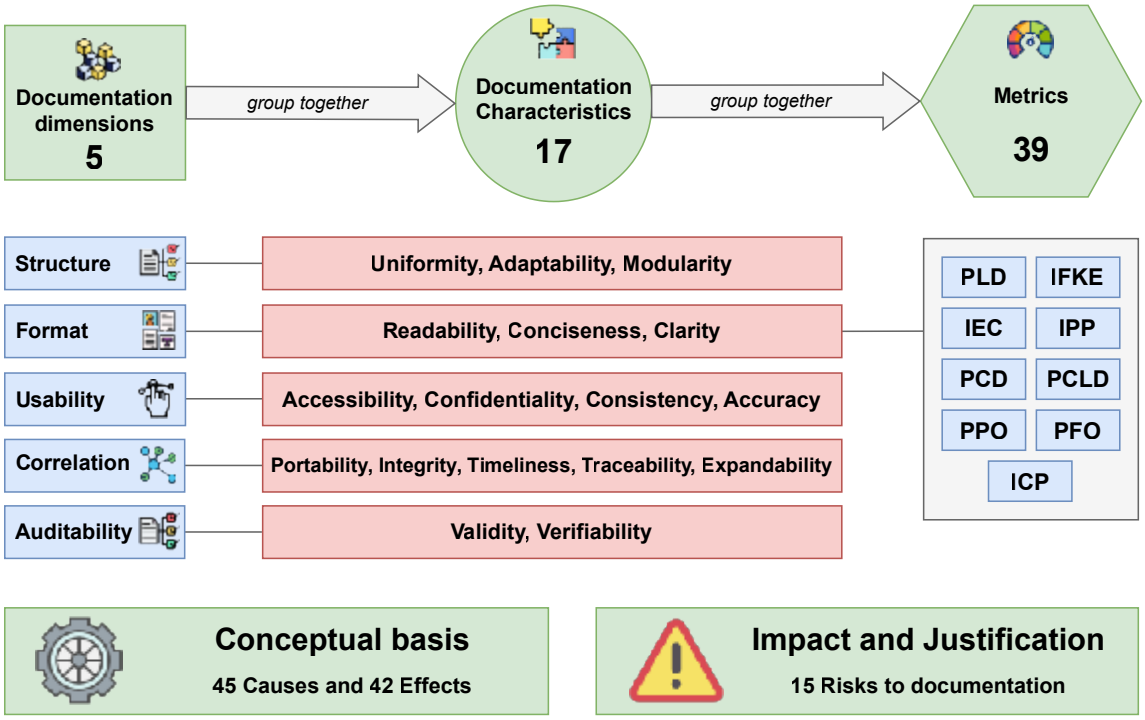

Figura 3. General architecture of the proposed metrics model

Source: own elaboration.

Metrics for the Format dimension

As defined in Section 2, the Format dimension encompasses the visual presentation and language of the artifact. Because deficiencies in this dimension can hinder comprehension and weaken long-term knowledge preservation—regardless of the technical accuracy of the content—this section details the specific metrics for its three key characteristics: Readability, Conciseness, and Clarity.

Readability Metrics

Readability is a subjective quality that determines the ease of reading. Since factors such as excessive technicality or typographical errors impair it, its evaluation requires a mixed approach: combining user perception with objective metrics that analyze the linguistic structure of the text.

The first metric (Equation 1) is the **Perceived Readability of Documentation (PLD)**, which quantifies users' subjective assessment of reading ease. It is measured on a scale of 0 to 100—where higher values indicate better quality—and is calculated using a four-question survey with ratings from 1 to 5, available at https://bit.ly/3ZZwvSz. For example, if a participant's responses yield a result of 62.5%, readability is classified as acceptable according to Table 3, indicating that the text is adequate but has shortcomings that require additional reader effort.

$$PLD = \left(\frac{(P21 + P22 + P23 + P24) - 4}{16}\right) * 100 \qquad (1)$$

Table 3. *Interpretation scale for the PLD metric*

Result	Classification	Interpretation
PLD ≥ 80	Excellent	Readability is satisfactory. The text is very easy to read and review.
60 ≤ PLD < 80	Good	Readabilityis good, although there are minor flaws that do not impede comprehension.
40 ≤ PLD < 60	Acceptable	Readability is fair, and significant shortcomings are identified that require effort to overcome.
10 ≤ PLD < 40	Poor	Readability is poor and there are critical shortcomings that seriously hinder reading and comprehension.
PLD < 10	Very poor	Readability is non-existent or very poor, and the text is practically incomprehensible or requires extreme effort to understand.

Source: own elaboration.

The second metric (Equation 2) is the **Flesch-Kincaid Index for the Spanish language (IFKE)** [22], which measures the linguistic complexity of the text to determine its ease of comprehension by an average reader. The result is expressed on a scale of 0 to 100, where a higher score indicates easier reading. For example, a fragment of a user story consisting of 72 words, 2 sentences, and 158 syllables would yield a result of 38.45, classifying the text as "Difficult" according to Table 4.

$$IFKE = 206.84 - 1.02\left(\frac{NTP}{NTO}\right) - 60\left(\frac{NTS}{NTP}\right) \qquad (2)$$

Table 4. *Interpretation scale for the IFKE metric*

Result	Classification	Interpretation
90 ≤ IFKE < 100	Very easy	The text is optimal and accessible to any reader without effort.
80 ≤ IFKE < 90	Easy	The text is simple and the risk of misunderstanding is very low.
70 ≤ IFKE < 80	Moderately easy	The text is clear and can be read without difficulty by most people.
60 ≤ IFKE < 70	Normal	The text is functional but requires additional effort for readers unfamiliar with its information.
50 ≤ IFKE < 60	Moderately difficult	The text is slightly complex, requires effort, and there is a risk of misinterpretation.
30 ≤ IFKE < 50	Difficult	The text is complex with a high risk of misunderstanding and requires considerable effort to understand its content.
0 ≤ IFKE < 30	Very difficult	The text is very dense or too technical.

Source: R. Flesch [22].

The third metric (Equation 3) is the **Content Structuring Index (IEC)**, based on the premise that objective readability depends not only on linguistic complexity (IFKE) but also on visual presentation. Its purpose is to measure structural richness by evaluating the density of formatting elements—headings, lists, and visual aids—that organize content and break up blocks of text. A higher value indicates better

structural readability. For example, an artifact with 20 paragraphs and 10 supporting elements would yield an IEC of 0.5, while the same content with only 1 heading would result in an IEC of 0.05, indicating dense text with very low structural readability. Table 5 provides the interpretation scale.

$$IEC = \frac{Nh+Nl+Nv}{Np} \qquad (3)$$

Table 5. *Interpretation scale for IEC*

Result	Classification	Interpretation
IEC = 0	Very Poor	No formatting elements exist. Structural readability is zero.
0 < IEC < 0.25	Poor	There are very few structural elements. The text remains dense and difficult to review.
0.25 ≤ IEC < 0.5	Acceptable	There are some structural elements. The text requires review.
0.5 ≤ IEC < 1.0	Good	There is at least 1 formatting element for every 2 paragraphs. The content is segmented and easy to review visually.
IEC ≥ 1	Excellent	There are one or more formatting elements (headings, lists, visuals) for every paragraph, with an excellent balance between content and visual structure.

Source: own elaboration.

The fourth metric (Equation 4) is the Paragraph Penalty Index (IPP), which quantifies excessively long paragraphs that increase cognitive load and hinder quick information retrieval. The metric compares the number of lines in each paragraph (LPi) against a predefined optimal threshold (LOP, e.g., 8 lines). A quadratic penalty is applied to lines exceeding this threshold, based on the premise that the negative impact on readability is non-linear: a very long paragraph is disproportionately more harmful than several medium-length ones. The result is the average of these penalties; a lower value indicates better quality (Table 6). For example, a document with three paragraphs (Np = 3) of 6, 10, and 14 lines, with an optimal threshold of 8, would generate an IPP of 13.33, classifying the format as Poor.

$$IPP = \frac{1}{Np}\sum_{i=1}^{Np}(\max(0, LPi - LOP))^2 \qquad (4)$$

Table 6. *Interpretation scale for IPP*

Result	Classification	Interpretation
IPP = 0	Optimal	No difficulties; all paragraphs are within the optimal threshold.
0 < IPP < 5	Good	Paragraph density is slight; paragraphs are moderately long, but their impact is minimal.
5 ≤ IPP < 20	Poor	The text is dense, with a notable presence of long paragraphs that hinder reading.
IPP ≥ 20	Very Poor	The text is very dense and contains extremely long paragraphs.

Source: own elaboration.

Conciseness metrics

Conciseness involves providing the necessary information without sacrificing accuracy; when absent, documentation becomes redundant, cumbersome, and difficult to understand. To measure it, the **Perception of Documentation Conciseness (PCD)** metric (Equation 5) is proposed, which determines whether users consider the content sufficiently detailed without including unnecessary information. It is expressed on a scale of 0 to 100 and is calculated from a six-question survey with ratings from 1 to 5 (https://bit.ly/46r9DxA). For example, if a user's responses yield a result of 75%, the perception of conciseness is classified as "Good" according to Table 7.

$$PCD = \left(\frac{(P25+P26+P27+P28+P29+P30)-6}{24}\right) * 100 \qquad (5)$$

Table 7. *Interpretation scale for PCD*

Result	Classification	Interpretation
PCD < 10	Very poor	There is excessive information overload, the content is redundant, and it lacks semantic efficiency.
10 ≤ PCD < 40	Poor	There is a high presence of superfluous information, making it difficult to extract relevant content.
40 ≤ PCD < 60	Acceptable	The documentation contains non-essential information that requires additional effort on the part of the reader.
60 ≤ PCD < 80	Good	The information is concise, with only minor redundancies that do not impede understanding.
PCD ≥ 80	Excellent	The information is accurate and efficient, presenting only the strictly necessary content.

Source: own elaboration.

Clarity metrics

Clarity is the ability of content to be intelligible without generating doubts or requiring reinterpretation. Given that its absence erodes trust, its evaluation requires a mixed approach that integrates the user's subjective perception with an objective analysis of the textual structure.

The first metric (Equation 6), **Perceived Clarity of Documentation (PCLD)**, assesses whether users perceive the content as understandable and intelligible. Results are expressed on a scale of 0 to 100, derived from a four-question survey with ratings from 1 to 5. For example, if a user's responses yield a result of 68.75%, clarity is classified as "Good" according to Table 8.

$$PCLD = \left(\frac{(P31 + P32 + P33 + P34)-4}{16}\right) * 100 \qquad (6)$$

Table 8. *Interpretation scale for PCLD*

Result	Classification	Interpretation
PCLD < 10	Very poor	The text is perceived as ambiguous and confusing, generating a high degree of uncertainty in the reader.
10 ≤ PCLD < 40	Poor	The content is perceived as difficult to understand and requires frequent reinterpretation, generating doubts about its meaning.
40 ≤ PCLD < 60	Acceptable	The text is moderately understandable but lacks the efficiency necessary to convey the message without generating uncertainty.
60 ≤ PCLD < 80	Good	The documentation is perceived as clear and intelligible, with only a few minor ambiguities that do not impede comprehension.
PCLD ≥ 80	Excellent	The content is perceived as fully understandable and intelligible, conveying the message efficiently and without raising doubts.

Source: own elaboration.

To complement the subjective evaluation, three objective metrics are proposed that analyze the structural complexity of the text.

The first is the **Average Words per Sentence (PPO)** metric (Equation 7), which quantifies excessively long sentences that increase cognitive load and hinder comprehension. It is expressed as a positive integer value; a lower number indicates greater clarity. For example, a PPO of 60 is classified as "Poor" (Table 9) because it requires significant memory effort to process.

$$PPO = \frac{TPC}{TOC} \qquad (7)$$

Table 9. *Interpretation scale for PPO*

Result	Classification	Interpretation
PPO < 15	Excellent	The text uses short, direct sentences. It is optimally clear.
10 ≤ PPO < 40	Good	The text uses sentences of standard length. It is easy to read for most people.
40 ≤ PPO < 60	Acceptable	The text uses moderately long sentences and requires more effort from the reader.
60 ≤ PPO < 80	Poor	The text uses long, complex sentences that increase cognitive load and the risk of ambiguity.
PPO ≥ 80	Very poor	The text uses excessively long sentences with a high risk of misunderstanding and reader fatigue.

Source: own elaboration.

The **Average Phrases per Sentence (PFO)** metric (Equation 8) assesses syntactic complexity by measuring the density of ideas per sentence. A low value is desirable, as an excess of clauses makes reading difficult. For example, if a text of 2 sentences (TOC) contains 7 clauses (TFC), PFO = 3.5, indicating poor clarity (Table 10).

$$PFO = \frac{TFC}{TOC} \qquad (8)$$

Table 10. *Interpretation scale for PFO*

Result	Classification	Interpretation
PPO = 1.0	Excellent	The syntactic structure is ideal; each sentence conveys a single idea, and the cognitive load is minimal.
1.0 < PFO ≤ 2.0	Good	Simple sentences that combine few ideas, are easy to process, and have a low risk of debt.
2.0 < PFO ≤ 3.0	Acceptable	Sentences are moderately dense, containing multiple ideas. Reading effort and the risk of debt due to ambiguity increase.
3.0 < PFO ≤ 4.0	Poor	Sentences are complex, syntactically nested, and there is a high density of ideas that increase cognitive load.
PFO > 4.0	Very poor	Sentences are excessively dense or chained, and the cognitive load is very high.

Source: Authors.

Finally, the **Prose Quality Index (ICP)** (Equation 9) measures the formal quality of the text by quantifying the presence of errors that generate uncertainty and affect clarity. Unlike PPO and PFO, which evaluate structure, ICP addresses correctness. The metric is normalized per 1,000 words and applies severity weighting, under the premise that grammatical errors are more detrimental to meaning than spelling errors. A lower value indicates higher prose quality.

$$ICP = \frac{(Eo*Wo)+(Eg*Wg)}{Pt/_{1000}} \qquad (9)$$

For example, a document with 2000 words (Pt) that has ten spelling errors (Eo) and four grammatical errors (Eg), using Wo=1 and Wg=3, the IPC would be 11, indicating acceptable prose (Table 11).

Table 11. *Interpretation scale for ICP*

Result	Classification	Interpretation
0 ≤ ICP < 2	Excellent	The prose is polished and virtually error-free.
2 ≤ ICP < 5	Good	There are some minor or slight errors that do not impede comprehension.
5 ≤ ICP < 15	Acceptable	There are noticeable errors that require revision and may compromise the clarity of the artifact.
ICP ≥ 15	Poor	The prose is sloppy and contains a high density of errors that negatively impact clarity and credibility.

Source: own elaboration.

Discussion

The main strength of the proposal lies in the combination of the team's subjective perception with the objective analysis of the artifacts. Perception metrics (such as PLD and PCLD) are crucial in agile environments to validate the practical value of documentation, because a technically sound document that is perceived as confusing is effectively unusable.

Objective metrics (such as IFKE and PPO) provide an empirical basis for diagnosing the root cause of poor perception. For example, a low subjective rating for clarity can be explained by a specific datum—an average sentence length that is too long (high PPO)—thereby transforming an abstract complaint into an actionable problem.

Beyond quality assessment, these metrics act as risk management tools. A deterioration in Format scores serves as an early warning that critical risks—such as source code incomprehensibility (R1), low system quality (R4), and communication failures (R15)—may materialize, enabling the team to move from reactive to proactive management.

The proposal also has limitations: the Format dimension is critical but insufficient on its own. A holistic diagnosis of documentation debt requires future evaluation of the remaining four dimensions: Structure, Usability, Correlation, and Auditability.

Conclusions and future work

This work addresses documentation debt in agile development as an engineering variable that has historically lacked formal measurement mechanisms because of its invisible nature. Its main contribution is a metrics model that transforms this abstract concept into measurable and actionable indicators.

The analysis of the Format dimension reveals that much project risk does not stem from a lack of information, but from how that information is presented. Objective metrics such as Average Words per Sentence (PPO) suggest that structural problems are often the root cause of low perceived clarity, increasing the likelihood of communication failures.

An exclusively objective or subjective approach is insufficient. True diagnostic capacity emerges from the combination of the two: while subjective perception (e.g., PCLD) identifies the existence of a problem, objective metrics (e.g., IFKE, PPO) diagnose its structural cause. This work therefore represents an initial step toward managing documentation quality not as an art, but as an engineering attribute that must be measured for proactive control.

Three lines of future work are proposed. First, the specification of metrics for the remaining four dimensions (Structure, Usability, Correlation, and Auditability) must be finalized to complete the model. Second, the model must be empirically validated in real industrial environments to assess its accuracy and practical usefulness. Third, the development of a software tool based on emerging technologies—such as Generative Artificial Intelligence (GenAI)—is planned to automate metric execution, facilitating adoption in industry and improving documentation processes throughout the software development lifecycle.

Referencias

[1] E. Aghajani *et al.*, "Software documentation issues unveiled," in *Proc. IEEE/ACM Int. Conf. Softw. Eng. (ICSE)*, Montreal, QC, Canada, 2019, pp. 1199–1210. https://doi.org/10.1109/ICSE.2019.00122

[2] G. Matturro, F. Raschetti, and C. Fontán, "A systematic mapping study on soft skills in software engineering," *J. Univers. Comput. Sci.*, vol. 25, no. 1, pp. 16–41, 2019. https://doi.org/10.3217/jucs-025-01-0016

[3] N. Rios, R. O. Spínola, M. Mendonça, and C. Seaman, "The practitioners' point of view on the concept of technical debt and its causes and consequences: A design for a global family of industrial surveys and its first results from Brazil," *Empir. Softw. Eng.*, vol. 25, no. 5, pp. 3216–3287, 2020. https://doi.org/10.1007/s10664-020-09832-9

[4] S. Al-Saqqa, S. Sawalha, and H. Abdelnabi, "Agile software development: Methodologies and trends," *Int. J. Interact. Mobile Technol.*, vol. 14, no. 11, pp. 246–270, 2020. https://doi.org/10.3991/ijim.v14i11.13269

[5] M. Fowler, "Technical debt quadrant," Oct. 2009. Accessed: Oct. 17, 2022. [Online]. Available: https://martinfowler.com/bliki/TechnicalDebtQuadrant.html

[6] A. Martini, T. Besker, and J. Bosch, "Process debt: A first exploration," in *Proc. Asia-Pacific Softw. Eng. Conf. (APSEC)*, Singapore, 2020, pp. 316–325. https://doi.org/10.1109/APSEC51365.2020.00040

[7] J. P. Zumba and C. A. L. Arreaga, "Evolución de las metodologías y modelos utilizados en el desarrollo de software," *INNOVA Res. J.*, vol. 3, no. 10, pp. 20–33, Oct. 2018. https://doi.org/10.33890/innova.v3.n10.2018.65

[8] N. Rios *et al.*, "Hearing the voice of software practitioners on causes, effects, and practices to deal with documentation debt," in *Lecture Notes in Computer Science*, vol. 12130. Cham, Switzerland: Springer, 2020, pp. 55–70. https://doi.org/10.1007/978-3-030-44429-7_4

[9] Y. Shmerlin, I. Hadar, D. Kliger, and H. Makabee, "To document or not to document? An exploratory study on developers' motivation to document code," in *Lecture Notes in Business Information Processing*, vol. 215. Cham, Switzerland: Springer, 2015, pp. 100–106. https://doi.org/10.1007/978-3-319-19243-7_10

[10] A. A. H. Alzahrani, "Software systems documentation: A systematic review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 8, 2024. https://doi.org/10.14569/IJACSA.2024.0150816

[11] D. V. Koznov, D. V. Luciv, and G. A. Chernishev, "Duplicate management in software documentation maintenance," *CEUR Workshop Proc.*, vol. 1989, pp. 195–201, 2017.

[12] J. Zhi, V. Garousi-Yusifoglu, B. Sun, G. Garousi, S. Shahnewaz, and G. Ruhe, "Cost, benefits and quality of software development documentation: A systematic mapping," *J. Syst. Softw.*, vol. 99, pp. 175–198, 2015. https://doi.org/10.1016/j.jss.2014.09.042

[13] J. Bayer and D. Muthig, "A view-based approach for improving software documentation practices," in *Proc. Int. Symp. Workshop Eng. Comput. Based Syst. (ECBS)*, Potsdam, Germany, 2006, pp. 269–278. https://doi.org/10.1109/ECBS.2006.18

[14] M. Zanoni, F. Perin, F. A. Fontana, and G. Viscusi, "Pattern detection for conceptual schema recovery in data-intensive systems," *J. Softw.: Evol. Process*, vol. 26, no. 12, pp. 1172–1192, 2014. https://doi.org/10.1002/smr.1656

[15] J. D. Arthur and K. T. Stevens, "Assessing the adequacy of documentation through document quality indicators," in *Proc. Conf. Softw. Maintenance (ICSM)*, Miami, FL, USA, 1989, pp. 40–49. https://doi.org/10.1109/icsm.1989.65192

[16] R. Plosch, A. Dautovic, and M. Saft, "The value of software documentation quality," in *Proc. Int. Conf. Quality Softw. (QSIC)*, Dallas, TX, USA, 2014, pp. 333–342. https://doi.org/10.1109/QSIC.2014.22

[17] M. Kajko-Mattsson, "A survey of documentation practice within corrective maintenance," *Empir. Softw. Eng.*, vol. 10, no. 1, pp. 31–55, 2004. https://doi.org/10.1023/B:LIDA.0000048322.42751.ca

[18] A. Forward and T. C. Lethbridge, "The relevance of software documentation, tools and technologies: A survey," in *Proc. 2002 ACM Symp. Document Eng.*, McLean, VA, USA: ACM, 2002, pp. 26–33. https://doi.org/10.1145/585058.585065

[19] N. Qamar, N. Sabahat, and A. Mosavi, "Evaluating the impact of pair documentation on requirements quality in agile software development," *IEEE Access*, vol. 13, pp. 45784–45794, 2025. https://doi.org/10.1109/ACCESS.2025.3550123

[20] J.-C. Narváez-Narváez, C.-J. Pardo-Calvache, and C.-E. Orozco-Garcés, "Deuda de la documentación en el desarrollo ágil de software: mapeo sistemático de la literatura," *Rev. Cient.*, vol. 46, no. 1, pp. 107–121, Jan. 2023. https://doi.org/10.14483/23448350.19670

[21] V. R. Basili and G. Caldiera, "The goal question metric paradigm," in *Encyclopedia of Software Engineering*, J. J. Marciniak, Ed. New York, NY, USA: Wiley, 1994, vol. 2, pp. 528–532. [Online]. Available: https://go.umd.edu/3ol7AtO

[22] R. Flesch, "A new readability yardstick," *J. Appl. Psychol.*, vol. 32, no. 3, pp. 221–233, 1948. https://doi.org/10.1037/h0057532

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.24858

INVESTIGACIÓN

Evaluación manual de accesibilidad web: estudio de caso en portal de estudiantes de una universidad pública

Web accessibility manual evaluation: case study of a public university student portal

Erick Daniel Martínez Martínez [1], Patricia Martínez Moreno [2], José Antonio Vergara Camacho [3], Gerardo Contreras Vega [4]

Fecha de Recepción: 12 de noviembre de 2025 **Fecha de Aceptación**: 12 de marzo de 2026

Cómo citar: E.D. Martínez Martínez, P. Martínez Moreno, J.A. Vergara Camacho, G.C. Contreras Vega, «Evaluación manual de accesibilidad web: estudio de caso en portal de estudiantes de una universidad pública», *Tecnura*, vol. 30, n.° 88, jun. 2026. 58–68. https://doi.org/10.14483/22487638.24858

Resumen

Objetivo: evaluar la accesibilidad web del portal de estudiantes de la Universidad Veracruzana bajo las pautas WCAG 2.2 para identificar barreras de acceso.

Metodología: se aplicó una evaluación manual basada en la metodología WCAG-EM sobre la página principal. Se auditaron 86 criterios de éxito empleando JAWS, WAVE y WCAG Color Contrast Checker.

Resultados: se identificó un 41.9 % de fallos en los criterios evaluables, principalmente por bajo contraste, falta de alternativas textuales y deficiencias en la navegación por teclado. El portal no alcanza el nivel mínimo de conformidad A.

Conclusiones: el estudio evidencia barreras críticas que limitan la inclusión digital, lo que subraya la necesidad de corregir los fallos técnicos detectados y establecer procesos de mejora continua en la plataforma.

Palabras clave: accesibilidad, evaluación, sitios web, universidades, alumnos con discapacidad.

Abstract

Objective: To evaluate the web accessibility of the Universidad Veracruzana student portal under WCAG 2.2 guidelines in order to identify access barriers.

Methodology: A manual evaluation based on the WCAG-EM methodology was applied to the main page. Eighty-six success criteria were audited using JAWS, WAVE, and the WCAG Color Contrast Checker.

Results: A total of 41.9% failures were identified in the evaluable criteria, mainly due to low contrast, lack of textual alternatives, and deficiencies in keyboard navigation. The portal does not meet the minimum Level "A" conformance.

Conclusions: The study reveals critical barriers that limit digital inclusion, underscoring the need to correct the identified technical failures and to establish continuous improvement processes within the platform.

Keywords: accessibility, evaluation, websites, universities, students with disabilities.

1 Estudiante de Ingeniería de Software de la Universidad Veracruzana campus Coatzacoalcos. Email: erickdanielmartinezmartinez123@gmail.com

2 Docente tiempo completo e investigadora del Programa Ingeniería de Software de la Universidad Veracruzana campus Coatzacoalcos. Email: pmartinez@uv.mx

3 Docente tiempo completo e investigador del Programa Ingeniería de Software de la Universidad Veracruzana campus Coatzacoalcos. Email: jvergara@uv.mx

4 Docente de tiempo completo e imparte asignaturas en el Programa Ingeniería de Software de la Universidad Veracruzana campus Xalapa. Email: gcontreras@uv.mx

Introducción

Existen millones de sitios web de educación superior, cada uno con su propio estilo y forma. Sin embargo, no todos los sitios web cumplen con las pautas propuestas por el World Wide Web Consortium (W3C) [1]. La accesibilidad web es un requisito esencial para que las personas con algún tipo de discapacidad puedan percibir, entender, navegar e interactuar con la información en igualdad de condiciones que el resto de los usuarios.

En el contexto de una universidad con más de 95 000 estudiantes [2], el portal web no solo es un recurso, sino también un servicio esencial e indispensable para la vida académica. En México, la accesibilidad digital es una obligación para las instituciones públicas, que deben asegurar el acceso a la información en igualdad de condiciones [3]. La falta de accesibilidad en esta plataforma constituye una barrera directa que amenaza a la inclusión digital y la igualdad de oportunidades. Por ello, el objetivo principal de este estudio es evaluar el nivel de accesibilidad web del portal de estudiantes de la Universidad Veracruzana mediante la aplicación de las Pautas de Accesibilidad para el Contenido Web (WCAG) 2.2, identificando barreras específicas y estableciendo una base para futuras mejoras. Este objetivo se concreta mediante los siguientes puntos específicos:

1. Delimitar la muestra a evaluar del sitio web.

2. Identificar los criterios de conformidad que cumple el sitio de estudiantes de la Universidad.

3. Realizar pruebas manuales detalladas para verificar el cumplimiento de las pautas WCAG 2.2.

4. Emitir recomendaciones para mejorar la accesibilidad web del sitio.

Accesibilidad

La accesibilidad web implica que las personas con discapacidad puedan usar la web en las mismas condiciones que el resto de las personas. En este sentido, la accesibilidad web se refiere al diseño y desarrollo que permite a estas personas percibir, entender, navegar e interactuar con la web [4].

Para ello, el World Wide Web Consortium (W3C) cuenta con las WCAG, actualmente en su versión 2.2. Estas pautas se definen como una serie de lineamientos que deben seguir los sitios web para que el contenido web sea más accesible para las personas con discapacidad. Además, se deben integrar desde las primeras etapas del desarrollo web y mantenerse a lo largo del ciclo de vida del sitio [7]. La Figura 1 representa los conceptos principales de las pautas, además de la explicación de los niveles presentes [8] [6].

Figura 1. Conceptos generales de la WCAG 2.2

Fuente: elaboración propia.

Los niveles de conformidad son las categorías que indican el nivel de aprobación que posee un sitio web acorde a los criterios de conformidad establecidos por la WCAG 2.2. Existen tres diferentes niveles [6]:

- Nivel A: es el nivel básico de accesibilidad web. Cumplir con este nivel implica cubrir los requisitos mínimos para considerar accesible un sitio. Incluye los primeros 31 criterios esenciales.

- Nivel AA: es el estándar para considerar inclusivo un sitio web. Cumplir con este nivel significa abordar los 55 criterios definidos por las WCAG.

- Nivel AAA: representa el nivel máximo de accesibilidad para un sitio web. Este nivel incluye mejoras para ofrecer la mejor experiencia de usuario posible, aunque es el nivel más difícil de alcanzar, muchas veces no se considera prioritario. Requiere cumplir con prácticamente todos los criterios de accesibilidad, lo que suele incluir criterios avanzados de contenido, navegación y diseño.

Metodología

Para realizar una evaluación completa de la accesibilidad web, es esencial definir con claridad la metodología aplicada. Con base en ello, se propone la siguiente metodología de la Figura 2, inspirada en la guía Website Accessibility Conformance Evaluation Methodology (WCAG-EM) [5] [9].

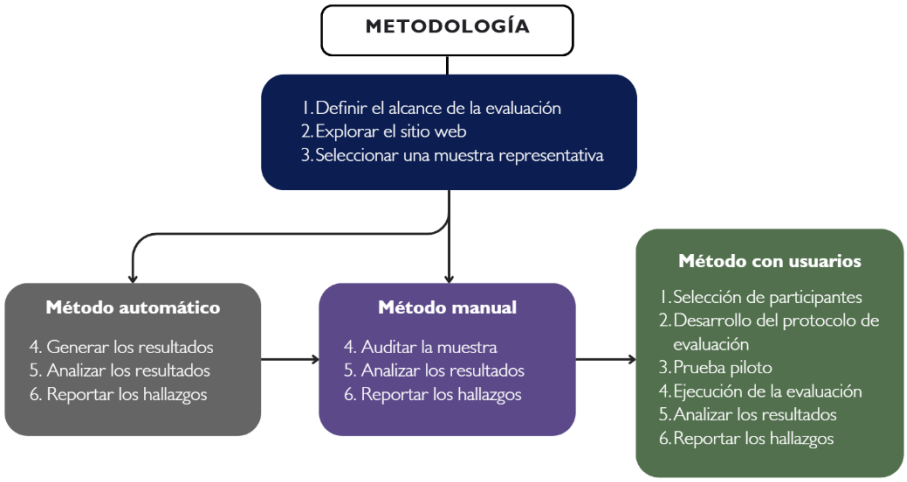

Figura 2. Metodología de los métodos de evaluación automático, manual y con usuarios

Fuente: elaboración propia.

Esta investigación se centra en reportar los hallazgos del método manual, el cual permite detectar problemas que una herramienta automática no puede identificar y debe ser realizado por una persona con experiencia en las pautas WCAG.

Alcance de la evaluación

El propósito de esta evaluación es efectuar un análisis técnico, exhaustivo y sistemático de la accesibilidad web de la página principal del portal estudiantil de la Universidad, aplicando los criterios establecidos en la WCAG 2.2, nivel AAA, con el objetivo de obtener una caracterización integral y precisa de su desempeño en accesibilidad [9].

Exploración del sitio web

El análisis preliminar del sitio web evidencia una estructura uniforme en la mayoría de sus páginas, compuestas por secciones destinadas a servicios escolares como calendarios, trámites y directorios de contacto. Dichas secciones integran elementos multimedia (imágenes y videos), marcos de redes sociales y múltiples hipervínculos.

En cuanto a la implementación tecnológica, el portal emplea HTML5 para la estructura, hojas de estilo en cascada (CSS) para la presentación y JavaScript para la gestión de la interactividad. Asimismo, se identifican componentes como menús desplegables, barras de búsqueda y diversas interacciones dinámicas en pantalla, relevantes para el proceso de evaluación.

Selección de muestra representativa

La selección de la página principal del portal de estudiantes (https://www.uv.mx/estudiantes/) como muestra representativa se fundamenta en su rol crítico como punto central de acceso.

Esta página constituye un punto central para la comunidad estudiantil y fue diseñada para proporcionar a los estudiantes información esencial sobre trámites escolares, noticias, enlaces de interés, entre otros, por lo cual integra diversos patrones de interacción.

Metodológicamente, esta página integra los diversos patrones de interacción (menús, enlaces, multimedia) que se replican en el resto del sitio. Esta concentración funcional permite evaluar una amplia gama de criterios WCAG en un contexto de uso real, lo cual resulta suficiente para evidenciar barreras de alto impacto que afectan a toda la comunidad.

La decisión de limitar la evaluación a esta página específica considera las restricciones de esta fase de la investigación. Este enfoque de estudio de caso permite un análisis detallado y profundo que sirve como una línea base crítica, estableciendo un precedente claro sobre la incidencia social de la accesibilidad en el portal.

Procedimiento de auditoría manual

De acuerdo con el paso 4 del método manual, se ejecutó la auditoría de la muestra. Este proceso se detalla para garantizar la reproducibilidad del estudio.

Herramientas de Evaluación: para el análisis técnico se empleó un conjunto de herramientas especializadas:

- JAWS (*Job Access With Speech*): utilizado como tecnología de apoyo principal para simular la experiencia de navegación de usuarios con discapacidad visual.
- WAVE (*Web Accessibility Evaluation Tool*): empleada para la detección inicial de fallos en criterios de conformidad en el código fuente de manera visual.
- WCAG Color Contrast Checker: usado para la medición de contrastes.
- WCAG-EM Report Tool: utilizada para la recolección sistemática de los datos de la auditoría.

Proceso de Auditoría: la evaluación manual se realizó con base en el análisis del código, la interfaz y la interacción con tecnologías de apoyo. Se aplicaron los 86 criterios de éxito del nivel AAA, siguiendo un procedimiento sistemático:

1. **Análisis de Código y Contraste**: se utilizó WAVE para la detección de fallos estructurales y WCAG Color Contrast Checker para medir las relaciones de contraste de texto y elementos no visuales.

2. **Pruebas de Navegación por Teclado**: se verificó la operabilidad completa del sitio usando únicamente el teclado, asegurando que todos los elementos interactivos fueran accesibles y recibieran el foco de manera correcta.

3. **Pruebas con Tecnología de Apoyo:** se utilizó el lector de pantalla JAWS para auditar la correcta lectura de etiquetas, encabezados, contenido multimedia y la coherencia de la interacción.

4. **Recolección de Datos:** todos los hallazgos para cada criterio fueron sistemáticamente documentados en la WCAG-EM Report Tool.

Resultados

La evaluación manual se realizó siguiendo el procedimiento descrito. Durante esta auditoría, se aplicaron los 86 criterios de éxito establecidos por las WCAG 2.2 en su nivel AAA, evaluando su cumplimiento dentro del portal. Cada criterio fue evaluado según su contexto específico, utilizando las herramientas especializadas correspondientes, y los resultados se documentaron sistemáticamente en la WCAG-EM Report Tool.

Figura 3. Resumen de la evaluación manual proporcionado por WCAG-EM Report Tool.

Fuente: Captura obtenida de WCAG-EM Report Tool [10].

Resultados de la auditoría

Los datos se recopilaron y organizaron sistemáticamente según los cuatro principios fundamentales de accesibilidad web establecidos por el W3C. La Tabla 1 presenta un desglose del cumplimiento de los criterios de accesibilidad según los cuatro principios de las WCAG 2.2: Perceptible, Operable, Comprensible y Robusto.

"Pasado" indica la cantidad de criterios que cumplieron con las pautas de accesibilidad por principio. En total, 36 criterios pasaron la evaluación. En contraste, "fallado" indica el número de criterios que no cumplieron con las pautas, con un total de 26 criterios los cuales representan el 41.9% de los criterios evaluables.

La columna, "no puedo decirlo" corresponde a los criterios no determinados, para los cuales no se pudo definir si pasaron o fallaron la prueba; el valor fue 0 para todos los principios. La columna "no presente" muestra el total de 24 criterios no evaluados porque el contenido o la funcionalidad no existían en el sitio web. La columna "no marcado", indicada con valor "0" corresponde a los criterios que no se evaluaron o que no se incluyeron en la auditoría.

El estudio evaluó 86 criterios de éxito en el nivel AAA, de los cuales 62 pudieron ser evaluados. Los resultados muestran que el portal de estudiantes no cumple con el nivel de conformidad "A" de las WCAG 2.2, ya que se deben cumplir con todos los criterios de ese nivel sin excepción para alcanzar la conformidad.

Tabla 1. *Resultados de WCAG-EM Report Tool ordenados por principio de accesibilidad.*

	Resultados				
Principio	**Pasado**	**Fallado**	**No puedo decirlo**	**No presente**	**No marcado**
Perceptible	7	16	0	6	0
Operable	18	9	0	7	0
Comprensible	10	1	0	10	0
Robusto	1	0	0	1	0
Total	36	26	0	24	0

Fuente: elaboración propia.

Análisis de los resultados

Para analizar los resultados y cuantificar objetivamente el grado de incumplimiento, se empleó la métrica de tasa de fallos (Failure-Rate, FR) que relaciona los puntos reales de fallo (B_p) con los puntos potenciales de fallo (P_p). Esta métrica tiene un valor comprendido entre 0 y 1, donde 0 indica accesibilidad total y 1 refleja inaccesibilidad absoluta [11].

$$l_p = \frac{B_p}{P_p}$$

De un total de 62 criterios correctamente evaluados (dado que 24 criterios no estaban presentes en el contenido del sitio y, por lo tanto, no fueron aplicables) se obtuvo el siguiente resultado:

$$l_p = \frac{26}{62} = 0.419$$

Este valor indica que el 41.9 % de los criterios potenciales de accesibilidad presenta fallos, lo cual refleja un cumplimiento parcial de las pautas WCAG 2.2.

El portal de estudiantes no alcanza conformidad con ningún nivel de las WCAG 2.2 (A, AA o AAA), ya que, para lograr conformidad incluso con el nivel A básico, se deben cumplir con todos los criterios de ese nivel sin excepción.

Hallazgos

Con base en los resultados obtenidos, el portal de estudiantes presenta diversas barreras de accesibilidad que requieren atención inmediata. Los principales fallos identificados, agrupados por los principios de las WCAG 2.2, son los siguientes:

Tabla 2. *Principales fallos de accesibilidad web identificados por principio WCAG 2.2*

Principio	Fallos encontrados
Perceptible	Bajo contraste en textos (3.5:1) Bajo contraste en elementos no visuales (1.96:1) Falta de audiodescripción o alternativa textual completa en videos y ausencia de alternativas textuales para ciertos contenidos multimedia
Operable	Problemas en la estructura de las interacciones con teclado El tamaño de algunos elementos no cumple con el tamaño mínimo requerido o no reciben el foco
Comprensible	No proporciona versiones simplificadas del contenido que podría resultar complejo. No incluye apoyos para usuarios con dificultad de lectura o lenguaje técnico
Robusto	No se encontraron fallos

Fuente: elaboración propia.

Sin embargo, también existen aspectos positivos como una estructura organizacional coherente del sitio, implementación parcialmente correcta de las etiquetas “name”, “role”, “value” y “aria-label”, control total de eventos por parte del usuario, y comprensión clara de los textos.

Amenazas a la validez

La validez de este estudio presenta limitaciones que deben considerarse al interpretar los resultados. En primer lugar, la evaluación se limitó exclusivamente a la página principal del portal de estudiantes, lo que impide obtener una visión completa del estado de accesibilidad del sitio en su conjunto. Otras secciones internas podrían contener problemas adicionales o, por el contrario, cumplir criterios no presentes en la página analizada. Asimismo, un 28% de los criterios WCAG no pudieron evaluarse por falta de contenido, reduciendo la cobertura total de los criterios de evaluación. El uso de la métrica de tasa

de fallos (Failure-Rate FR) permitió cuantificar el grado de incumplimiento; sin embargo, la ausencia de triangulación con otros métodos de evaluación puede afectar la solidez de las conclusiones. Dado que el estudio es experimental, los resultados deben considerarse como un diagnóstico inicial más que como una valoración definitiva del estado de accesibilidad del portal.

Análisis crítico

La evaluación reveló hallazgos críticos que requieren atención para garantizar la inclusión digital de todos los usuarios. El portal no alcanza conformidad con ningún nivel de las WCAG 2.2, con un 41.9 % de criterios evaluables presentando fallos.

Los principales problemas identificados incluyen deficiencias críticas en el contraste de colores, ausencia de alternativas textuales para contenido multimedia y problemas en la navegación por teclado. Estas barreras pueden impedir significativamente el acceso a información académica para estudiantes con discapacidades visuales, motoras y cognitivas.

Se recomienda implementar un plan que aborde los problemas críticos identificados, así como establecer procesos de evaluación continua para mantener y mejorar los estándares de accesibilidad en todo el sitio web. Este estudio representa un primer paso hacia la construcción de un entorno digital más inclusivo y contribuye al objetivo institucional de brindar educación superior de calidad para todos los estudiantes.

Conclusiones

Se concluye que desarrollar sitios web basados en los principios de accesibilidad web brinda beneficios para la sociedad en la búsqueda de “una web para todos”, pero también genera beneficios económicos en las organizaciones. Por ejemplo, la accesibilidad mejora la usabilidad y favorece una mejor experiencia de usuario en general, para todos y no solo para quienes tienen discapacidad [12]; lo que puede generar un mayor tráfico, fidelidad de clientes y una percepción positiva de la marca. De igual forma, se estima que las empresas que priorizan la accesibilidad logran un retorno de la inversión saludable, dado que los sitios accesibles suelen ser más rápidos, eficientes y fáciles de mantener [13].

Las empresas que implementan buenas prácticas de accesibilidad mejoran su alcance del mercado, ya que las personas con discapacidad representan cerca del 15 % de la población mundial, un grupo con poder adquisitivo creciente [14]. Asimismo, al diseñar sitios web accesibles, evitan el riesgo de fuertes multas y sanciones legales por incumplimiento de normativas [15].

Como línea de trabajo futuro, se propone ampliar la evaluación hacia otras secciones críticas del portal estudiantil con el fin de obtener una muestra más representativa del sitio completo, por ejemplo, evaluar la consulta de calificaciones, formularios de inscripción, o las páginas de trámites escolares.

Asimismo, se plantea complementar este análisis manual con métodos automáticos que, aunque se realizan mediante herramientas rápidas y eficaces, no siempre detectan todos los problemas, especialmente aquellos vinculados con la experiencia del usuario.

Finalmente, el estudio continuará con evaluaciones realizadas con usuarios en la Unidad de Accesibilidad Tecnológica de la institución. Las pruebas con personas con discapacidad permiten obtener una perspectiva real de las barreras que enfrentan al interactuar con el sitio, lo que, no solo valida los hallazgos previos, sino que también revela problemas que las evaluaciones automáticas y manuales no detectan. De este modo, se identifican inconvenientes de accesibilidad que solo son visibles mediante su aplicación conjunta, proporcionando un diagnóstico completo y fiable del estado real de accesibilidad del portal web.

Referencias

[1] P. Acosta-Vargas, T. Acosta, and S. Lujan-Mora, "Challenges to assess accessibility in higher education websites: A comparative study of Latin America universities," *IEEE Access*, vol. 6, pp. 36500–36508, 2018. https://doi.org/10.1109/access.2018.2848978 ↑

[2] Universidad Veracruzana, "Universidad Veracruzana," 2025. [Online]. Available: https://www.uv.mx ↑

[3] Secretaría de la Función Pública, "Acuerdo por el que se establecen las disposiciones generales de accesibilidad web que deben observar las dependencias y entidades de la Administración Pública Federal y las empresas productivas del Estado," *Diario Oficial de la Federación*, Mexico, 2015. [Online]. Available: https://www.imer.gob.mx/phpwrappers/NormatecaInterna/apitrck/uploads/acuerdo_establecen_disp_grales_accesibilidad_web_deben_obs_depend_entid_apf_empresas_produc_edo.pdf ↑

[4] M. Campoverde-Molina, S. Lujan-Mora, and L. V. Garcia, "Empirical studies on web accessibility of educational websites: A systematic literature review," *IEEE Access*, vol. 8, pp. 91676–91700, 2020. https://doi.org/10.1109/access.2020.2994288 ↑

[5] A. Nuñez, A. Moquillaza, and F. Paz, "Web accessibility evaluation methods: a systematic review," in *Design, User Experience, and Usability. Practice and Case Studies*, A. Marcus and E. Rosenzweig, Eds. Springer, Cham, 2019, pp. 226-237. https://doi.org/10.1007/978-3-030-23535-2_17 ↑

[6] W3C, "Understanding Conformance," 2025. [Online]. Available: https://www.w3.org/WAI/WCAG22/Understanding/conformance ↑

[7] W3C, "Web Content Accessibility Guidelines (WCAG) 2.2," 2024. [Online]. Available: https://www.w3.org/TR/WCAG22 ↑

[8] W3C, "Introduction to understanding WCAG 2.2," 2025. [Online]. Available: https://www.w3.org/WAI/WCAG22/Understanding/intro ↑

[9] W3C, "Website Accessibility Conformance Evaluation Methodology (WCAG-EM) 1.0," 2014. [Online]. Available: https://www.w3.org/TR/WCAG-EM/ ↑

[10] W3C, "WCAG-EM Report Tool: Website Accessibility Conformance Evaluation Report Tool," W3C Web Accessibility Initiative (WAI), 2024. [Online]. Available: https://www.w3.org/WAI/eval/report-tool/ ↑

[11] B. Martins and C. Duarte, "Large-scale study of web accessibility metrics," *Univ. Access Inf. Soc.*, vol. 22, pp. 1145–1159, 2022. https://doi.org/10.1007/s10209-022-00956-x ↑

[12] J. Lazar, D. F. Goldstein, and A. Taylor, *Ensuring Digital Accessibility through Process and Policy*. Burlington, MA, USA: Morgan Kaufmann, 2015. https://doi.org/10.1016/C2013-0-13367-3 ↑

[13] W3C, "The Business Case for Digital Accessibility," 2024. [Online]. Available: https://www.w3.org/WAI/business-case/ ↑

[14] World Health Organization, *World Report on Disability*, illustrated ed. Geneva, Switzerland: World Health Organization, 2011, ISBN: 978-92-4-156418-2.↑

[15] F. Filipe, I. M. Pires, and A. J. Gouveia, "Why web accessibility is important for your institution," *Procedia Comput. Sci.*, vol. 219, pp. 20–27, 2023. https://doi.org/10.1016/j.procs.2023.01.259 ↑

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.23438

REFLEXIÓN

Oportunidades del Aprendizaje Automático Adversarial (AML) para fortalecer la ciberseguridad de la IA en el contexto colombiano

Opportunities of Adversarial Machine Learning for Strengthening Cybersecurity of AI in Colombian context

Felipe Santiago Valderrama Ballesteros [1], Juan Manuel Cortés Jiménez [2] y Jorge Eliecer Camargo Mendoza [3]

Fecha de Recepción: 26 de marzo de 2025 **Fecha de Aceptación**: 18 de abril de 2026

Cómo citar: F.S. Valderrama-Ballesteros, J.M. Cortés Jiménez, y J.E. Camargo Mendoza, «Oportunidades del Aprendizaje Automático Adversarial (AML) para fortalecer la ciberseguridad de la IA en el contexto colombiano», *Tecnura*, vol. 30, n.° 88, jun. 2026. 69–84. https://doi.org/10.14483/22487638.23438

Resumen

Objetivo: revisar los fundamentos del Aprendizaje Automático Adversarial (AML) y evaluar su potencial para el refuerzo de la ciberseguridad en sistemas de Inteligencia Artificial (IA) en Colombia.

Metodología: se realizó una revisión documental analítica sobre ataques adversariales tradicionales y vulnerabilidades emergentes, con énfasis en la IA Generativa (inyección de *prompt*). Posteriormente, se analizó el marco regulatorio local (CONPES 4144) y se evaluaron cuatro casos de estudio representativos en los sectores de salud, agricultura, planeación pública y asistentes virtuales corporativos (*chatbots*).

Resultados: los sistemas de IA en Colombia enfrentan riesgos críticos que abarcan desde el fraude predictivo hasta la exfiltración de datos en Modelos de Lenguaje Grande (LLMs). Para mitigar estas amenazas es imperativo transitar hacia arquitecturas de seguridad por diseño y aplicar estrategias de AML adaptadas al entorno.

Conclusiones: la integración segura de la IA en el país requiere superar barreras estructurales significativas como la limitación presupuestal de las MiPymes, la escasez de talento técnico especializado y la actual fragmentación regulatoria. Superar estos retos dependerá de una colaboración estrecha entre el gobierno, el sector privado y la academia para consolidar un entorno digital resiliente.

Palabras clave: Aprendizaje Automático Adversarial, ciberseguridad, ataque cibernético, defensa cibernética, Inteligencia Artificial, inyección de prompt.

1 Estudiante del Departamento de Ingeniería de Sistemas e Industrial de la Universidad Nacional de Colombia. Miembro del grupo de investigación UNSECURLAB. Email: fvalderramab@unal.edu.co

2 Estudiante del Departamento de Ingeniería de Sistemas e Industrial de la Universidad Nacional de Colombia. Miembro del grupo de investigación UNSECURLAB. Email: jcortesj@unal.edu.co

3 Doctor en ingeniería y profesor asociado del Departamento de Ingeniería de Sistemas e Industrial de la Universidad Nacional de Colombia. Miembro del grupo de investigación UNSECURLAB. Email: jecamargom@unal.edu.co

Abstract

Objective: To review the fundamentals of Adversarial Machine Learning (AML) and evaluate its potential to strengthen the cybersecurity of Artificial Intelligence (AI) systems in Colombia.
Methodology: An analytical documentary review was conducted on traditional adversarial attacks and emerging vulnerabilities, focusing on Generative AI (prompt injection). Subsequently, the local regulatory framework (CONPES 4144) was analyzed, and four representative case studies were evaluated in the healthcare, agriculture, public planning, and corporate virtual assistants (chatbots) sectors.
Results: AI systems in Colombia face critical risks ranging from predictive fraud to data exfiltration in Large Language Models (LLMs). To mitigate these threats, it is imperative to transition towards security-by-design architectures and apply AML strategies adapted to the environment.
Conclusions: The secure integration of AI in the country requires overcoming significant structural barriers, such as the budget limitations of MSMEs, the shortage of specialized technical talent, and current regulatory fragmentation. Overcoming these challenges will depend on close collaboration among the government, the private sector, and academia to consolidate a resilient digital environment.
Keywords: Adversarial Machine Learning, Cybersecurity, Cyberattack, cyber defenses, Artificial Intelligence, prompt injection.

Introducción

La inteligencia artificial (IA), en especial el Aprendizaje Automático (ML del inglés *Machine Learning*), continúa siendo un motor de transformación en numerosos sectores: mejora la productividad, impulsa el desarrollo tecnológico, optimiza la atención al cliente y gestiona sistemas complejos, entre muchas otras aplicaciones. En Colombia, la adopción de estas tecnologías ha experimentado un notable crecimiento, lo cual ha impulsado el desarrollo económico y la modernización de diversos servicios [1].

Sin embargo, esta acelerada integración tecnológica, enmarcada en una adopción global sin precedentes [2], trae consigo nuevos desafíos en materia de ciberseguridad. La evolución hacia modelos más complejos, sumada a la reciente irrupción de la inteligencia artificial generativa (GenAI), ha ampliado significativamente la superficie de ataque. Informes recientes advierten que los ciberdelincuentes están explotando estas mismas tecnologías para identificar debilidades algorítmicas y escalar sus operaciones maliciosas [3], [4].

En respuesta a estas vulnerabilidades emergentes, la política pública CONPES 4144 para regular la inteligencia artificial en Colombia subraya el compromiso del Estado con el desarrollo ético y seguro de la inteligencia artificial [5]. Este documento no solo impulsa la adopción de la IA en el país, sino que también señala la necesidad de establecer medidas de seguridad robustas para proteger tanto a las infraestructuras críticas como a los usuarios. En este contexto, el estudio del Aprendizaje Automático Adversarial (AML del inglés *Adversarial Machine Learning*) se presenta como una oportunidad vital para anticipar y mitigar riesgos potenciales pues ofrece estrategias que permiten salvaguardar la integridad y confiabilidad de los sistemas inteligentes.

Este artículo explora los fundamentos del AML, abarcando tanto el aprendizaje automático tradicional como las vulnerabilidades emergentes de los modelos de lenguaje grande (LLM), e identifica las oportunidades que ofrece para reforzar la ciberseguridad en el contexto colombiano, a la vez que enfatiza en la importancia de un enfoque preventivo de la mano con la constante evolución tecnológica.

Para lograr este objetivo, se presentan inicialmente los fundamentos teóricos del AML. Posteriormente, se analizan los desafíos específicos que plantea el contexto colombiano a través de casos de estudio representativos, complementados con la formulación de estrategias de defensa adaptadas. Finalmente, se ofrecen conclusiones sobre los hallazgos encontrados.

Metodología

Este artículo de reflexión se deriva de una revisión documental analítica. Para su desarrollo, se diseñó un esquema metodológico estructurado en dos fases principales, orientadas a comprender las amenazas teóricas de la inteligencia artificial y evaluar su impacto potencial en el entorno nacional.

Revisión de fundamentos del AML

La primera fase consistió en una exploración de la literatura centrada en los conceptos teóricos del Adversarial Machine Learning, que abarcó tanto modelos clásicos como las vulnerabilidades emergentes de los Modelos de Lenguaje Grande (LLMs). Las acciones metodológicas iniciaron con la consulta de bases de datos académicas y repositorios reconocidos como *IEEE Xplore*, *Scopus* y *arXiv*, con el empleo de cadenas de búsqueda con términos clave como 'Adversarial Machine Learning', 'AI Cybersecurity', 'Data Poisoning', 'Evasion Attacks', 'Prompt Injection' y 'LLM Security'. Para abordar los avances más recientes en IA Generativa, la búsqueda sistemática se complementó con una técnica de minería de referencias, a través del análisis de las referencias bibliográficas de reportes técnicos de instituciones referentes (ej. NIST, OWASP, Microsoft) para identificar literatura académica de vanguardia sobre estrategias de mitigación [6], [7], [8]. El análisis se enfocó en categorizar los ejes temáticos según el nivel de conocimiento del atacante y el vector de ataque, lo cual consolidó un marco teórico robusto.

Análisis del contexto colombiano

La segunda fase tuvo como propósito contextualizar estos conceptos globales a la realidad tecnológica del país. Para llevar a cabo este análisis, el estudio se dividió en dos frentes: el entorno regulatorio y la aplicación práctica en la industria. En el frente regulatorio, se seleccionó y analizó la política pública CONPES 4144 [5], al ser el principal y más reciente instrumento gubernamental vigente que dicta los lineamientos éticos y de seguridad para la adopción de IA en Colombia. Por otro lado, para evaluar la materialización empírica de los riesgos, se realizó una selección de casos de estudio representativos en el territorio nacional. Dado que la documentación académica indexada sobre implementaciones locales

específicas de IA aún es emergente, la metodología incluyó la revisión de literatura gris y fuentes primarias corporativas y gubernamentales. Bajo este criterio, se analizaron cuatro casos de uso representativos del entorno nacional: ***Arkangel AI*** en el sector salud [9], ***Demetria*** en el sector agropecuario [10], las iniciativas predictivas del Departamento Nacional de Planeación (DNP) en el sector público [11], y el reciente despliegue de asistentes virtuales corporativos basados en IA Generativa en el Grupo Aval en alianza con Microsoft [12]. El análisis sobre estos casos consistió en identificar la criticidad de los datos que procesan y proyectar cómo las vulnerabilidades adversariales (desde la evasión clásica hasta la inyección de *prompts*) podrían afectar sus operaciones, justificando así la pertinencia de las estrategias de defensa sugeridas.

Resultados

Fundamentos del Adversarial Machine Learning

Según Vassilev, A et al. [6], el AML puede definirse como el estudio de técnicas que buscan comprometer el funcionamiento de sistemas de aprendizaje automático mediante la manipulación de datos de entrada o el modelo mismo, con el fin de inducir errores en las predicciones. Esta manipulación intencionada no sólo desafía la integridad de los modelos, sino que representa una preocupación real que puede generar serias afectaciones. Por ello, se describen las bases de estas técnicas y los principales ataques existentes.

Para empezar, los ejemplos adversariales se definen como "las entradas dadas a un modelo Aprendizaje Automático, intencionalmente diseñadas para causar errores en sus predicciones" [13]. Es decir, es la manipulación de los datos de entrada con el fin de generar predicciones incorrectas, con la particularidad de intentar ser lo menos detectable para los seres humanos. Por ejemplo, está la ya conocida imagen de Goodfellow, I et al. [14] que prueba un ejemplo adversarial en un modelo de clasificación de imágenes llamado GoogLeNet.

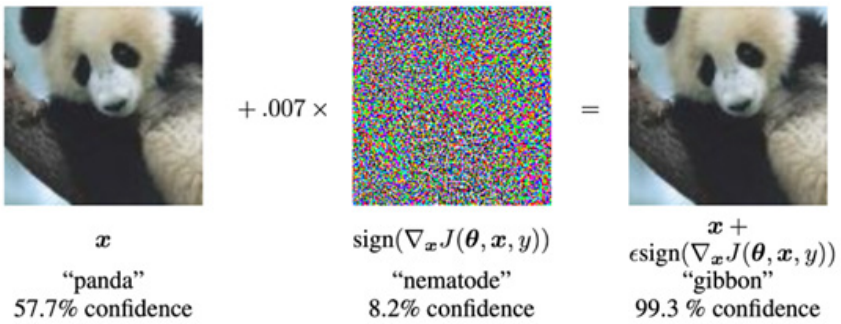

Figura 1. Ejemplo adversarial aplicado en el cual una pequeña perturbación imperceptible cambia la clasificación del modelo.

Fuente: Goodfellow, J. Shlens y C. Szegedy [14]

Esta perturbación de los datos es problemática para los modelos en diferentes niveles (de acuerdo con las características propias de su algoritmo). No obstante, en general mantienen un objetivo claro: alterar las predicciones del modelo; ahora bien, se pueden mencionar los tipos de ataques, que en términos generales buscan generar ejemplos adversariales y con esto afectar la integridad, disponibilidad o privacidad del modelo [6].

Existen diversas clasificaciones para cada tipo de ataque teniendo en cuenta diferentes factores. Vassilev, A et al. [6] los clasifica de acuerdo con el conocimiento del atacante:

- **Ataques de caja blanca:** el atacante posee un acceso total al modelo, en su arquitectura, hiper parámetros y conjuntos de datos de entrenamiento [6]. Aunque este tipo de casos no es tan probable, pueden servir como base para probar las vulnerabilidades del modelo, con el fin de observar los resultados respecto a los ejemplos adversariales y planificar qué acciones se pueden tomar para mitigar las posibles afectaciones al modelo. Wiyatno, R et al. [13] provee una extensa serie de técnicas usadas de acuerdo con el algoritmo de aprendizaje automático, destacándose las basadas en la Optimización del Gradiente o la Optimización Restringida.

- **Ataques de caja negra:** a diferencia de los anteriores, estos reflejan la situación contraria en la que los atacantes desconocen por completo los detalles de funcionamiento del modelo y solamente pueden acceder a la salida que este genera [13]. Debido a esto, este tipo es uno de los más comunes y sencillos de llevar a cabo.

- **Ataques de caja gris:** estos son un híbrido entre los de caja negra y blanca. En este escenario, el atacante tiene información parcial sobre el modelo, como por ejemplo el acceso a una distribución de datos similar a la usada para entrenar el modelo [6]. Por consiguiente, puede generar ejemplos adversariales con mayor efectividad.

A partir del conocimiento que posee un atacante, este puede utilizar diferentes ataques adversariales como los que se reseñan en la Tabla 1.

Con la reciente irrupción de la Inteligencia Artificial Generativa (GenAI), las técnicas adversariales han evolucionado más allá de la alteración de píxeles o datos numéricos, hasta abarcar ahora la manipulación del lenguaje natural. Los Modelos de Lenguaje Grande (LLMs) introducen nuevas superficies de ataque, siendo la inyección de *prompt* y el *jailbreaking* las amenazas más críticas, clasificadas por la *Open Web Application Security Project* (OWASP) como la vulnerabilidad principal en estas aplicaciones [7]. A diferencia de los ataques clásicos, estas técnicas explotan la inmensa flexibilidad lingüística del modelo para comprometer sistemas integrados, como arquitecturas de generación aumentada por recuperación (RAG) o agentes autónomos, con lo cual logran exfiltrar datos corporativos mediante instrucciones maliciosas de forma casi indetectable [16], [17].

Tabla 1. *Técnicas adversariales y sus descripciones*

Ataque	Descripción
Envenenamiento de datos	Introducción de datos maliciosos durante el entrenamiento de los modelos para comprometer su comportamiento [15]. Por ejemplo, introducir imágenes manipuladas en un modelo de clasificación para generar precisiones incorrectas que afecten su veracidad.
Evasión	Ingreso de datos alterados con el fin de "confundir" al modelo y que este genere predicciones incorrectas. La diferencia con el anterior es que estos ataques no se realizan durante el entrenamiento sino cuando el modelo está en una etapa productiva.
Extracción de modelos	Obtención de información sobre el modelo (sus parámetros o estructura) a través de consultas y técnicas de ingeniería inversa [15], con el único fin de encontrar vulnerabilidades y explotarlas.
Inyección de *prompt* (*Prompt Injection*)	Manipulación de las entradas de un Modelo de Lenguaje Grande (LLM) para evadir sus barreras de seguridad o extraer información sensible. Puede ser directa (por el usuario) o indirecta (oculta en documentos procesados por el modelo). Un subtipo crítico es el '*jailbreaking*', que fuerza al modelo a ignorar sus protocolos de seguridad [7], [16].

Fuente: Elaboración propia con base en Birch [15].

La comprensión detallada de estas técnicas adversariales, desde la evasión en algoritmos tradicionales hasta la manipulación semántica de los LLMs, trasciende la mera curiosidad teórica; constituye, pues, una herramienta analítica indispensable para evaluar la robustez de cualquier implementación. Al analizar estas vulnerabilidades con un enfoque crítico, resulta evidente que la simple adopción de modelos predictivos o generativos de terceros introduce riesgos sistémicos si no se auditan la calidad de los datos de entrenamiento o las superficies de interacción. Si bien estas amenazas representan retos significativos a nivel global, en el contexto colombiano adquieren matices particulares debido a factores como el nivel de madurez tecnológica de las infraestructuras, las capacidades específicas de los actores de ciberseguridad nacional y el marco regulatorio existente que sigue en desarrollo. Es precisamente esta intersección entre las vulnerabilidades algorítmicas y nuestra realidad institucional la que hace imperativo analizar cómo se están abordando estos desafíos desde la política pública.

Avances en política pública respecto a IA y ciberseguridad en Colombia

En Colombia, el uso de la inteligencia artificial ha aumentado en contextos gubernamentales, empresariales y cotidianos debido a su efecto disruptivo y las numerosas ventajas que trae implementarla. Esta adopción es clave para enfrentar "desafíos sociales, económicos y ambientales, tales como mejorar la seguridad alimentaria, reducir la pobreza, y avanzar hacia una economía basada en el conocimiento." [5]. Por esto, el gobierno ha centrado sus esfuerzos en la creación de una "Política Nacional sobre la Inteligencia Artificial, CONPES 4144" [5], la cual sirve como el insumo más adecuado para analizar los desafíos del AML en la ciberseguridad en Colombia.

Si bien el CONPES 4144 marcó un hito directivo fundamental, el ecosistema normativo colombiano se encuentra en una fase de rápida evolución legislativa para responder a las nuevas amenazas. Recientemente, este panorama ha comenzado a materializarse con iniciativas como la Ley 2502 de 2025, enfocada en penalizar severamente la suplantación de identidad agravada por el uso de IA, y el Proyecto de Ley 043 de 2025, que propone un marco de supervisión basado en categorías de riesgo y la creación de entornos de prueba controlados (*sandboxes*) para validar sistemas de manera segura [18], [19]. A pesar de estos notables avances, la academia e investigadores del sector advierten que el entorno regulatorio nacional aún es fragmentado [20]. Diversos análisis del ecosistema [21] coinciden en que el país enfrenta el enorme desafío de estructurar políticas que mitiguen los riesgos de ciberseguridad sin asfixiar la innovación tecnológica local.

Es precisamente debido a esta etapa de transición legislativa que los diagnósticos estructurales del documento CONPES 4144 mantienen plena vigencia. En él se exponen una serie de dificultades iniciales que están estrechamente relacionadas con las vulnerabilidades frente a ataques de AML en la ciberseguridad colombiana:

Falta de políticas públicas y regulación sobre IA y ciberseguridad

Quizás uno de los mayores desafíos es el no reconocer el riesgo latente, pues "En Colombia no se han generado políticas públicas específicas con respecto a los riesgos y efectos no deseados relacionados con la IA" [5]. Esto es un serio problema, ya que a pesar de que en la nueva política se mencionan avances en el tema, como la Política Nacional de Confianza y Seguridad Digital (CONPES 3995) [5], aún no hay una regulación específica que contemple los ataques adversariales a modelos de IA y su impacto en la seguridad nacional.

Infraestructura tecnológica vulnerable

Colombia tiene un obstáculo considerable: el país no posee la infraestructura adecuada para "desarrollar y operar de forma eficiente y sostenible los sistemas de IA" [5]. Es decir, el país tiene dificultades para abordar este tipo de avances tecnológicos y así mismo se encuentra en una posición vulnerable debido a ser uno de los países "con más ataques de ciberseguridad en Latinoamérica" [22]. Esto recalca la importancia de una mayor conciencia e inversión sobre la ciberseguridad en la infraestructura tecnológica del país.

Desconocimiento sobre la seguridad en el campo de la IA

A pesar del crecimiento en la adopción de la inteligencia artificial en sectores empresariales y gubernamentales, las estrategias de seguridad en estos sistemas no han avanzado al mismo ritmo. El documento CONPES 4144 advierte sobre el desconocimiento generalizado en torno a la seguridad digital

en los sistemas de IA, lo que representa una preocupación significativa [5]. Asimismo, diversos índices internacionales califican a Colombia como un país con un compromiso moderado en la implementación de políticas de ciberseguridad [5]. Esta brecha de conocimiento sugiere que muchos de los principales usuarios de IA, tanto a nivel institucional como individual, podrían no ser plenamente conscientes de las vulnerabilidades inherentes a estos sistemas ni de su posible explotación mediante ataques de AML.

El CONPES 4144 destaca una extensa serie de oportunidades de mejora para que el país pueda tener una adopción de la IA sostenible, segura y beneficiosa. No obstante, es importante mencionar que el principal desafío es la falta de concienciación y capacitación en seguridad digital, lo cual expone a organizaciones y ciudadanos a riesgos crecientes como la AML en entornos de IA. Por esto se resalta la necesidad de estrategias educativas y regulatorias para mitigar los impactos negativos de estas amenazas y garantizar una implementación responsable de la IA en Colombia.

Aplicaciones de la IA y ML en Colombia

Colombia ha mostrado un creciente interés en la adopción de tecnologías de inteligencia artificial, como se pudo evidenciar con el desarrollo de políticas públicas que regulen el tema. Sin embargo, aquí se enfatiza en tres aplicaciones puntuales de estas nuevas tecnologías en iniciativas nacionales para distintos sectores, a partir de su relevancia y beneficios para el contexto colombiano.

Caso 1: Sector de la salud

El ML está optimizando el diagnóstico y la gestión de recursos médicos. Un caso de estudio es el de la *startup* ***Arkangel AI***, empresa colombiana que emplea algoritmos de ML para analizar imágenes médicas y detectar enfermedades como malaria, leucemia y COVID-19 en segundos. Con esta tecnología se han realizado más de 21.000 detecciones en Colombia y otros países, mejorando el acceso a diagnósticos precisos en zonas rurales y urbanas [9]. Además, ***Arkangel AI*** ofrece estas soluciones como servicio, lo que permite que instituciones de salud creen modelos predictivos sin la necesidad de conocimientos técnicos, en un intento de democratizar el uso de la inteligencia artificial para esta área [23]. Su colaboración con entidades como UNICEF demuestra su impacto en la atención médica y su alineación con la necesidad de soluciones innovadoras en un país con desafíos de cobertura sanitaria.

Caso 2: Sector agropecuario

La agricultura colombiana también hace uso de técnicas de aprendizaje de máquina para mejorar sus procesos. Por ejemplo, la *startup* ***Demetria*** utiliza ML para analizar datos ambientales y de calidad, con el fin de ayudar a los productores a optimizar el sabor y la gestión del café en la cadena de suministro [10]. Además, investigaciones locales han aplicado ML para predecir el rendimiento de cosechas y clasificar

zonas aptas para el cultivo de cacao, lo cual fortalece la seguridad alimentaria y la economía rural [24], [25], [26]. Estas aplicaciones son vitales en un país cuyo sector agrícola es un pilar económico.

Caso 3: Sector Público

El gobierno colombiano ha integrado el ML para mejorar la eficiencia en la gestión pública. El Departamento Nacional de Planeación (DNP) emplea modelos predictivos para evaluar la viabilidad de proyectos de inversión, a través del análisis de más de 8.000 iniciativas históricas con un 76 % de precisión. Esta herramienta ha identificado proyectos inviables, con un potencial ahorro de $3 000 000 000 de pesos si se hubiera implementado antes [11]. El DNP planea expandir su uso a programas sociales, lo que refleja el potencial del ML para optimizar recursos y apoyar los objetivos del CONPES 4144 [5]. Como propuesta inicial, el gobierno colombiano, a través del MinTIC, ha impulsado la educación en ML como parte de su estrategia de transformación digital [27].

Caso 4: IA Generativa y asistentes virtuales en el sector corporativo

El ecosistema corporativo e institucional colombiano ha acelerado vertiginosamente la adopción de IA generativa, especialmente en la interacción con sus usuarios mediante asistentes virtuales y arquitecturas basadas en Modelos de Lenguaje Grande (LLMs). Organizaciones como Empresas Públicas de Medellín (EPM), a través de su asistente "Ema", o diversas entidades del sector financiero mediante la integración de herramientas corporativas como Copilot, evidencian una masificación de estos esquemas conversacionales [12], [21]. Paralelamente, el ecosistema de *startups* locales robustece esta oferta, lo cual amplía el acceso a asistentes impulsados por IA para el servicio al cliente y la optimización de procesos [21], [28].

Estas nuevas iniciativas de empresas salientes, junto con las propuestas gubernamentales, están posicionando a Colombia como un actor emergente en el ecosistema global de IA. Sin embargo, desafíos como la privacidad de datos, los sesgos en los modelos y la necesidad de educación continua deben abordarse para mitigar riesgos en un contexto en el que la adopción de estas tecnologías sigue creciendo y se busca maximizar los beneficios.

Riesgos y oportunidades de mejora

El aumento en la adopción de modelos de aprendizaje automático (ML) en Colombia, como se describió anteriormente, trae consigo riesgos asociados a vulnerabilidades que pueden ser explotadas mediante técnicas de *Adversarial Machine Learning* (AML). Estos riesgos, detallados en la sección de fundamentos, incluyen ataques como el envenenamiento de datos, la evasión y la extracción de modelos [29]. En este contexto, el AML no solo representa una amenaza, sino también una oportunidad para desarrollar estrategias de defensa que protejan los sistemas de IA, y el subsecuente fortalecimiento de la ciberseguridad en el país.

Vulnerabilidades en el contexto colombiano

Los modelos algorítmicos aplicados en sectores clave enfrentan riesgos específicos que varían según su arquitectura:

- En salud, un ataque de evasión mediante alteraciones imperceptibles a nivel de píxel en imágenes médicas puede engañar a los sistemas de clasificación diagnóstica para que emitan resultados erróneos con altísima confianza. Más allá del evidente riesgo vital para los pacientes, en el ámbito administrativo estas vulnerabilidades algorítmicas podrían ser explotadas para cometer fraudes a gran escala burlando los sistemas automatizados de reclamaciones y facturación del sistema de salud [30].

- En agricultura, los modelos predictivos dependen en gran medida de datos climáticos y registros empíricos provistos por los campesinos para optimizar el manejo de cultivos y mitigar riesgos asociados a fenómenos ambientales [24]. Un envenenamiento de estos conjuntos de datos podría alterar la evaluación de los entornos e inducir al algoritmo a recomendar decisiones catastróficas en la planificación agrícola, lo que amenazaría directamente la economía rural y la seguridad alimentaria regional.

- En políticas públicas, la manipulación de datos históricos o demográficos de entrada en modelos de ML del DNP [11] podría alterar las predicciones de éxito de los proyectos de infraestructura propuestos y desviar millonarios recursos públicos hacia obras inviables.

- En el sector corporativo y financiero, la reciente adopción de asistentes virtuales basados en LLMs introduce una superficie de ataque crítica. Como quedó demostrado con el descubrimiento de la vulnerabilidad EchoLeak (CVE-2025-32711) en plataformas como Microsoft 365 Copilot, los atacantes pueden lograr la exfiltración de datos corporativos privados y escalar privilegios sin interacción del usuario (*zero-click*), utilizando simplemente correos maliciosos diseñados para evadir los clasificadores de seguridad [31]. Para instituciones colombianas altamente integradas a estos ecosistemas, la inyección de *prompt* representa un riesgo de compromiso total.

Especialmente en el último caso, la magnitud de estas amenazas emergentes ha llevado a firmas de ciberseguridad a catalogar la inyección de *prompt* como "la nueva inyección SQL" [32]. Esta analogía advierte que, así como la inyección de código fue la vulnerabilidad reina en los inicios de las bases de datos web, la manipulación de instrucciones (*prompts*) se ha convertido en la vulnerabilidad número uno y fundacional en esta nueva era de la IA [7]. Para Colombia, donde el costo promedio de una brecha de datos podría desestabilizar severamente a las organizaciones locales [33], la contención se vuelve una urgencia. Estas vulnerabilidades se agravan por factores intrínsecos como la infraestructura tecnológica limitada y el desconocimiento generalizado sobre seguridad en IA, ambos señalados en el CONPES 4144 [5]. Además, dado que Colombia se posiciona como uno de los países con más ataques cibernéticos en América Latina [22], la necesidad de implementar defensas robustas es inaplazable.

Estrategias de defensa

Para contrarrestar estos riesgos, se proponen las siguientes estrategias basadas en AML, adaptadas al contexto colombiano:

1. **Entrenamiento adversarial**

   Esta técnica consiste en entrenar modelos con ejemplos adversariales para aumentar su resistencia a manipulaciones [29]. Por ejemplo, en el sector salud, fortalecería la robustez de modelos predictivos frente a alteraciones en imágenes médicas en la fase de entrenamiento de los modelos.

2. **Destilación defensiva**

   Se refiere al uso de un modelo secundario para reducir la sensibilidad a perturbaciones [34]. En el sector público, su aplicación ayudaría a estabilizar las predicciones del DNP, protegiendo la asignación de recursos y con ello la viabilidad de los proyectos de inversión.

3. **Privacidad diferencial**

   Consiste en añadir ruido estadístico para proteger datos sensibles y mitigar ataques [35]. Aplicada al ecosistema sanitario, podría salvaguardar información confidencial de los pacientes frente a intentos de extracción.

4. **Monitoreo continuo**

   Detección de anomalías y desviaciones en el rendimiento del modelo en producción, que indiquen probables ataques [36]. En el agro, identificaría envenenamiento en predicciones de cosechas, asegurando su integridad.

5. **Defensa en profundidad (*Defense in Depth*) para sistemas de IA generativa**

   La naturaleza autorregresiva de los LLMs impide garantizar la seguridad con una sola barrera [37]. Es imperativo adoptar arquitecturas multicapa que incluyan el particionamiento de instrucciones (como la técnica de *Spotlighting* [8], [38]), filtros rigurosos de entrada y salida (*guardrails*), y estrictas políticas de control de acceso basadas en el principio de menor privilegio [31].

6. **Auditoría y estandarización normativa (seguridad por diseño)**

   Adoptar marcos internacionales como el OWASP Top 10 for GenAI [7] o los catálogos de tácticas de MITRE ATLAS [17] funcionaría como una defensa preventiva fundamental. Estos lineamientos

proporcionan reglas arquitectónicas estrictas que permiten a los equipos de desarrollo realizar pruebas de estrés (*Red Teaming*) e identificar vulnerabilidades antes de que el modelo salga a producción. Es decir, evitan que las organizaciones desplieguen sistemas con fallos de diseño estructurales, pasando de una seguridad reactiva a una resiliencia planificada y auditable.

Estas estrategias de defensa señalan oportunidades de mejora tangibles para la robustez de los modelos presentes en el contexto colombiano. Sin embargo hay que tener en cuenta algunas consideraciones para implementar con éxito dichas estrategias: primero, es crucial formar profesionales en de AML y ciberseguridad, aspecto que hay que tener en cuenta en los programas de capacitación como los que se están adelantando por parte del MinTIC [27], lo cual demanda más inversión en el área de la tecnología; segundo, dado que ninguna estrategia es infalible por sí sola, lo recomendable es combinar múltiples enfoques para lograr una protección más robusta, adaptada a los posibles desafíos del contexto colombiano [29].

Conclusiones

La creciente integración de la inteligencia artificial en Colombia representa una oportunidad transformadora para impulsar la innovación en sectores estratégicos. Sin embargo, la evolución desde el aprendizaje automático tradicional hacia la adopción masiva de modelos generativos (LLMs) ha expandido drásticamente la superficie de ataque, posicionando vulnerabilidades como la inyección de *prompt* como riesgos sistémicos para las organizaciones [7]. Aunque aún no se han documentado incidentes específicos de ataques adversariales en el país, las vulnerabilidades inherentes de los modelos de inteligencia artificial hacen indispensable adoptar estrategias preventivas. Ante esta realidad, la incorporación de técnicas derivadas del *Adversarial Machine Learning* (AML) deja de ser una opción teórica para convertirse en un imperativo operativo.

No obstante, materializar estas defensas preventivas en el contexto colombiano trasciende la voluntad técnica y se enfrenta a barreras estructurales específicas. En primer lugar, existe una profunda barrera económica: los altos costos asociados al despliegue de infraestructuras de ciberseguridad avanzadas, auditorías algorítmicas y monitoreo continuo resultan prohibitivos para las micro, pequeñas y medianas empresas (MiPymes). Estas empresas constituyen la base del tejido empresarial del país y, al adoptar aceleradamente estas nuevas tecnologías sin el presupuesto adecuado para asegurarlas, quedan altamente expuestas a posibles vulneraciones [21]. En segundo lugar, Colombia enfrenta una aguda escasez de talento humano especializado [21]; el ecosistema requiere urgentemente profesionales capacitados no solo en ciberseguridad tradicional, sino en pruebas de estrés adversarial *(Red Teaming*) y mitigación de amenazas nativas de la IA. Finalmente, la actual fragmentación y transición del marco regulatorio nacional genera un escenario de incertidumbre que dificulta la adopción estandarizada de políticas de seguridad corporativa [20].

Superar estos obstáculos estructurales exige que el impulso normativo actual, ejemplificado en el CONPES 4144 y las iniciativas legislativas en curso, se materialice mediante una colaboración articulada entre el gobierno, el sector privado y la academia. Esta sinergia es vital para democratizar el acceso a herramientas de defensa, replicar modelos internacionales de aseguramiento (como *Project Glasswing* [39] o los marcos de MITRE ATLAS [17]) y fomentar programas de capacitación técnica y retención de talento en el país.

En definitiva, el camino a seguir para Colombia no es frenar la adopción de la inteligencia artificial ante el panorama adversarial, sino blindar su integración. Asumir la seguridad por diseño, cerrar la brecha de talento especializado y consolidar un marco regulatorio unificado son pasos ineludibles para garantizar que el avance tecnológico se traduzca en beneficios sostenibles, competitivos y seguros para la sociedad colombiana.

Referencias

[1] Fedesoft, "Colombia avanza en la adopción de la Inteligencia Artificial Generativa," Fedesoft. Accessed: Apr. 16, 2026. [Online]. Available: https://fedesoft.org/colombia-avanza-en-la-adopcion-de-la-inteligencia-artificial-generativa-el-29-de-las-empresas-estan-en-fase-de-experimentacion-activa-revela-sondeo-de-fedesoft/

[2] Stanford HAI, "The 2026 AI Index Report," Stanford University Human-Centered Artificial Intelligence. Accessed: Apr. 16, 2026. [Online]. Available: https://hai.stanford.edu/ai-index/2026-ai-index-report

[3] IBM, "IBM 2026 X-Force Threat Index: AI-Driven Attacks are Escalating as Basic Security Gaps Leave Enterprises Exposed," IBM Newsroom. Accessed: Apr. 16, 2026. [Online]. Available: https://newsroom.ibm.com/2026-02-25-ibm-2026-x-force-threat-index-ai-driven-attacks-are-escalating-as-basic-security-gaps-leave-enterprises-exposed

[4] P. Girnus, V. Ciancaglini, M. Swimmer, D. Fiser, A. Oliveira, and B. Zigh, "Fault Lines in the AI Ecosystem: TrendAI™ State of AI Security Report | Trend Micro (US)," Trend. Accessed: Apr. 16, 2026. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/fault-lines-in-the-ai-ecosystem-trendai-state-of-ai-security-report

[5] G. F. Petro Urrego *et al.*, *CONPES 4144: POLÍTICA NACIONAL DE INTELIGENCIA ARTIFICIAL*. 2025. [Online]. Available: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

[6] A. Vassilev, A. Oprea, A. Fordyce, H. Anderson, X. Davies, and M. Hamin, "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," National Institute of Standards and Technology, Gaithersburg, MD, NIST AI 100-2e2025, 2025. doi: https://doi.org/10.6028/NIST.AI.100-2e2025

[7] OWASPGenAIProject Editor, "LLM01:2025 Prompt Injection," OWASP Gen AI Security Project. Accessed: Apr. 15, 2026. [Online]. Available: https://genai.owasp.org/llmrisk/llm01-prompt-injection/

[8] A. Paverd, "How Microsoft defends against indirect prompt injection attacks," Microsoft. Accessed: Apr. 16, 2026. [Online]. Available: https://www.microsoft.com/en-us/msrc/blog/2025/07/how-microsoft-defends-against-indirect-prompt-injection-attacks

[9] J. Zea, "Arkangel Ai AI use cases for HealthCare." Aug. 15, 2025. [Online]. Available: https://arkangel.ai/en/research/arkangel-ai-predictive-models-reduce-hospital-admissions-45-68-million-chronic-patients

[10] "Sobre Demetria," Demetria. Accessed: Apr. 16, 2026. [Online]. Available: https://www.demetria.ag/colombia/sobre-a-demetria

[11] Emilio, "Machine Learning enhances Public Policy in Colombia," Technology and Operations Management. Accessed: Apr. 16, 2026. [Online]. Available: https://d3.harvard.edu/platform-rctom/submission/machine-learning-enhances-public-policy-in-colombia/

[12] News Center Microsoft Latinoamérica, "Grupo Aval y Microsoft se unen para impulsar la revolución de la inteligencia artificial en todas sus entidades," News Center Latinoamérica. Accessed: Apr. 16, 2026. [Online]. Available: https://news.microsoft.com/es-xl/grupo-aval-y-microsoft-se-unen-para-impulsar-la-revolucion-de-la-inteligencia-artificial-en-todas-sus-entidades/

[13] R. R. Wiyatno, A. Xu, O. Dia, and A. de Berker, "Adversarial Examples in Modern Machine Learning: A Review," Nov. 15, 2019, *arXiv*: arXiv:1911.05268. doi: https://doi.org/10.48550/arXiv.1911.05268

[14] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," Mar. 20, 2015, *arXiv*: arXiv:1412.6572. doi: https://doi.org/10.48550/arXiv.1412.6572

[15] L. Birch, "AI Under Attack: Six Key Adversarial Attacks and Their Consequences," Mindgard. Accessed: Apr. 16, 2026. [Online]. Available: https://mindgard.ai/blog/ai-under-attack-six-key-adversarial-attacks-and-their-consequences

[16] S. Gulyamov *et al.*, "Prompt Injection Attacks in Large Language Models and AI Agent Systems: A Comprehensive Review of Vulnerabilities, Attack Vectors, and Defense Mechanisms," *Information*, vol. 17, no. 1, p. 54, Jan. 2026, doi: https://doi.org/10.3390/info17010054

[17] The MITRE Corporation, "Case Studies | MITRE ATLAS™." Accessed: Apr. 16, 2026. [Online]. Available: https://atlas.mitre.org/studies

[18] *Ley 2502 de 2025 Congreso de la República de Colombia*. Accessed: Apr. 16, 2026. [Online]. Available: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?dt=S&i=188454

[19] MINCIENCIAS, *Proyecto de Ley "Por medio del cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético y responsable y se dictan otras disposiciones"*. 2025. Accessed: Apr. 16, 2026. [Online]. Available: https://minciencias.gov.co/sites/default/files/upload/noticias/pl_ia_finalizado.pdf

[20] A. S. Barliza, I. C. Gómez, J. M. Caballero, and S. V. Muñoz, "Towards a National Artificial Intelligence Policy in Colombia: A Comparative Analysis of International Frameworks," *OnBoard Knowl. J.*, pp. 1–13, Feb. 2026, doi: https://doi.org/10.70554/OBJK2025.v01n01.02

[21] S. Defelipe Díaz, "IA en Colombia: Innovación y casos de éxito reciente," Impacto TIC. Accessed: Apr. 16, 2026. [Online]. Available: https://impactotic.co/inteligencia-artificial/ia-en-colombia-innovacion-y-casos-de-exito-reciente/

[22] Forbes Staff, "Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM," Forbes Colombia. Accessed: Apr. 16, 2026. [Online]. Available: https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica/

[23] J. Zea, "2024_Hippocrates_Ark_Whitepaper." Aug. 15, 2025. [Online]. Available: https://arkangel.ai/en/research/no-code-hippocrates-automl-builds-pediatric-leukemia-ai-models-tenfold-faster

[24] J. Cock, D. Jiménez, H. Dorado, and T. Oberthür, "Operations research and machine learning to manage risk and optimize production practices in agriculture: good and bad experience," *Curr. Opin. Environ. Sustain.*, vol. 62, p. 101278, Jun. 2023, doi: https://doi.org/10.1016/j.cosust.2023.101278

[25] C. A. Ramírez Gómez, "Aplicación del Machine Learning en agricultura de precisión," *Rev. CINTEX*, vol. 25, no. 2, pp. 14–27, Dec. 2020, doi: https://doi.org/10.33131/24222208.356

[26] L. Talero-Sarmiento, S. Roa-Prada, L. Caicedo-Chacon, and O. Gavanzo-Cardenas, "A Data-Driven Approach to Improve Cocoa Crop Establishment in Colombia: Insights and Agricultural Practice Recommendations from an Ensemble Machine Learning Model," *AgriEngineering*, vol. 7, no. 1, p. 6, Jan. 2025, doi: https://doi.org/10.3390/agriengineering7010006

[27] J. D. Ayazo, "Formación gratuita en ciencia de datos e IA – Convocatorias," Impacto TIC. Accessed: Apr. 16, 2026. [Online]. Available: https://impactotic.co/innovacion/convocatorias-tic/oportunidad-para-formarse-de-manera-gratuita-en-ciencia-de-datos-e-ia-convocatorias/

[28] Redacción Canal Trece Colombia, "Inteligencia Artificial hecha en Colombia: empresas y creadores que están marcando la diferencia | Canal Trece." Accessed: Apr. 16, 2026. [Online]. Available: https://canaltrece.com.co/noticias/inteligencia-artificial-hecha-en-colombia-empresas-y-creadores-que-estan-marcando-la-diferencia/

[29] J. E. Fonseca Núñez and Nestlé Global Cyber SOC, "Adversarial Machine Learning for Cyber Security," MASTER'S DEGREE THESIS, Universitat Politecnica de Catalunya Barcelonatech, 2022. [Online]. Available: https://upcommons.upc.edu/server/api/core/bitstreams/5a8cde84-4c2c-4ee4-9a2b-ac74cbca634c/content

[30] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," *Science*, vol. 363, no. 6433, pp. 1287–1289, Mar. 2019, doi: https://doi.org/10.1126/science.aaw4399

[31] P. Reddy and A. S. Gujral, "EchoLeak: The First Real-World Zero-Click Prompt Injection Exploit in a Production LLM System," Sep. 06, 2025, *arXiv*: arXiv:2509.10540. doi: https://doi.org/10.1609/aaaiss.v7i1.36899

[32] G. Tziakouris and Y. Kramarz, "Prompt injection is the new SQL injection, and guardrails aren't enough," Cisco Blogs. Accessed: Apr. 16, 2026. [Online]. Available: https://blogs.cisco.com/ai/prompt-injection-is-the-new-sql-injection-and-guardrails-arent-enough

[33] IBM, "Cost of a data breach 2025 | IBM." Accessed: Apr. 16, 2026. [Online]. Available: https://www.ibm.com/reports/data-breach

[34] P. Bountakas, A. Zarras, A. Lekidis, and C. Xenakis, "Defense strategies for Adversarial Machine Learning: A survey," *Comput. Sci. Rev.*, vol. 49, p. 100573, Aug. 2023, doi: https://doi.org/10.1016/j.cosrev.2023.100573

[35] G. W. Muoka *et al.*, "A Comprehensive Review and Analysis of Deep Learning-Based Medical Image Adversarial Attack and Defense," *Mathematics*, vol. 11, no. 20, p. 4272, Jan. 2023, doi: https://doi.org/10.3390/math11204272

[36] Y. Wang *et al.*, "Adversarial Attacks and Defenses in Machine Learning-Powered Networks: A Contemporary Survey," arXiv.org. Accessed: Apr. 16, 2026. [Online]. Available: https://arxiv.org/abs/2303.06302v1

[37] M. Russinovich, A. Salem, S. Zanella-Béguelin, and Y. Zunger, "The Price of Intelligence: Three risks inherent in LLMs," *Queue*, vol. 22, no. 6, pp. 38–61, Dec. 2024, doi: https://doi.org/10.1145/3711679

[38] K. Hines, G. Lopez, M. Hall, F. Zarfati, Y. Zunger, and E. Kiciman, "Defending Against Indirect Prompt Injection Attacks With Spotlighting," Mar. 20, 2024, *arXiv*: arXiv:2403.14720. doi: https://doi.org/10.48550/arXiv.2403.14720

[39] "Project Glasswing: Securing critical software for the AI era," Anthropic. Accessed: Apr. 16, 2026. [Online]. Available: https://www.anthropic.com/glasswing

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.24853

REVISIÓN

Ciberseguridad cuántica en sistemas ciberfísicos e infraestructuras críticas: un estado del arte

Quantum Cybersecurity in Cyber-Physical Systems and Critical Infrastructures: A State of the Art

Katerine Márceles Villalba [1], César Pardo Calvache [2] y Siler Amador Donado [3]

Fecha de Recepción: 12 de noviembre de 2025 **Fecha de Aceptación**: 12 de marzo de 2026

Cómo citar: K.M. Villalba, C. Pardo Calvache, S.A. Donado, «Ciberseguridad cuántica en sistemas ciberfísicos e infraestructuras críticas: un estado del arte», *Tecnura*, vol. 30, n.° 88, jun. 2026. 85–101. https://doi.org/10.14483/22487638.24853

Resumen

Contexto: este artículo presenta la creciente vulnerabilidad de los sistemas ciberfísicos en las infraestructuras críticas, producto del avance de la computación cuántica. Esta tecnología pone en entredicho los esquemas actuales de criptografía y coloca en riesgo servicios como la energía, la salud y otros esenciales para la sociedad.
Objetivo: caracterizar los estándares, marcos de trabajo y las vulnerabilidades emergentes encontradas en estudios científicos publicados en el período 2020-2025.
Metodología: marco metodológico basado en una revisión sistemática de la literatura, utilizando los protocolos PRISMA y Kitchenham. A través de este método, se eligieron un total de 40 estudios primarios.
Resultados: la revisión evidencia que, aunque normativas como ISO/IEC 27001 e IEC 62443 son ampliamente adoptadas, carecen de medidas de control específicas frente a amenazas cuánticas como los algoritmos de Shor y Grover. Asimismo, se identificó una desconexión entre los modelos taxonómicos actuales y la protección técnica de activos operativos.
Conclusiones: la investigación concluye que existe una urgencia por integrar la criptografía postcuántica y desarrollar marcos de gobernanza adaptativa que fortalezcan la resiliencia en las infraestructuras críticas. Finalmente, se propuso una hoja de ruta para la creación de modelos ontológicos que unifiquen la gestión de riesgos en esta era tecnológica.
Palabras clave: Ciberseguridad, Cuántica, Infraestructuras críticas, sistemas ciber-físicos.

Abstract

Context: This article presented the growing vulnerability of cyber-physical systems (CPS) in critical infrastructures resulting from the advancement of quantum computing. This technology challenges current cryptographic schemes and puts services such as energy, healthcare, and other essential social sectors at risk.

1 Ingeniera de Sistemas y Magíster en Seguridad Informática. Miembro del grupo de investigación In2Lab. Universidad de Antioquia. Email: katerine.marceles@udea.edu.co

2 Ingeniero de Sistemas y PhD. en Tecnologías Informáticas Avanzadas. Miembro del grupo de investigación GTI. Universidad del Cauca. Email: cpardo@unicauca.edu.co

3 Ingeniero de Sistemas y PhD. (c) Ciencias de la Computación. Miembro del grupo de investigación GTI. Universidad del Cauca. Email: samador@unicauca.edu.co

Objective: The goal was to characterize the standards, frameworks, and emerging vulnerabilities found in scientific studies published during the 2020-2025 period.
Methodology: The study was conducted through a methodological framework based on a systematic literature review using the PRISMA and Kitchenham protocols. Through this method, a total of forty primary studies were selected.
Results: The analysis evidenced that , although standards such as ISO/IEC 27001 and IEC 62443 are widely adopted, they lack specific control measures against quantum threats such as the Shor and Grover algorithms. Furthermore, a disconnection was identified between current taxonomic models and the technical protection of operational assets.
Conclusions: The research concluded that there is an urgent need to integrate post-quantum cryptography and develop adaptive governance frameworks to strengthen resilience in critical infrastructures. Finally, a roadmap was proposed for the creation of ontological models to unify risk management in this technological era.
Keywords: Cybersecurity, Critical Infrastructures, Cyber-physical systems, Quantum.

Introducción

La ciberseguridad en infraestructuras críticas (IC) se ha consolidado como campo estratégico para garantizar la continuidad y la estabilidad de servicios esenciales en la sociedad [1]. Infraestructuras como la energética, la sanitaria, las de agua o transporte están cada vez más integradas con sistemas ciber-físicos (SCF) que articulan componentes digitales y físicos para el monitoreo y control automatizado de procesos [2]. Los SCF son entornos en los cuales los sistemas computacionales interactúan con procesos físicos mediante sensores, actuadores y redes de comunicación, lo que los hace fundamentales, pero altamente vulnerables ante ciberataques. De hecho, esta integración ha ampliado la superficie de ataque y ha aumentado la exposición ante amenazas que pueden impactar tanto los sistemas de información como los dispositivos físicos que controlan entornos sensibles [3]. A pesar de su importancia, la protección de los SCF en entornos críticos aún presenta desafíos metodológicos y técnicos significativos. Actualmente es posible observar la falta de marcos formales de evaluación, así como de metodologías para la prevención de ataques avanzados [4].

La computación cuántica, entendida como un paradigma que utiliza principios de la mecánica cuántica para procesar información, ha generado nuevas amenazas en términos de ciberseguridad, ya que pone en riesgo los algoritmos criptográficos actuales. En particular, el algoritmo de Shor permite factorizar números grandes en tiempo polinomial, comprometiendo la seguridad de sistemas como RSA (Rivest-Shamir-Adleman) y ECC (Criptografía de Curva Elíptica), mientras que el algoritmo de Grover reduce drásticamente el tiempo de búsqueda en claves simétricas, lo cual afecta la fortaleza de mecanismos como AES (Advanced Encryption Standard)[4], [14].

La aparición de nuevas tecnologías disruptivas, como la computación cuántica, abre una línea de riesgo emergente para los mecanismos criptográficos tradicionales, especialmente en contextos en los cuales la seguridad y la disponibilidad son requisitos no negociables. Esto genera la necesidad revisar las medidas de seguridad, no solo desde una perspectiva técnica, sino también desde la planificación

estratégica al interior de las IC. Por tanto, la ausencia de una visión articulada de los SCF y las amenazas cuánticas ha desencadenado una serie de riesgos en el desarrollo de nuevas políticas, tecnologías y prácticas.

Entre estos riesgos se destacan: (i) decisiones de seguridad basadas en artefactos obsoletos [1], [10], [26], (ii) la subestimación de las vulnerabilidades emergentes [4], [14], (iii) la ausencia de estándares de protección cuántica [13], [15], (iv) inversiones en soluciones no escalables [13], [12], [26], (v) el diseño de infraestructuras centrado en la seguridad no postcuántica [4], [14], [24], (vi) la desarticulación entre sectores industriales y científicos [10], [13], [27], (vii) las limitaciones para generar respuestas resilientes [9], [22], [28]. Durante los últimos años se han realizado estudios relevantes que exploran temas como la seguridad en SCF, el uso de inteligencia artificial para defensa, y la criptografía resistente a computadoras cuánticas. En virtud de ello, revisiones previas como las de Amador et al. [24] y Borja Rivadeneira y Gómez [25] evidenciaron que aún son escasos los estudios que integran de forma articulada los tres dominios: SCF, IC y ciberseguridad cuántica, lo que constituye una brecha en el conocimiento actual.

Por consiguiente, este artículo se enfoca en la estructuración del estado del arte, basado en la necesidad de comprender la seguridad de SCF en IC ante la llegada de la era cuántica. Dado a lo anterior, el objetivo principal fue caracterizar los estándares, marcos de trabajo y vulnerabilidades emergentes reportadas en la literatura científica (comprendida entre los periodos 2020–2025) sobre ciberseguridad cuántica en SCF e IC, identificando brechas, patrones y enfoques metodológicos predominantes. Para ello, se siguió un protocolo híbrido basado en PRISMA 2020 [5] y en las directrices metodológicas de Kitchenham [6].

El resto del artículo se estructura así: la Sección 2 describe el protocolo metodológico; la Sección 3 presenta los resultados obtenidos; la Sección 4 desarrolla la discusión y limitaciones a partir de los hallazgos y la Sección 5 presenta las conclusiones y proyecciones futuras.

Metodología

Para la estructuración del estado del arte se adoptó un protocolo híbrido fundamentado en los lineamientos metodológicos de Kitchenham y Brereton [6] y PRISMA 2020 [5], complementado con el modelo GQM (Goal-Question-Metric). Este enfoque combina la rigurosidad conceptual del primero, orientado a la ingeniería del conocimiento, con la trazabilidad y transparencia del segundo, propio de revisiones en ciencias aplicadas. De esta manera, se minimizaron los sesgos en la formulación de preguntas, la selección de fuentes, la evaluación de pertinencia y la delimitación de objetivos. En el siguiente repositorio en Zenodo: https://doi.org/10.5281/zenodo.16944681, se presenta gráficamente el flujo de actividades realizadas durante la revisión. La metodología abordó literatura científica publicada entre los años 2020 y 2025, y se focalizó en estudios que articulan la intersección entre SCF, ciberseguridad e

impactos de la computación cuántica en IC. A pesar del esfuerzo por priorizar literatura revisada por pares, la escasez de investigaciones específicas sobre ciberseguridad cuántica en SCF e IC requirió complementar la búsqueda con fuentes emergentes de alto impacto, lo que permitió fortalecer la caracterización del dominio estudiado.

Las actividades desarrolladas en cada etapa del protocolo aplicadas al tema de dominio central fueron:

- *Objetivo de búsqueda y preguntas de investigación:* el objetivo (Ob) principal de este estado del arte fue analizar los estándares, marcos de trabajo y prácticas de ciberseguridad aplicados a SCF e IC, con el fin de caracterizar los requerimientos asociados con la gestión de las amenazas en la era cuántica. Para ello, se establecieron los siguientes objetivos de búsqueda:

Ob1: caracterizar los tipos de estándares y marcos de trabajo aplicados a SCF e IC mediante una búsqueda estructurada en bases académicas relevantes.

Ob2: identificar vulnerabilidades emergentes derivadas de la computación cuántica que afectan a SCF e IC a partir de una revisión de literatura.

Las preguntas que guiaron el desarrollo del estado del arte se formularon bajo el método Goal-Question-Metric (GQM) [6] presentados en la Tabla 1, combinando los criterios de refinamiento del enfoque PICOC [7] y la validación mediante FINER[8], lo que garantizó su viabilidad, interés y relevancia. Las preguntas fueron validadas por expertos antes de ser aplicadas y respondidas con el análisis de los estudios primarios.

Tabla 1. *Pregunta, métrica y motivación.*

ID	Pregunta	Métrica	Motivación
Ob1.	P1: ¿Cuáles son los principales estándares y marcos de trabajo utilizados en la ciberseguridad de SCF y IC?	Número de estándares y marcos de trabajo documentados que abordan la ciberseguridad en SCF e IC.	Identificar los marcos de referencia permite establecer las bases normativas y técnicas sobre las cuales se construyen las prácticas de seguridad actuales, y evaluar su pertinencia ante nuevos desafíos como la era cuántica.
Ob2.	P2: ¿Qué vulnerabilidades asociadas con la computación cuántica están emergiendo en la ciberseguridad de SCF e IC?	Número de vulnerabilidades cuánticas identificadas en el contexto de ataques de red a SCF e IC.	Comprender las vulnerabilidades emergentes asociadas a la computación cuántica para anticipar riesgos futuros.

Abreviaciones utilizadas: Objetivo (Ob), Pregunta (P).

Fuente: elaboración propia.

- *Búsqueda de literatura:* las fuentes de búsqueda seleccionadas fueron: *Scopus*, *Springer* y *Google Scholar*, escogidas por su pertinencia temática, disponibilidad de literatura actualizada y revisada por pares. Google Scholar se utilizó para acceder a investigaciones emergentes, debido a su cobertura y acceso abierto, lo que facilitó una búsqueda amplia y estructurada, así como el rastreo de estudios relevantes mediante funciones de citación, filtros por año y tipo de documento. En consecuencia, este enfoque permitió acceder a investigaciones que, aunque no siempre registradas en las bases principales, sí estaban revisadas por pares y vinculadas a dominios especializados de SCF y ciberseguridad cuántica.

La Tabla 2 presenta la cadena de búsqueda básica , construida a partir de los términos clave definidos en el protocolo y optimizada según el esquema PICOC. En el siguiente repositorio en Zenodo: https://doi.org/10.5281/zenodo.17129173 se presenta el PICOC definido para la cadena de búsqueda de este estado del arte.

Tabla 2. *Cadena de búsqueda básica.*

"cyber-physical systems" **OR** "CPS" **AND** "cybersecurity evaluation model" **OR** "ontology evaluation model" **OR** "assessment model" **OR** "quantum cybersecurity model" **AND** "best practices" **OR** "cybersecurity frameworks" **AND** "quantum era" **OR** "critical infrastructure"

Fuente: elaborción propia.

La cadena de búsqueda se adaptó cuidadosamente para cada fuente seleccionada, para garantizar la consistencia en el uso de operadores booleanos y la compatibilidad con los parámetros específicos de cada buscador. En el repositorio disponible en Zenodo (https://doi.org/10.5281/zenodo.17545367) se puede consultar la versión específica de la cadena para cada plataforma. Durante el proceso, se identificaron un total de 420 artículos. De estos, se eliminaron 7 por duplicación, quedando 413. Posteriormente, se evaluaron preliminarmente por título y resumen, con lo cual se redujo el conjunto a 140 artículos. Finalmente, tras aplicar los criterios de inclusión y exclusión definidos en la Tabla 3, se seleccionaron 64 estudios relevantes.

La distribución de artículos por fuente fue: Google Scholar: 256 identificados, 130 incluidos preliminarmente, 54 relevantes; Springer: 89 identificados, 10 relevantes; Scopus: 75 identificados, 0 relevantes. Este resultado reflejó dos aspectos clave: por un lado, la escasa representación de literatura especializada en ciberseguridad cuántica dentro de bases como Scopus; y por otro, la importancia de incluir buscadores más amplios como Google Scholar en revisiones sistemáticas sobre áreas en rápido desarrollo.

Cabe resaltar que varios artículos identificados en Google Scholar provenían de congresos de alto impacto y revistas indexadas no necesariamente cubiertas por Scopus, lo cual refuerza su valor como repositorio complementario. De esta forma, se garantizó la cobertura de literatura emergente relevante en dominios como criptografía post-cuántica y evaluación ontológica aplicada a SCF e IC.

Tabla 3. Criterios de inclusión y exclusión.

Criterios de Inclusión	Criterios de Exclusión
Artículos sobre ciberseguridad en sistemas ciber-físicos e IC.	Artículos que no traten sobre ciberseguridad en SCF e IC.
Artículos sobre el uso de modelos de evaluación basados en ontología.	Artículos que no mencionen modelos ontológicos o su aplicación en ciberseguridad.
Estudios sobre impacto de la computación cuántica en la ciberseguridad de SCF e IC.	Artículos que no consideren amenazas o ciberseguridad cuánticas.
El artículo debe estar entre el año 2020 - 2025	Libros, tesis o artículos no revisados por pares.
Artículos publicados en inglés.	Artículos en otros idiomas diferente al inglés
Artículos que aborden cómo los modelos ontológicos, mejores prácticas de seguridad y framework de ciberseguridad que puedan aplicarse para prevenir ataques en SCF e IC, con enfoque en la era cuántica.	Artículos que no se centren en modelos ontológicos, mejores prácticas de seguridad y framework de ciberseguridad que puedan aplicarse para prevenir ataques en SCF e IC.

Fuente: elaboración propia.

Tras la aplicación de los criterios de inclusión, de 420 artículos iniciales se obtuvieron 64 artículos finales relevantes, lo que corresponde aproximadamente a un 15.2%, (Figura 1).

La selección de los estudios se realizó mediante un proceso secuencial y validado, en el cual un primer revisor efectuó la identificación y preselección inicial, seguida de una revisión independiente por un segundo evaluador experto. Para asegurar la objetividad del proceso, no se calculó el coeficiente Kappa, sino que se aplicó una matriz de valoración estructurada que permitió estimar el grado de acuerdo entre revisores con base en criterios definidos. Cada artículo fue evaluado utilizando una tabla de valoración por criterios de inclusión, donde se asignaron los siguientes puntajes: 1 (Cumple – Nivel Bueno), 0.5 (Cumple parcialmente – Nivel Regular) y 0 (No cumple – No pertinente). Este sistema de ponderación permitió cuantificar la pertinencia de los artículos y establecer umbrales mínimos para su selección (≥ 0.75), lo que garantizó un proceso sistemático, reproducible y libre de sesgos individuales.

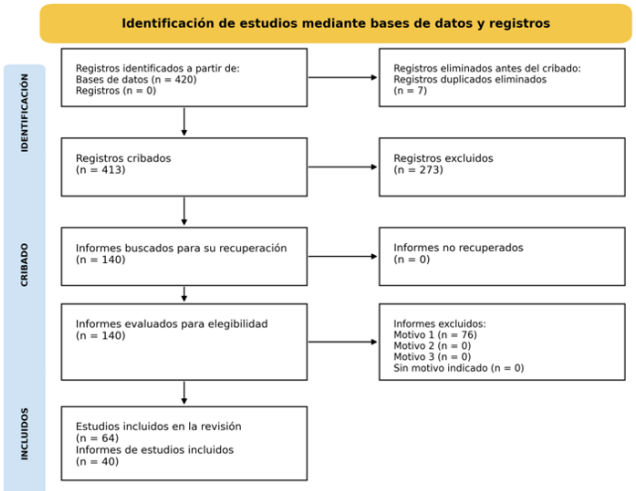

Figura 1. Proceso de selección de los estudios primarios.

Fuente: elaboración propia.

- *Evaluación de pertinencia:* para seleccionar los estudios primarios, se aplicó una metodología basada en cuatro categorías: claridad, rigor, relevancia y credibilidad, inspirada en el enfoque de Kitchenham et al. [6]. Esta herramienta permitió una evaluación cualitativa y cuantitativa, lo que facilitó la identificación de estudios pertinentes y la detección de posibles sesgos en la selección. Cada artículo fue calificado en una escala de 1 a 3 por criterio, distribuidos en las siguientes categorías: Claridad (2 criterios), Rigor (4 criterios), Relevancia (2 criterios) y Credibilidad (2 criterios), para un total de 10 criterios evaluativos por artículo. Por tanto, el puntaje total posible por artículo osciló entre 10 y 30 puntos, siendo convertido a una escala de promedio entre 1 y 3 para facilitar la comparación.

Los criterios de evaluación utilizados son:

- **Claridad:** eelevancia temática y aporte del estudio al campo.

- **Rigor:** objetivo explícito, metodología adecuada, replicabilidad del entorno experimental y representatividad de los datos.

- **Relevancia:** aplicabilidad al dominio de SCF e IC, y posibilidad de proyección a investigaciones futuras.

- **Credibilidad:** discusión metodológica clara y resultados comprensibles.

Se estableció un umbral mínimo de aceptación de 2.75 sobre 3 como promedio general, lo que garantizó la inclusión de estudios con una significativa calidad metodológica y pertinencia temática. Las exclusiones fueron justificadas documentalmente, con el fin de garanrtizar transparencia en el proceso. Como resultado, 40 artículos cumplieron con los criterios establecidos y fueron incluidos como estudios primarios (ver Figura 1). La lista completa está disponible en Zenodo: https://doi.org/10.5281/zenodo.16945744.

Cabe mencionar que se descartaron todos los artículos provenientes de Scopus (n = 75), al no alcanzar los umbrales mínimos de pertinencia contextual, profundidad técnica y/o enfoque explícito en ciberseguridad cuántica aplicada a SCF e IC.

- *Extracción de datos:* se realizó con base en las preguntas y los objetivos definidos en la primera etapa, a través de un instrumento que incluyó campos como ID del artículo, título, fuente, resumen, puntajes por criterio —claridad, rigor, relevancia, credibilidad— y puntaje total. Esto permitió identificar estándares aplicados a SCF e IC, así como vulnerabilidades emergentes relacionadas con la computación cuántica, los cuales fueron insumos claves. Para garantizar la validez de los hallazgos, se aplicó un análisis de certeza de la evidencia considerando criterios como reputación de la fuente (priorizando bases indexadas), claridad metodológica, pertinencia temática en el dominio cuántico de SCF en IC y revisión por pares. Aunque no

se utilizó formalmente el sistema GRADE (marco metódico usado internacionalmente para evaluar la calidad de la evidencia y determinar la fuerza de las recomendaciones en revisiones sistemáticas) se adoptó una clasificación equivalente: alta, media y baja, documentada en la matriz de extracción, la cual se puede consultar en el siguiente enlace en Zenodo: https://doi.org/10.5281/zenodo.17540633. Esta evaluación permitió filtrar estudios especulativos y priorizar evidencia robusta y confiable.

- *Síntesis y análisis de resultados:* el análisis mostró un aumento progresivo en la producción académica sobre ciberseguridad cuántica, con el año 2024 como aquel de mayor producción como se muestra en la Figura 2. Este crecimiento refleja el interés creciente en el impacto de la computación cuántica sobre las IC. Por otra parte, el análisis de palabras claves reveló una alta frecuencia en términos como: "ciberseguridad", "cuántico", "infraestructura crítica", "ontología" y "frameworks de ciberseguridad", agrupados en la Figura 3. Las palabras clave "infraestructura crítica" y "sistemas ciberfísicos (CPS)" fueron las más recurrentes, cada una con una frecuencia del 29,4%, lo que evidencia una fuerte orientación temática hacia la seguridad de entornos industriales complejos. También destacan los términos "mejores prácticas" (14,7%) y "ontología" (13,7%), lo que sugiere un creciente interés por enfoques estructurados de gestión del conocimiento y aplicación de marcos normativos. No se realizó análisis de subgrupos debido a la heterogeneidad metodológica, lo que se reconoce como una limitación y oportunidad para investigaciones futuras más específicas por sector o región.

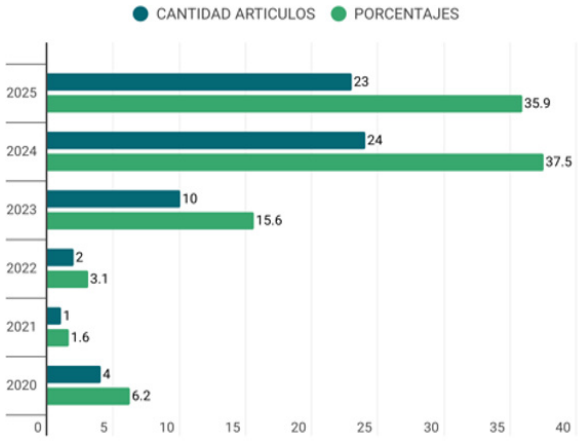

Figura. 2. Cantidad de artículos publicados por año

Fuente: elaboración propia.

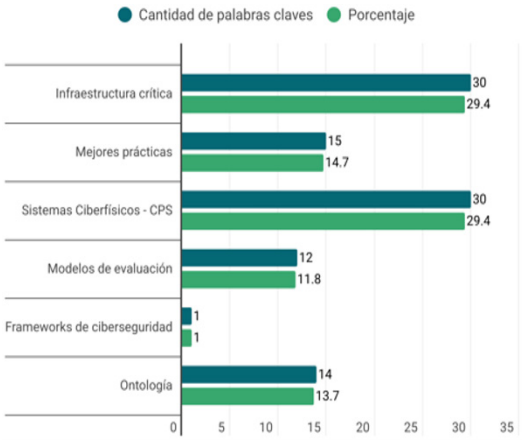

Figura. 3. Frecuencia de palabras claves en los estudios primarios

Fuente: elaboración propia.

Resultados

A continuación, se responden las preguntas de investigación formuladas que orientaron el estado del arte.

P1: ¿Cuáles son los principales estándares y marcos de trabajo utilizados en la ciberseguridad de SCF e IC?

A partir de la revisión realizada, se identificaron diversos marcos y estándares adoptados por organizaciones vinculadas con las IC. Los análisis mostraron una tendencia hacia la aplicación de marcos basados en estándares, muchos de ellos certificables, lo cual favorece el cumplimiento normativo y la seguridad organizacional [1], [9], [10].

Entre los marcos más destacados se encuentran NIST e IEC 62443, reconocidos por su disponibilidad documental y facilidad de acceso. No obstante, la implementación del IEC 62443 presenta desafíos técnicos y económicos, ya que demanda personal con la preparación, lo cual puede limitar su adopción, especialmente en pymes [1], [9], [10]. Por otro lado, se ha evidenciado un incremento en la adopción del estándar ISO/IEC 27001 debido a su flexibilidad y enfoque adaptable a múltiples sectores, especialmente a través de la implementación de controles del Anexo A (documento normativo o guía que apoya la implementación de los controles de seguridad establecidos en la norma ISO 27001) [11], [12], [13]. Mientras tanto, IEC 62443 y NIST SP 800-82 se utilizan más en sectores industriales como energía y manufactura. En cuanto a la adopción por regiones, los estudios señalan que en Estados Unidos predominan NIST SP 800-82 y NIST CSF, en parte por exigencias regulatorias. En Europa, se emplean ampliamente IEC 62443 e ISO/IEC 27001, asociados también con normativas como GDPR [11], [12], [13], [2]. En Asia y Oriente Medio se observa una integración creciente de ISO/IEC 27001 junto con IEC 62443, mientras que en Latinoamérica aumenta la aplicación de ISO/IEC 27001 por presión de regulaciones gubernamentales. A pesar de su popularidad, la aplicación práctica de estos marcos varía según factores como el tamaño de la empresa, cultura organizacional y la disponibilidad de recursos.

Los principales desafíos se centran en la implementación técnica, especialmente en normas como IEC 62443, debido a su complejidad técnica, necesidad de interoperabilidad entre sistemas legados y nuevos y el alto costo asociado a su adopción en infraestructuras críticas. En contraste, ISO/IEC 27001 tiende a ser más accesible para diferentes tamaños de organizaciones debido a su estructura modular y sus guías de implementación más flexibles.

En términos de frecuencia, ISO/IEC 27001 fue referenciado porel 27% de los estudios primarios, seguido por IEC 62443 (22%) y NIST SP 800-82 (18%). Otras normativas como NIST CSF, ISO/IEC 27019 y el marco COBIT también fueron identificadas, aunque con menor presencia porcentual.

La Tabla 4 presenta la frecuencia de aparición de los principales marcos normativos en los estudios analizados entre 2020 y 2025, lo que permite observar el liderazgo de ISO/IEC 27001, seguido por IEC 62443 y NIST SP 800-82 como los más representativos en el dominio de SCF e IC.

Tabla 4. *Análisis comparativo de estándares y marcos normativos aplicados a SCF e IC (2020–2025).*

Marco Normativo	Frecuencia de aparición	% de estudios	Sectores de Aplicación	Ventajas	Limitaciones
ISO/IEC 27001	18	27%	Multisectorial	Flexible, adaptable, certificable	Puede requerir ajustes específicos para entornos industriales
IEC 62443	15	22%	Industria, energía, manufactura	Alta especificidad técnica	Complejidad técnica y alto costo de implementación
NIST SP 800-82	12	18%	Industria, energía	Enfoque técnico en ICS	Menor adopción fuera de EE.UU.
NIST CSF	9	14%	Gobierno, servicios públicos	Claridad y alineación con políticas públicas	Enfocado en contexto estadounidense
ISO/IEC 27019	7	11%	Energía eléctrica	Adaptado a sistemas de gestión energética	Aplicación más restringida a sector energético
COBIT	3	5%	TI y gobernanza corporativa	Integración con gobierno de TI	No especializado en ciberseguridad industrial o cuántica
No aplica	-	3%	-	-	-

Fuente: elaboración propia.

P2: ¿Qué vulnerabilidades asociadas con la computación cuántica están emergiendo en la ciberseguridad de SCF e IC?

La computación cuántica introdujo nuevas vulnerabilidades en los SCF e IC, lo cual afectó especialmente a los algoritmos criptográficos tradicionales como RSA y ECC (algoritmos de clave pública o asimétrica), que son vulnerables ante el algoritmo cuántico de Shor (algoritmo para factorizar números grandes) [14], [15], [16], [17]. Asimismo, el algoritmo cuántico de Grover (algoritmo para la búsqueda en una secuencia no ordenada de datos con N componentes) reduce la seguridad de los algoritmos simétricos [14], [17]. Se destaca también las debilidades en sistemas heredados como SCADA (Supervisory Control And Data Acquisition), que presentan dificultades de actualización [13], [18], y los riesgos en la cadena de suministro por componentes vulnerables [19]. Los protocolos de autenticación y distribución de claves como Diffie-Hellman también son susceptibles a ataques cuánticos [17], [20]. Además, se evidenció el surgimiento de amenazas vinculadas con inteligencia artificial (IA) y modelos de lenguaje, incluyendo técnicas como: inyección de prompts, *jailbreaking* y *backdoors* [21], [22]. Los ataques más frecuentes incluyen: ataques cuánticos (Shor y Grover), ataques a QKD (Distribución de Clave Cuántica), y amenazas tradicionales como: *ransomware*, *malware*, DoS/DDoS e ingeniería social siguen aún vigentes [3], [10], [23], [24]. Frente a este panorama, varios estudios recomiendan la migración urgente a algoritmos postcuánticos, la protección de activos de tecnología de la operación (TO) y la gestión de amenazas internas [14], [18], [24], [25].

Para clarificar la naturaleza y el impacto de estas vulnerabilidades, se estructuró una categorización comparativa que agrupa los hallazgos en cinco dominios clave: criptográficas, de comunicación, de dispositivos/IoT, humanas y de terceros.La Tabla 5 resume esta clasificación y establece para cada categoría

el tipo de vulnerabilidad más relevante, su causa raíz, su impacto directo sobre la tríada de la seguridad (confidencialidad, integridad, disponibilidad) y un ejemplo representativo extraído de los estudios revisados.

Esta tabla facilita la lectura transversal del problema al conectar las vulnerabilidades emergentes con escenarios específicos de amenaza y permite identificar patrones comunes, como la recurrencia de debilidades en infraestructuras heredadas, la presión regulatoria para adoptar nuevos protocolos, o la falta de controles para mitigar riesgos provenientes de proveedores externos. Las vulnerabilidades identificadas se agruparon en cinco categorías y estas se alinean con la tríada de seguridad: confidencialidad, integridad y disponibilidad [25], [26], [27], [28]. También se evidenció que las investigaciones analizaron y aplicaron ontologías y taxonomías especializadas como CVO (*Conceptual Vulnerability Ontology*) y TRACI (*Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure*), las cuales fueron utilizadas para clasificar los ataques con base en los activos comprometidos, los riesgos asociados y las motivaciones subyacentes. Estas herramientas conceptuales permitieron estructurar el conocimiento sobre amenazas emergentes en entornos críticos, facilitando una mejor comprensión de los vectores de ataque en función del contexto operacional de los SCF e IC [25], [26], [27].

Por último, se identificaron múltiples causas subyacentes a las vulnerabilidades descritas: los avances en computación cuántica, la persistencia de sistemas heredados con limitadas capacidades de actualización, los errores humanos durante procesos operativos, la ausencia de estándares unificados en entornos industriales y las restricciones presupuestales y técnicas que dificultaron la migración a esquemas de criptografía postcuántica [16], [18], [25]. Las consecuencias reportadas en la literatura incluyeron la exposición de datos sensibles, la interrupción de servicios críticos, daños físicos en infraestructuras estratégicas y el deterioro de la reputación institucional ante brechas de seguridad [17], [19], [23].

Tabla 5. *Categorización comparativa de vulnerabilidades emergentes en SCF e IC frente a la computación cuántica.*

Categoría	Tipo de vulnerabilidad	Causa raíz	Impacto principal	Ejemplo representativo
Criptográfica	Ruptura de algoritmos RSA, ECC y AES	Algoritmos cuánticos (Shor, Grover)	Compromiso de la confidencialidad	Ataques a certificados digitales
Comunicación	Intercepción de canales QKD, Diffie-Hellman	Debilidades en protocolos	Pérdida de integridad de datos	Suplantación de identidad remota
Dispositivos/IoT	Dispositivos heredados, sin actualizaciones	Limitaciones en SCADA y TO antiguos	Interrupción de servicios críticos	Falla en sensores de planta eléctrica
Humanas	Ingeniería social, mal uso de IA	Errores humanos o manipulación	Acceso no autorizado o fuga de datos	Inyección de prompts en IA
Terceros	Suministro de componentes no confiables	Dependencia de proveedores externos	Pérdida de disponibilidad o sabotaje	***Firmware* modificado en routers**

Fuente: elaboración propia.

Discusión y limitaciones: los resultados de la revisión mostraron que, si bien existen marcos internacionales consolidados en ciberseguridad para IC, el surgimiento de la computación cuántica plantea retos inéditos. Estos desafíos aún no han sido abordados integralmente en la literatura reciente. En particular, se evidenció una escasa articulación entre los enfoques de seguridad cuántica y los modelos ontológicos o taxonómicos existentes, lo que limita el desarrollo de herramientas semánticas avanzadas. Los hallazgos revelan que, aunque existen ontologías como CSO [25] y TRACI [26], su aplicación en contextos cuánticos aún es incipiente. Esto limita su utilidad para afrontar amenazas emergentes en SCF e IC.

La mayoría de los estudios revisados se centraron en componentes técnicos o criptográficos, dejando de lado las dimensiones organizacionales, regulatorias y humanas. Esta concentración temática puede dificultar la implementación de soluciones holísticas, especialmente en sectores donde la operación confiable de los Sistemas Ciberfísicos (SCF) resulta esencial para la estabilidad nacional, como los de energía, transporte y salud.

Asimismo, se observó que los trabajos con mayor profundidad técnica y alcance institucional fueron desarrollados en contextos del hemisferio norte, particularmente en Estados Unidos, Europa y Asia. En contraste, en Latinoamérica se identificaron esfuerzos aún emergentes, lo que evidencia la necesidad de consolidar agendas regionales de investigación orientadas hacia la transición postcuántica y de fortalecer capacidades institucionales para la adaptación de estándares internacionales. Este hallazgo coincide con lo expuesto por Liyanage *et al.* [7] quienes destacan la asimetría en la adopción de marcos de madurez y evaluación de capacidades de ciberseguridad a nivel global.

Se identificó como hallazgo clave la necesidad de cooperación internacional en el desarrollo de ontologías y taxonomías adaptadas a amenazas tradicionales y cuánticas en IC y SCF. Además, se subraya la urgencia de integrar los conceptos clave entre dominios, evitando la fragmentación conceptual que limita el avance del campo.

En esta línea, algunos avances preliminares han sido formulados en estudios como los de Amador *et al.* [24], quienes realizaron una revisión sistemática sobre SCF, IC y ciberseguridad cuántica; Plachkinova y Vo con su taxonomía TRACI [26]; Martins et al. con un marco conceptual para la caracterización de ontologías en ciberseguridad [27]; y Kozlenko , quien propone una ontología difusa para la evaluación de riesgos y el impacto de ataques [28]. Sin embargo, estos desarrollos permanecen en fases iniciales y dispersas, lo cual es un obstáculo para su adopción industrial y su integración en marcos regulatorios consolidados. Cabe aclarar, que todos los estudios citados forman parte del conjunto de 40 artículos analizados en esta revisión sistemática, los cuales se encuentran documentados en el repositorio Zenodo (https://doi.org/10.5281/zenodo.17540633). Aunque no todos se mencionan explícitamente en el cuerpo del texto, han contribuido directamente en distintas etapas del trabajo, ya sea como soporte de las preguntas de investigación, en la construcción del marco teórico o en la fundamentación metodológica del estudio.

Otro aspecto que emergió con fuerza fue la ausencia de mecanismos estandarizados de interoperabilidad entre sistemas ontológicos aplicados a IC y SCF, lo cual limita la integración de herramientas automatizadas en entornos operativos reales. Esta limitación afecta directamente la capacidad de anticipación, correlación y respuesta coordinada frente a amenazas avanzadas, particularmente aquellas potenciadas por algoritmos cuánticos o técnicas de inteligencia artificial maliciosa. Desde una perspectiva práctica y política, los resultados evidencian la necesidad de formular estrategias nacionales e internacionales que promuevan la estandarización semántica, la inversión en infraestructura de ciberseguridad postcuántica y la formación de talento humano especializado. Esto implica también el fortalecimiento de marcos de gobernanza digital adaptativa, que permitan responder de manera flexible a la evolución acelerada del riesgo tecnológico, garantizando resiliencia institucional y la protección de activos críticos.

Finalmente, los hallazgos fueron interpretados considerando las principales limitaciones del estudio. En primer lugar, la disponibilidad de literatura científica reciente en bases indexadas de acceso abierto pudo haber restringido la incorporación de ciertos estudios relevantes. En segundo lugar, la ausencia de resultados relevantes en *Scopus* evidencia la subrepresentación de la temática en repositorios académicos tradicionales, lo que refuerza la importancia de integrar buscadores amplios como *Google Scholar* para garantizar una cobertura más inclusiva en campos de investigación emergentes. Asimismo, la heterogeneidad metodológica de los estudios incluidos impidió realizar análisis cuantitativos o metaanálisis estadísticos; sin embargo, la síntesis cualitativa obtenida proporciona una base sólida para avanzar hacia modelos de evaluación integrales, contextualizados y validados empíricamente en el dominio de la ciberseguridad cuántica aplicada a infraestructuras críticas.

Conclusiones

Este trabajo permitió identificar una baja integración entre los modelos taxonómicos, ontológicos y la ciberseguridad cuántica, especialmente en el contexto de IC y SCF. La mayoría de los estudios se enfocó en aspectos técnicos, dejando de lado dimensiones organizacionales y regulatorias necesarias para enfrentar riesgos emergentes. Los hallazgos mostraron que, si bien existen avances en la formulación de marcos y modelos orientados a la protección de los sistemas ciberfísicos, aún no se ha consolidado un enfoque holístico que articule conceptos ontológicos, criterios de gobernanza y mecanismos de adaptabilidad frente al entorno cuántico. En particular, se evidenció una fragmentación entre las propuestas dirigidas a la protección de activos, la evaluación de riesgos y la gestión institucional, lo cual limita la construcción de políticas públicas y planes estratégicos con enfoque integral. En respuesta, se propone como trabajo futuro una de ruta en tres fases. Estas tres fases fueron sintetizadas en la Tabla 6, la cual permite visualizar el tránsito progresivo desde la conceptualización semántica, pasando por el diseño institucional, hasta la validación contextual de las propuestas. Este esquema busca orientar la futura investigación y el desarrollo de soluciones prácticas, particularmente en sectores industriales sensibles como energía, salud o transporte.

La primera fase plantea el desarrollo del Modelo Ontológico de Resiliencia Ciber-Cuántica (MORCC), orientado a representar, mediante estructuras semánticas, las relaciones entre activos críticos, tipos de amenazas (clásicas y cuánticas) y capacidades de respuesta. La segunda fase propone el diseño del Marco de Gobernanza Adaptativa Cuántica (MGAC), que articula políticas, roles institucionales y procesos de toma de decisiones frente a riesgos emergentes en SCF e IC. La tercera fase contempla la ejecución de estudios piloto en sectores priorizados, con el fin de validar empíricamente los modelos propuestos. Esta etapa incluiría una evaluación sistemática mediante indicadores comocobertura de amenazas, capacidad de respuesta, interoperabilidad semántica y alineación con marcos regulatorios nacionales o internacionales.

Tabla 6. *Ruta para el desarrollo de un modelo ontológico y marco de gobernanza adaptativa cuántica.*

Fase	Nombre	Objetivo	Resultados esperados
1	MORCC	Diseñar un modelo ontológico que represente relaciones entre activos, amenazas cuánticas y capacidades de defensa en IC y SCF.	Ontología formalizada y repositorio de conceptos normalizados.
2	MGAC	Proponer un marco de gobernanza adaptativa cuántica para guiar respuestas organizacionales y normativas.	Directrices y políticas para respuesta institucional en contextos críticos.
3	Validación en casos de estudio	Implementar los modelos en entornos reales o simulados y evaluar su impacto.	Evidencia empírica, lecciones aprendidas y recomendaciones de mejora.

Fuente: elaboración propia.

Con el fin de fortalecer la validación empírica de la propuesta anterior, se plantearon indicadores preliminares que permitirán evaluar la implementación de los modelos MORCC y MGAC en entornos piloto. Estos indicadores abordan aspectos técnicos, organizacionales y estratégicos, alineándose con los principios de gobernanza adaptativa, resiliencia operativa y ciberseguridad post-cuántica. La Tabla 7 resume estos indicadores clave.

Estos indicadores podrán ser refinados según el contexto del piloto y su análisis permitirá evaluar la pertinencia, escalabilidad y adaptabilidad de las soluciones propuestas, así como su alineación con estándares emergentes en ciberseguridad cuántica. Además, facilitarán la comparación entre distintas instituciones o sectores, generando evidencia para la formulación de políticas públicas más robustas en entornos críticos. Finalmente, aunque este estudio se centró en la proyección metodológica sin aplicación directa en entornos reales, se reconoce la necesidad de validación empírica. El desarrollo de pilotos en infraestructuras críticas de sectores estratégicos, a fin de evaluar los modelos propuestos, ajustar supuestos teóricos y fortalecer su aplicabilidad bajo marcos regulatorios específicos es una perspectiva de trabajo futuro

Tabla 7. *Propuesta de indicadores para evaluar pilotos de implementación del modelo ontológico y de gobernanza cuántica.*

Categoría	Indicador Propuesto	Métrica / Unidad	Nivel de Evaluación
Técnico	Porcentaje de cobertura de activos modelados en la ontología	Porcentaje activos críticos representados	Completo / Parcial / Bajo
	Tiempo medio de respuesta ante un incidente cuántico simulado	Minutos / horas	Cuantitativo
	Nivel de interoperabilidad entre sistemas heredados y soluciones nuevas	Índice de compatibilidad	Bajo / Medio / Alto
Organizacional	Nivel de apropiación del modelo por parte de los equipos técnicos	Escala Likert (1 a 5)	Percepción cualitativa
	Porcentaje de implementación de controles post-cuánticos	Porcentaje controles aplicados del marco	Cuantitativo
	Presencia de roles y responsabilidades definidos en MGAC	Sí / No	Binario
Estratégico / Gobernanza	Existencia de un plan de continuidad actualizado con enfoque cuántico	Documento validado	Sí / Parcial / No
	Frecuencia de actualización del modelo ontológico	Número de revisiones por año	Cuantitativo
	Inclusión del modelo en la política institucional de seguridad	Grado de integración	Ninguno / Parcial / Total

Fuente: elaboración propia.

Agradecimientos

Gracias a la Universidad del Cauca, especialmente al grupo de investigación GTI 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] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection," *Int. J. Comput. Intell. Syst.*, Dec. 2024. https://doi.org/10.1007/s44196-024-00644-z.

[2] M. Habibul Arif, H. Rahman Rabby, N. Yasmin Nadia, M. Iftekhar Monzur Tanvir, and A. Al Masum, "AI-driven risk assessment in national security projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects," *J. Comput. Sci. Technol. Stud.*, 2025. https://doi.org/10.32996/jcsts

[3] M. T. Islam, M. R. Mission, T. K. Refat, and M. Kynatun, "Cybersecurity Risk Assessment Frameworks For Engineering Databases: A Systematic Literature Review", *SDMI*, vol. 2, no. 01, pp. 224–243, Feb. 2025. https://doi.org/10.71292/sdmi.v2i01.22 .

[4] M. Ekerå, "On post-processing in the quantum algorithm for computing short discrete logarithms," *Des. Codes Cryptogr.*, vol. 88, no. 11, pp. 2313–2335, Nov. 2020. https://doi.org/10.1007/s10623-020-00783-2

[5] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, art. n71, Mar. 2021. https://doi.org/10.1136/bmj.n71

[6] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, Dec. 2013. https://doi.org/10.1016/j.infsof.2013.07.010

[7] L. Liyanage, N. A. G. Arachchilage, and G. Russello, "SoK: Identifying limitations and bridging gaps of cybersecurity capability maturity models (CCMMs)," arXiv preprint arXiv:2408.16140, 2024. [Online]. Available: https://arxiv.org/abs/2408.16140

[8] S. Mohanan and N. Parameswaran, "FINER criteria – What does it mean?" *Cosmoderma*, vol. 2, art. 115, Nov. 2022. https://doi.org/10.25259/csdm_123_2022

[9] S. Islam, D. Javeed, M. S. Saeed, P. Kumar, A. Jolfaei, and A. K. M. N. Islam, "Generative AI and cognitive computing-driven intrusion detection system in industrial CPS," *Cognit. Comput.*, vol. 16, no. 5, pp. 2611–2625, Sep. 2024. https://doi.org/10.1007/s12559-024-10309-w

[10] A. AlHarmali, S. Ali, W. Aman, and O. Hussain, "Cyber risk assessment for cyber-physical systems: A review of methodologies and recommendations for improved assessment effectiveness," in *Proc. Comput. Sci. Inf. Technol. (CS & IT)*, AIRCC, Aug. 2024, pp. 77–94. https://doi.org/10.5121/csit.2024.141608

[11] A. Budžys, O. Kurasova, and V. Medvedev, "Deep learning-based authentication for insider threat detection in critical infrastructure," *Artif. Intell. Rev.*, vol. 57, no. 10, art. 263, Oct. 2024. https://doi.org/10.1007/s10462-024-10893-1

[12] A. Akbarzadeh and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems," *Int. J. Inf. Secur.*, vol. 22, pp. 563–578, Jun. 2023. https://doi.org/10.1007/s10207-022-00608-4

[13] B. G. de Soto, A. Georgescu, B. Mantha, Ž. Turk, A. Maciel, and M. S. Sonkor, "Construction cybersecurity and critical infrastructure protection: New horizons for construction 4.0," *J. Inf. Technol. Constr.*, vol. 27, pp. 571–594, 2022. https://doi.org/10.36680/j.itcon.2022.028

[14] S. Berríos, F. Alonso, B. Gana, and S. Contreras, "Advances and strategies in quantum computing integration for cybersecurity: A systematic literature review," in *Commun. Comput. Inf. Sci.*, Springer, 2025, pp. 269–282. https://doi.org/10.1007/978-3-031-84078-4_19

[15] D. Silva and R. Núñez, "Exploración de las posibilidades de la computación cuántica para la criptografía," *CIENCIA INTELIGENTE*, vol. 1, no. 2, pp. 35–53, 2023, Accessed: May 27, 2026. [Online]. Available: https://cienciainteligente.com/index.php/CIN/article/view/16

[16] S. Narula, M. Ghasemigol, J. Carnerero-Cano, A. Minnich, E. Lupu, and D. Takabi, "Exploring AI security: A systematic mapping study," *IEEE Access*, 2025. https://doi.org/10.1109/ACCESS.2025.3567195

[17] Í. Oliveira *et al.*, "An Ontological Model of the Phishing Attack Process," *Lecture Notes in Business Information Processing*, pp. 274–289, 2025, https://doi.org/10.1007/978-3-031-95397-2_17

[18] S. Dash, H. Seker, and M. Shahpasand, "From data to defense: How ontology fuels AI in cyber threat detection," in *Proc. 8th Int. Conf. Adv. Artif. Intell. (ICAAI 2024)*, ACM, Mar. 2025, pp. 121–133. https://doi.org/10.1145/3704137.3704176

[19] B. Cinar, "Supply chain cybersecurity: Risks, challenges, and strategies for a globalized world," *J. Eng. Res. Rep.*, vol. 25, no. 9, pp. 196–210, Oct. 2023. https://doi.org/10.9734/jerr/2023/v25i9993

[20] R. Ghosh, von Stockhausen, M. Schmitt, G. M. Vasile, S. K. Karn, and O. Farri, "CVE-LLM : Ontology-Assisted Automatic Vulnerability Evaluation Using Large Language Models," *arXiv.org*, 2025. https://doi.org/10.48550/arXiv.2502.15932

[21] U. Ullah, M. Haleem, and A. Ullah, "OntoSecAI: Ontology-driven security automation for AI-enabled systems," *PLOS ONE*, vol. 20, no. 12, art. e0337806, Dec. 2025. https://doi.org/10.1371/journal.pone.0337806

[22] Y. Guan, Y. Zhang, J. Yue, Y. Lu, and Y. Xie, "Enhancing cybersecurity situation awareness through knowledge graphs: An integrated survey including threats, vulnerabilities, and assets," *SSRN*, preprint, 2025. [Online]. Available: https://ssrn.com/abstract=5221263

[23] U. O. Obonna *et al.*, "Detection of man-in-the-middle (MitM) cyber-attacks in oil and gas process control networks using machine learning algorithms," *Future Internet*, vol. 15, no. 8, art. 280, Aug. 2023. https://doi.org/10.3390/fi15080280

[24] S. Amador Donado, C. J. Pardo Calvache, and R. Mazo Peña, "Revisión preliminar: ciberseguridad para tecnología de la operación en la era cuántica contra ataques de red a infraestructuras críticas," *Rev. INGE CUC*, vol. 20, no. 2, 2024.

[25] W. F. Borja Rivadeneira y O. S. Gómez Gómez, «Cybersecurity Ontologies: A Systematic Literature Review», *ReCIBE*, vol. 9, n.º 2, pp. C2–18, mar. 2021 https://doi.org/10.32870/recibe.v9i2.181.

[26] M. Plachkinova and A. Vo, "A taxonomy for risk assessment of cyberattacks on critical infrastructure (TRACI)," *Commun. Assoc. Inf. Syst.*, vol. 52, art. 2, 2023. https://doi.org/10.17705/1cais.05202.

[27] B. F. Martins *et al.*, "A framework for conceptual characterization of ontologies and its application in the cybersecurity domain," *Software and Systems Modeling*, vol. 21, no. 4, pp. 1437–1464, July 2022, https://doi.org/10.1007/s10270-022-01013-0

[28] O. Kozlenko, "Example of fuzzy ontology usage for risk assessment and attack impact," *Theor. Appl. Cybersecur.*, vol. 6, no. 1, 2024. https://doi.org/10.20535/tacs.2664-29132024.1.312677

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.24865

INVESTIGACIÓN

Análisis de prácticas para reducir el consumo de energía en las pruebas de software: una revisión sistemática de la literatura

Analysis of practices to reduce energy consumption in software testing: A Systematic Literature Review

Eduardo López-Chacón [1], Juan Carlos Pérez-Arriaga [2], Ángel J. Sánchez-García [3], Lizbeth Alejandra Hernández-González [4]

Fecha de Recepción: 12 de noviembre de 2025 **Fecha de Aceptación**: 12 de marzo de 2026

Cómo citar: E. López-Chacón, J.C. Pérez-Arriaga, A.J. Sánchez-García, L.A. Hernández-Gonzáles, «Análisis de prácticas para reducir el consumo de energía en las pruebas de software: una revisión sistemática de la literatura», *Tecnura*, vol. 30, n.° 88, jun. 2026. 102–125. https://doi.org/10.14483/22487638.24865

Resumen

Contexto: El consumo de energía es importante para el desarrollo tecnológico actual, no solo por su impacto económico sino también por sus implicaciones ambientales. En el desarrollo de software, el consumo se intensifica en etapas con mayor demanda de energía, siendo la prueba una de las más notables. Aunque se han establecido nuevas directrices centradas en la sostenibilidad del software, poco se sabe aún sobre las prácticas específicas en la etapa de prueba para disminuir el consumo de energía. Los desarrolladores de software, a menudo, se centran en la funcionalidad y en la prueba de software sin considerar la eficiencia energética.
Objetivo: Este estudio analiza las prácticas que minimizan el consumo energético en la etapa de prueba de software, los métodos utilizados para su implementación, e identifica las herramientas de automatización que contribuyen a la reducción del consumo de energía.
Metodología: revisión sistemática de la literatura por medio del enfoque de Kitchenham.
Resultados: Se analizaron 30 estudios primarios en los que se identificaron prácticas enfocadas en el ahorro de energía durante las pruebas de software. Se destacan la optimización de recursos y el escalado dinámico de voltaje y frecuencia (*DVFS*) que reduce el consumo de energía al ajustar la velocidad de procesamiento en función de la demanda esperada.
Conclusiones: Este trabajo proporciona una base de referencia para interesados en el desarrollo de software que busquen estrategias sustentables durante la fase de prueba.

1 Estudiante en Ingeniería de Software por la Universidad Veracruzana. Email: zS20015721@estudiantes.uv.mx

2 Maestro en Ciencias de la Computación y Profesor de Tiempo Completo en la Facultad de Estadística e Informática de la Universidad Veracruzana. Email: juaperez@uv.mx

3 Licenciado en Informática por la Universidad Veracruzana en 2011. En el 2013 obtuvo su grado de Maestro en Inteligencia Artificial y un año más tarde el grado de Especialista en Métodos Estadísticos por dicha Universidad. En 2018 Obtuvo su grado de Doctor en Inteligencia Artificial por el Centro de Investigación en Inteligencia Artificial de la Universidad Veracruzana. Actualmente es profesor de tiempo completo en la Facultad de Estadística e Informática en la Universidad Veracruzana, Licenciatura en Ingeniería de Software, Xalapa, Veracruz, México. Email: angesanchez@uv.mx

4 Licenciada en Informática y Maestra en Ingeniería de Software por la Universidad Veracruzana. Doctora en Ciencias de la Ingeniería por el Instituto Tecnológico de Orizaba, parte del Tecnológico Nacional de México. Hasta la fecha es profesora de tiempo completo en la Universidad Veracruzana en la Licenciatura en Ingeniería de Software campus Xalapa, Veracruz, México. Email: lizhernandez@uv.mx

Palabras clave: Energía verde, Eficiencia energética, Consumo de energía, Pruebas de Software, Ingeniería de software, Pruebas Automatizadas.

Abstract

Context: Energy consumption is important for current technological development, not only due to its economic impact but also because of its environmental implications. In software development, consumption intensifies in stages with higher energy demand, with testing being one of the most notable. Although new guidelines focused on software sustainability have been established, little is yet known about specific practices in the testing stage to reduce energy consumption. Software developers often focus on functionality and software testing without considering energy efficiency.
Objective: This study analyzes the practices that minimize energy consumption in the software testing stage, the methods used for their implementation, and identifies automation tools that contribute to reducing energy consumption.
Methodology: Systematic literature review using the Kitchenham approach.
Results: Thirty primary studies were analyzed, identifying practices focused on energy savings during software testing. Notable among them are resource optimization and Dynamic Voltage and Frequency Scaling (DVFS), which reduces energy consumption by adjusting processing speed based on expected demand.
Conclusions: This work provides a baseline reference for stakeholders in software development seeking sustainable strategies during the testing phase.
Keywords: Green energy, Energy efficiency, Energy consumption, Software testing, Software engineering, Automated testing.

Introducción

En la actualidad, los sistemas de software se han convertido en un elemento clave en entornos cotidianos, educativos y organizacionales. Estos sistemas se diseñan para resolver problemas de diversa índole y facilitar actividades en empresas e instituciones. Durante el proceso de desarrollo se hace un uso intensivo de energía eléctrica debido a la variedad de herramientas empleadas para su construcción, así como durante la etapa de prueba de software, lo que contribuye a las emisiones de CO2 [1].

La ingeniería de software verde puede definirse como la aplicación de principios y prácticas sostenibles durante las etapas del desarrollo de software [2], con el objetivo de reducir su impacto ambiental negativo. Esto implica disminuir tanto el consumo de energía como el uso de materiales a lo largo del proceso de desarrollo.

La eficiencia energética del software es un aspecto fundamental para promover la ingeniería de software verde. El término software ecológico se refiere al software energéticamente eficiente; para lograrlo, es necesario disminuir el consumo de energía desde las primeras etapas de desarrollo de un producto de software y mantener una revisión constante durante todo su ciclo de vida [3].

La prueba de software es un proceso de control de calidad orientado a verificar que los sistemas desarrollados funcionen correctamente y sin complicaciones. Esta etapa es relevante en la industria del

software por la variedad de recursos y conocimientos técnicos que requiere, así como por los elementos que pueden incidir en el resultado final de un proyecto. De acuerdo con Valle [4], completar las etapas del proceso de pruebas de forma manual y repetitiva supone un gran esfuerzo; de hecho, el proceso completo de pruebas puede representar hasta el 40 % del costo total de los proyectos.

Aunque los desarrolladores de software tienen conciencia sobre el uso de energía, este aspecto no siempre se considera formalmente durante el proceso de desarrollo. Esto se debe, en parte, a que la información sobre prácticas para optimizar el consumo energético se encuentra dispersa y a que el esfuerzo de desarrollo suele enfocarse en el rendimiento del hardware y en los aspectos funcionales del software. Sin embargo, la eficiencia energética es un requisito no funcional esencial que requiere mayor atención y comprensión por parte de la comunidad de desarrollo de software [5]. Esta revisión sistemática de la literatura (RSL) analiza y clasifica las prácticas que reducen el consumo de energía en la fase de prueba de software, con el fin de reunir información sobre esta etapa desde una perspectiva sostenible.

Trabajos relacionados

En los últimos años, diversos estudios han abordado la eficiencia energética desde diferentes perspectivas; Sin embargo, pocos estudios se han centrado explícitamente en las prácticas adoptadas durante la fase de prueba de software.

En el trabajo de Asadi. [6] se realizó una revisión sistemática de la literatura sobre Green IT con el objetivo de analizar el estado actual de la investigación en esta área entre los años 2007 y 2016. La revisión identificó 131 estudios primarios enfocados en la sostenibilidad ambiental dentro del ámbito de las tecnologías de la información. Los autores destacan que el impacto ambiental de las tecnologías de la información se origina en todas las etapas de su ciclo de vida: diseño, desarrollo, uso y disposición, lo que genera un consumo de energía y contribuye a las emisiones de CO_2, equivalentes al 2 % del total mundial. Uno de los desafíos importantes en desarrollo de software sobre eficiencia energética es la capacidad de medir y reducir el consumo de energía durante la ejecución de la fase de prueba. El trabajo de Jabbarvand *et al.* [7] representa una contribución significativa al proponer técnicas destinadas a minimizar el consumo de energía en aplicaciones móviles. Su investigación se centra en tres enfoques clave: generación de pruebas, evaluación de la adecuación del conjunto de pruebas y minimización del conjunto de pruebas.

Bruce et al. [8] introducen una técnica basada en pruebas dirigidas por búsqueda (SBST), que aplica un algoritmo genético para reducir el consumo de energía del software. Este tipo de enfoque es parte del campo de la ingeniería de software basada en búsquedas y utiliza algoritmos de optimización y heurística para resolver problemas complejos dentro de las pruebas de software, particularmente aquellos

que implican explorar amplios espacios de solución, logrando una reducción del 25 % en el consumo evaluado del programa.

En el ámbito de la ingeniería de software con enfoque sostenible, A.C. Moisés [9) presenta un estudio donde identifico 170 prácticas, de las que 70 están relacionadas con el consumo energía. Aunque el trabajo no se centra exclusivamente en la etapa de prueba, algunas de estas prácticas pueden aplicarse directamente a dicha fase del desarrollo de software. Asimismo, el estudio identifica otras categorías relevantes, como las prácticas de evaluación de la eficiencia energética, centradas en métodos y técnicas de medición del consumo en casos prácticos reales. En particular, para la etapa de prueba, se enfatiza el uso de herramientas y técnicas de monitorización y medición del consumo energético en tiempo real, lo que permite identificar las áreas del proceso que demandan mayor cantidad de recursos y energía, y, en consecuencia, orientar acciones de optimización.

A diferencia de los estudios anteriores, la presente investigación se enfoca específicamente en la identificación, clasificación y análisis de las prácticas que reducen el consumo energético durante la fase de prueba de software. Mientras que las revisiones previas han abordado el tema de la sostenibilidad de manera general o desde perspectivas de hardware, desarrollo o uso, este estudio profundiza en el ámbito de las pruebas, una etapa clave pero poco explorada en términos de eficiencia energética. Además, se incorporan métodos, técnicas y herramientas documentadas en la literatura reciente (2013–2024), estableciendo una base actualizada para tratar el consumo de energía en la etapa de prueba de software.

Metodología

Este estudio siguió el método propuesto por Kitchenham et al. [10]. Como complemento a la estrategia, se integró el método de búsqueda automatizada Cuasi-Gold Standard, propuesto por Zhang et al. [11], para facilitar la identificación de estudios en el campo de la Ingeniería del Software. Una vez extraídos los datos de los estudios primarios, los hallazgos se organizaron y analizaron utilizando un enfoque de síntesis narrativa, siguiendo el procedimiento descrito por Popay et al. [12].

A) Planeación

1. Preguntas de investigación

Nuestro estudio se estructuró en torno a las siguientes preguntas principales de investigación, que se presentan en la Tabla 1.

Tabla 1. *Preguntas de investigación*

Pregunta de investigación
RQ1. ¿Cuáles son las prácticas reportadas en la literatura que contribuyen a reducir el consumo de energía en la fase de prueba de software?
RQ2. ¿Qué actividades de prueba de software están asociadas con el consumo de energía?
RQ3. ¿Qué métodos se utilizan para reducir el consumo de energía en las prácticas de prueba identificadas?
RQ4. ¿Qué aportación tienen las herramientas de automatización en la reducción del consumo de energía en actividades de prueba?

Fuente: elaboración propia.

B) Conducción

1. Cadena de búsqueda

Las cadenas de búsqueda se crearon y evaluaron siguiendo el enfoque de Zhang et al. [9]. Como parte de este proceso, se obtuvo una lista inicial de estudios relevantes mediante la exploración manual del motor de búsqueda *IEEE Xplore*. La cadena de búsqueda con mejor rendimiento logra un retorno del 83 %, recuperando un total de 86 estudios, con un esfuerzo del 5,95 %, esta se conforma de la siguiente manera:

("software testing" OR "green practices" OR "green testing" OR "green software engineering") and ("energy minimization" or "energy consumption" or "energy awareness" or "efficient activity") and ("practices" or "methods" or "technique*")

2. Motores de búsqueda

En la búsqueda automatizada, se seleccionaron *IEEE Xplore*, *SciencieDirect*, SpringerLink, *ACM Digital Library* fuentes destacadas por Zhang et al. [11], para la búsqueda de estudios.

3. Selección de estudios primarios

En esta sección se presentan los criterios utilizados para la selección o exclusión de estudios en las Tabla **2** y **3**.

Tabla 2. *Criterios de inclusión*

Identificador	Criterio
CI-1	Estudios publicados entre 2013 y diciembre de 2024
CI-2	El artículo de investigación fue publicado en idioma inglés
CI-3	El título muestra indicios de responder al menos 1 pregunta de investigación
CI-4	El resumen da indicios para responder al menos 1 pregunta de investigación.
CI -5	El texto del estudio responde al menos a 1 pregunta de investigación.

Fuente: elaboración propia.

Tabla 3. *Criterios de exclusión*

Identificador	Criterio
CE-1	No se tiene acceso al estudio completo
CE-2	El estudio es referente a la disciplina de la ingeniería de software
CE-3	El estudio no está relacionado con el consumo de energía en la prueba de software
CE-4	El estudio es redundante o duplicado de otros trabajos ya incluidos en la revisión.
CE-5	Es un libro, póster, presentación, resumen o tutorial.

Fuente: elaboración propia.

4. Proceso de selección

La selección de los estudios se realizó mediante un sistema de filtrado en fases consecutivas. En cada etapa, se aplicaron criterios progresivamente más restrictivos (de lo general a lo específico), descartando tempranamente los estudios irrelevantes. La Figura 1 resume este proceso.

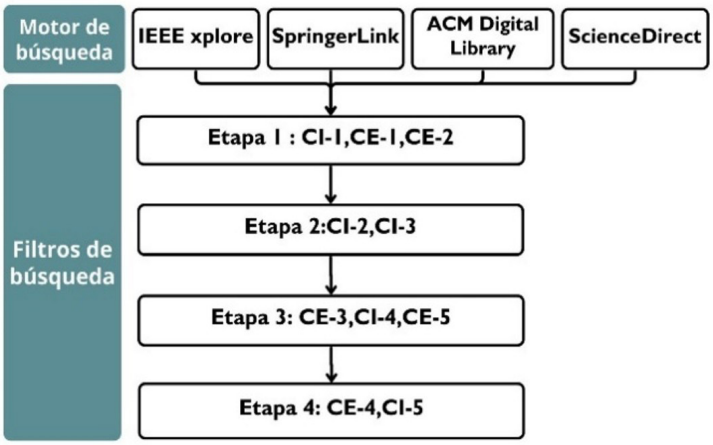

Figura 1. Proceso de selección de estudios primarios

Fuente: elaboración propia.

5. *Snowballing*

Para complementar la búsqueda automatizada, se llevó un proceso iterativo de bola de nieve hacia atrás y hacia adelante en los estudios identificados inicialmente, siguiendo las pautas metodológicas de Wohlin [13]. Todos los nuevos estudios identificados a través de este proceso iterativo se sometieron al mismo protocolo de selección detallado en la Figura 1, lo que garantiza la consistencia metodológica de nuestra revisión.

6. Síntesis

Para la síntesis de datos, se optó el método de síntesis narrativa propuesto por Popay et al. [12], un enfoque flexible que puede complementar otras metodologías de síntesis. Este proceso de síntesis, así como referencias de los estudios primarios se encuentra en ExtracciónDeDatos.xlsx (https://

docs.google.com/spreadsheets/d/1Fe47vuB7aWOBeZa1bq9xCoE4715d-OCN/edit?gid=1828509478#-gid=1828509478) de EP1 (Estudio primario 1) hasta EP30.

Resultados

Después de implementar la estrategia de búsqueda mediante la cadena definida en las fuentes seleccionadas, se obtuvieron 16 estudios iniciales. Este conjunto inicial sirvió de base para aplicar la interacción de bola de nieve hacia adelante y hacia atrás, utilizando los mismos criterios de selección establecidos. Como resultado, se incorporaron 14 estudios adicionales, que pasaron por las mismas etapas de selección, como se muestra en detalle en la Figura 2b. Así, se conformó una selección final de 30 estudios primarios que constituyen la base de esta investigación. Los resultados de la búsqueda automatizada se presentan en detalle en la Figura 2, y la distribución de estudios por año, en la Figura 3.

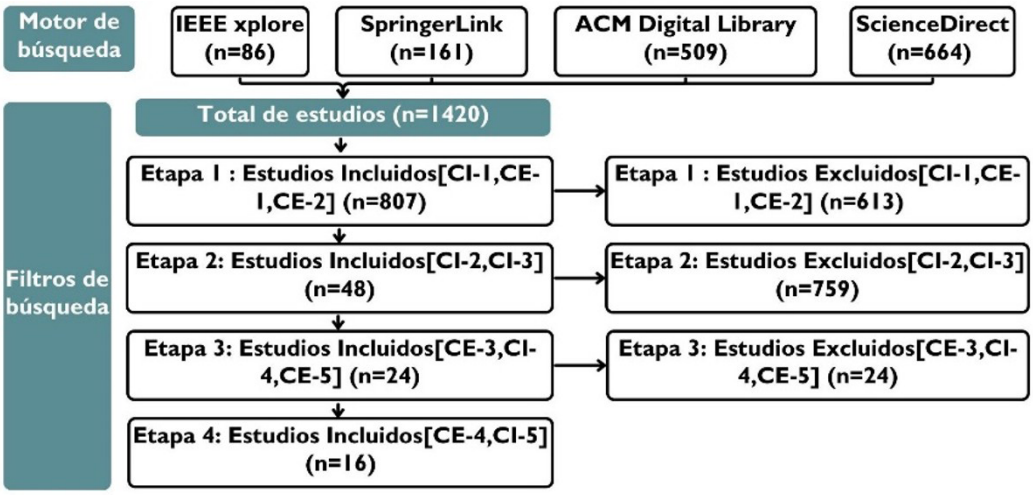

Figura 2. Resultados de selección de estudios primarios por etapa

Fuente: elaboración propia.

El proceso de selección de estudios mediante la técnica de *snowballing*, aplicada en ambas direcciones (*backward y forward*) sobre los resultados obtenidos en *Google Scholar*. A partir de un total de 946 estudios identificados inicialmente (433 provenientes del backward y 513 de la primera iteración), se aplicaron los criterios de inclusión y exclusión en cuatro etapas sucesivas. En la Etapa 1, se incluyeron 459 estudios que cumplían con los criterios iniciales (CI-1 y CE-1, CE-2), mientras que 487 fueron descartados. En la Etapa 2, tras aplicar los criterios CI-2 y CI-3, se mantuvieron 107 estudios, excluyéndose 352. Posteriormente, en la Etapa 3, al aplicar los criterios CE-3, CI-4 y CE-5, se seleccionaron 53 estudios adicionales. Finalmente, en la Etapa 4, se validaron 14 estudios que cumplían con los criterios CE-4 y CI-5, conformando el conjunto final derivado del snowballing. Este proceso, basado en fuentes provenientes de Google Scholar, permitió agregar más fuentes de literatura y garantizar la relevancia y calidad de los estudios primarios incluidos en la revisión.

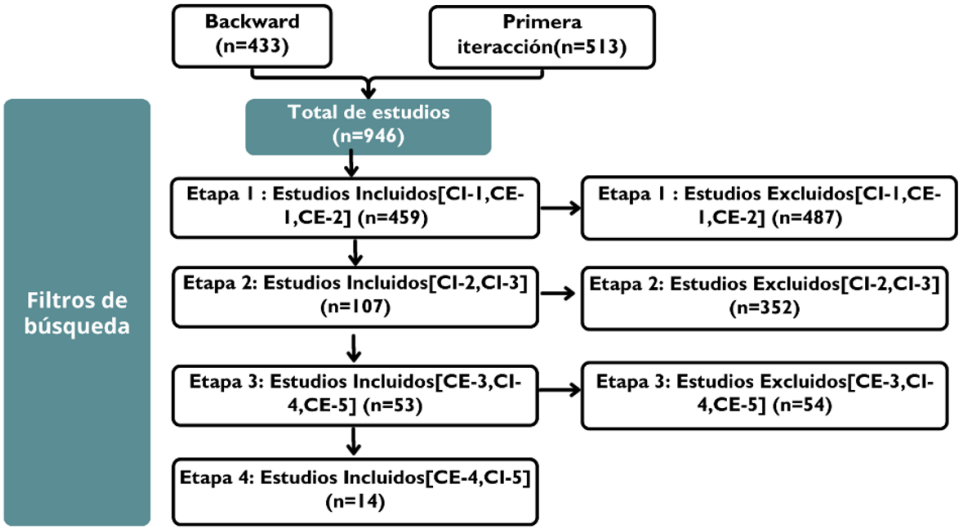

Figura 2b. Resultados de selección de snowballing de estudios primarios por etapa

Fuente: elaboración propia.

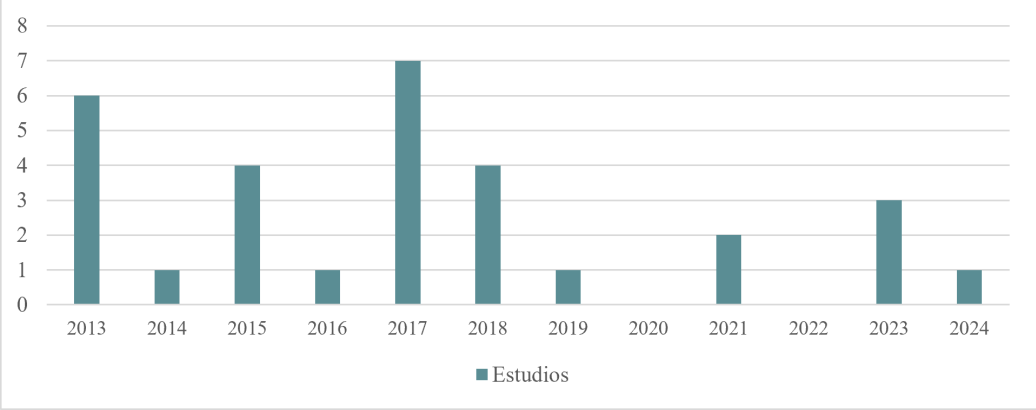

Figura 3. Distribución de estudios por año de publicación

Fuente: elaboración propia.

PI1. ¿Qué prácticas reportadas en la literatura contribuyen a reducir el consumo de energía en la fase de prueba de software?

Durante esta investigación, se analizaron diferentes enfoques, técnicas y métodos para identificar prácticas relacionadas a reducir el consumo de energía en pruebas de software. Estas prácticas se presentan en estudios que buscan hacer que el proceso de prueba sea más eficiente energéticamente, como la reducción de casos de prueba, el uso de algoritmos de optimización, herramientas de estimación de energía y técnicas de monitoreo de energía. La Figura 4 muestra las prácticas identificadas en los artículos.

Figura 4. Frecuencia de Prácticas

Fuente: elaboración propia.

A. Uso de técnicas de evaluación de energía

El consumo de energía en las pruebas de software ha sido abordado desde varias perspectivas. Se han propuesto el uso de minería de datos y aprendizaje automático para construir modelos predictivos de consumo energético, mientras que otros han explorado las pruebas metamórficas como una alternativa para evaluar la relación entre entradas y salidas sin necesidad de un valor de salida esperado. Sin embargo, este enfoque enfrenta desafíos como la definición de relaciones metamórficas y la automatización del proceso. Otra técnica utilizada es la creación de perfiles de energía de software, que permite estimar el consumo basándose en datos de aplicaciones similares, aunque su precisión puede verse afectada por la influencia del entorno de ejecución [14, 3, 15]. Uno de los ejemplos para aplicar este tipo de práctica, es el enfoque que integra los niveles tradicionales de prueba con la medición del consumo energético, aprovechando casos de uso existentes para evaluar tanto la funcionalidad como el impacto energético. La Estimación del consumo energético mediante el tamaño, complejidad y dependencias del código (EP1). El estimador de energía desarrollado busca reducir el impacto de las características del hardware y permite realizar pruebas mediante monitoreo de hardware y técnicas de perfilado.

B. Uso de técnicas de ahorro de energía

Para este tipo de práctica a diferencia de utilizar técnicas de evaluación, el ahorro energético es durante todo el proceso de prueba de software de recursos físicos que están involucrados. Esto puede lograrse mediante estrategias que optimicen el uso de los recursos computacionales, una de las técnicas en este ámbito es el Escalado Dinámico de Voltaje y Frecuencia (DVFS), que reduce el consumo de energía al ajustar la velocidad de procesamiento de acuerdo con la demanda esperada [16]. Esta práctica resulta

útil en pruebas de regresión, donde los casos de prueba se ejecutan repetidamente en diferentes versiones del software, ofreciendo la oportunidad de aplicar enfoques adaptativos sin afectar el rendimiento. Un estudio piloto con programas de escala media demostró que la aplicación de DVFS puede generar un ahorro energético promedio del 34,2%, evidenciando su eficacia en entornos de prueba. En dicho estudio se compararon diversos algoritmos de asignación de frecuencia, entre los cuales PAST (P) ajusta la frecuencia del CPU en función de su utilización (aumentándola por encima del 70% y reduciéndola por debajo del 50%), mientras que Online (O) emplea aprendizaje en línea para seleccionar la frecuencia óptima.

C. Evaluación de energía en técnicas de prueba

La evaluación energética en las técnicas de prueba representa una práctica que busca integrar criterios de sostenibilidad en los procesos de prueba que comúnmente se ocupan. Asi como también existe una gran variedad de técnicas de prueba, el consumo de energía puede variar significativamente según factores como el tipo de prueba, la configuración del entorno y la complejidad del software evaluado. El estudio informa que el uso de herramientas como Green-JEXJ permite la medición simultánea de la efectividad de las pruebas y su impacto energético [17]. Esta herramienta integra JEXJ, utilizado para calcular la cobertura de sucursales en programas Java, con JouleMeter, que permite monitorizar el consumo energético. La evaluación energética se realiza durante la ejecución del caso de prueba, lo que permite la identificación de pruebas costosas en términos de consumo. Además, se incorporan componentes como JEXNCT, que mejora la cobertura a través de transformaciones de código, y JCUTE, una herramienta de ejecución simbólica dinámica que supera las limitaciones comunes en los motores concolic.

D. Uso de técnicas minimización en prueba

El uso de técnicas de minimización en pruebas se presenta como una práctica esencial para optimizar recursos y mejorar la calidad del producto. Entre los elementos más notables de estas técnicas se encuentra la priorización de casos de prueba [18], que permite reducir los casos de prueba sin poner en riesgo la detección de fallos. Uno de estos ejemplos es la optimización de pruebas de regresión, una estrategia clave para reducir el esfuerzo de prueba, especialmente a través de la priorización de casos de prueba. Este enfoque busca ejecutar los casos en un orden que maximice la detección temprana de fallas de regresión, utilizando criterios de cobertura y algoritmos de búsqueda para definir dicho orden [19].

Otro elemento relevante es el uso de algoritmos genéticos basados en hipervolumen (HGA) para priorizar casos de prueba considerando múltiples criterios [20]. Los resultados de este enfoque sugieren que HGA es más eficiente y rentable que otros métodos, ya que mantiene una alta cobertura y reduce el consumo energético asociado a las pruebas. La minimización de suites de prueba basada en el consumo energético (EP3) aborda la minimización de suites orientadas a energía mediante la priorización

de casos de prueba que cubren puntos críticos de consumo energético. Por su parte, la minimización de suites de prueba para aplicaciones móviles (EP10) responde a la necesidad de gestionar eficientemente grandes suites diseñadas para evaluar el consumo energético de aplicaciones móviles. Se introducen métricas como eCoverage, que mide la cobertura de segmentos de código con alto consumo energético por cada caso de prueba y permite priorizar los casos más relevantes. Los resultados experimentales indican una reducción promedio del 84 % en el tamaño de las suites de prueba, manteniendo su efectividad en la detección de errores energéticos.

La optimización de suites de prueba basada en energía (EP11) utiliza programación lineal entera (ILP) para optimizar suites de prueba, asegurando que los casos seleccionados cumplan criterios específicos de minimización energética. Esta técnica logra una reducción de hasta el 95 % en el consumo energético de las pruebas, manteniendo la cobertura de requisitos. El método propuesto optimiza el consumo de energía en suites de prueba, en las que la selección de casos se formula como un problema de minimización con restricciones. Cada caso de prueba se representa con una variable binaria (bi), y el objetivo es minimizar la energía total mientras se cumplen criterios como la cobertura de código, expresados mediante restricciones lineales. La técnica se integra fácilmente en flujos existentes y es compatible con diversos criterios de prueba.

Otro ejemplo es la comparación del consumo energético de suites de prueba minimizadas mediante EDTSO (Energy Directed Test Suite Optimizer) frente a un método tradicional basado en tamaño, a partir de 70 000 problemas de minimización (10 000 por aplicación) con requisitos de cobertura aleatorios. Los resultados mostraron que, en el 92 % de los casos, EDTSO produjo suites con menor consumo energético que el enfoque tradicional, sin ningún caso de mayor consumo, con ahorros promedio del 3,8 % al 17,9 % y mejoras máximas cercanas al 100 % en ejecuciones individuales. Estos hallazgos evidencian que EDTSO es consistentemente más eficiente y permite reducciones significativas en el consumo de energía sin comprometer la cobertura de prueba.

E. Uso de Herramientas de Evaluación de Energía

Para implementar la ingeniería de software ecológica y sostenible, los equipos de desarrollo pueden apoyarse en herramientas como la Integración Continua (CI), que permite minimizar el esfuerzo de integración y obtener retroalimentación constante sobre la calidad del software (EP8). Al integrar la medición de eficiencia energética en este proceso, los desarrolladores pueden monitorear el consumo de energía a lo largo del ciclo de desarrollo. Se utilizan métodos como medidores de potencia de hardware y modelos de estimación de consumo energético basados en el uso de CPU para medir el impacto de las pruebas. Herramientas como *TestNG* y servidores CI como Jenkins pueden extender sus informes para incluir métricas de eficiencia energética, lo que permite a los desarrolladores identificar y corregir problemas de consumo energético.

Diversos estudios han explorado formas de medir el consumo energético del software (SEC), comparando el consumo de energía entre diferentes versiones de productos y proporcionando información relevante para los desarrolladores. Sin embargo, se ha identificado un conocimiento limitado sobre la eficiencia energética y la falta de prácticas claras para reducir el SEC, además de incertidumbre sobre cómo el software consume energía. En este contexto, se ha desarrollado un estudio de casos múltiples que propone un tablero de energía para monitorear el consumo energético durante el desarrollo del software [21]. Para medir el consumo energético del software (SEC), se utilizó Microsoft Joulemeter (JM), un enfoque basado en software que estima el consumo total de energía del sistema en tiempo de ejecución, con mediciones cada segundo. El tablero muestra el consumo de recursos con base en un punto de referencia, en los resultados se evidenció una reducción del 2,15% en el consumo energético de un nuevo lanzamiento en comparación con el anterior, representado visualmente mediante colores que indican la magnitud del cambio: verde para disminuciones y rojo para incrementos. Este enfoque, aplicado a múltiples lanzamientos, permite evaluar la evolución del consumo energético a lo largo del tiempo.

F. Correción de Code Smells

Los olores de código en Android podrían afectar el consumo de energía, se presentan dos herramientas: Adoctor, que detecta 15 olores de código específicos de Android mediante análisis estático y fue evaluado en 18 aplicaciones. Los resultados muestran que los "code smells" aumentan significativamente el consumo de energía, especialmente aquellos métodos que contienen múltiples olores de código. Cuatro olores de código con mayor impacto en el consumo energético fueron identificados: *"Leaking Thread", "Member Ignoring Method*", "*Slow Loop*" e "*Internal Setter*". La refactorización de estos olores juega un papel crucial en la mejora de la eficiencia energética [22]. PETRA es una herramienta que extrae perfiles de energía de aplicaciones Android, y se evaluó con 54 aplicaciones móviles utilizando un conjunto de datos público, comparando sus mediciones de energía con datos reales de consumo. La corrección de olores de código en pruebas de software es una estrategia efectiva para mejorar el consumo de energía durante la fase de prueba. Misu et al. [23] demuestra que los *test smells*, es decir, malas prácticas o estructuras ineficientes en el código de prueba, incrementan significativamente el consumo. Esta situación se agrava cuando un test case acumula múltiples instancias de smells, ya que la energía requerida crece proporcionalmente.

Entre los *test smells* que el autor asoció con un alto consumo energético destacan *Assertion Roulette* (AR), *Lazy Test* (LT) y *Eager Test* (ET). Estos olores no solo dificultan la mantenibilidad del código, sino que también generan sobrecarga computacional innecesaria durante la ejecución de pruebas, lo cual se traduce directamente en mayor gasto de energía. La eliminación mediante reescritura o reestructuración del código permite reducir este consumo, las evidencias de pruebas refactorizadas presentaron reducciones significativas en el consumo energético, con una diferencia promedio de hasta

20 joules por caso de prueba. Este resultado valida que la corrección de test smells no solo mejora la calidad del código, sino que también contribuye a la sostenibilidad del proceso de prueba.

PI2. ¿Qué actividades de prueba de software están asociadas con el consumo de energía?

Gestión de datos y entornos de prueba [24], es una actividad crítica que puede influir en el consumo de energía. El conocimiento sobre la organización, sus procesos, el negocio, el dominio del producto y las preferencias de los colegas es esencial para lograr los objetivos del proyecto. En este contexto, los desafíos relacionados con la gestión del conocimiento pueden explicarse por la falta de recursos adecuados, como conjuntos de datos y entornos de prueba mal aprovisionados, además de una estructura organizativa que no asigna recursos dedicados a las actividades de prueba.

En la Figura 5, se puede apreciar actividades con mayor consumo reportado en los artículos.

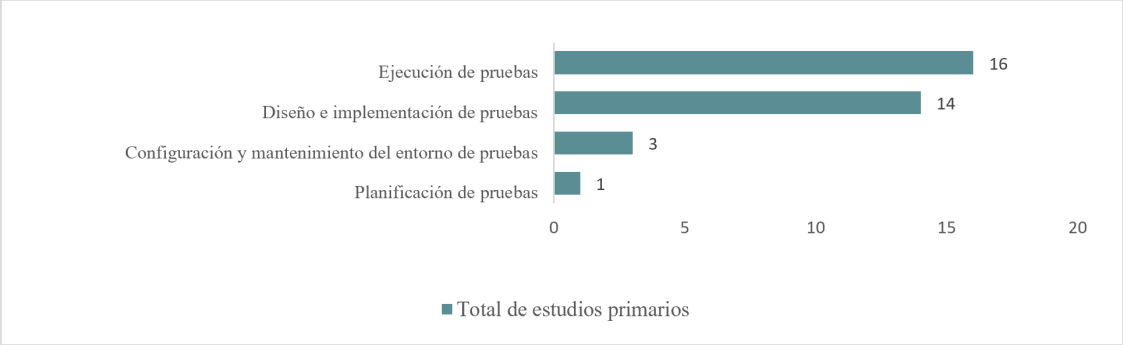

Figura 5. Actividades con mayor consumo de energía

Fuente: elaboración propia.

Las actividades de prueba de software asociadas con el consumo de energía incluyen la ejecución del conjunto de pruebas. Se ha observado que el consumo de energía de una prueba de funcionamiento es menor en comparación con una construcción completa, lo que representa entre el 65 % y el 73 % del consumo total de energía de una construcción. Sin embargo, existe en el consumo de energía una diferencia entre la construcción del software y la ejecución de pruebas, dependiendo de la plataforma utilizada [18].

La estimación del consumo de energía en las pruebas de software depende no solo de la ejecución directa de la prueba, sino también de factores estructurales del software, como las dependencias del método [14]. Desde esta perspectiva, la dependencia energética se refiere a la energía consumida por fragmentos de código ejecutados en el contexto del método bajo prueba; es decir, incluye el consumo de cualquier método invocado directamente. Esta información se puede derivar del gráfico de llamadas del programa, que proporciona una visión más completa del impacto energético de una prueba individual.

PI3. ¿Qué métodos se utilizan para reducir el consumo de energía en las prácticas de prueba identificadas?

Los métodos representan enfoques técnicos y estratégicos que buscan optimizar tanto la ejecución de pruebas como el uso de recursos computacionales. En este sentido, la Tabla 4 presenta de manera organizada los principales métodos encontrados dentro de los estudios analizados.

Tabla 4. *Métodos para reducir el consumo de energía*

ID	Práctica	Método o herramienta	Estudio
P1	Uso de técnicas de evaluación de energía	Energy profiling Random decision forests for profiling energy usage Estimación de consumo energético mediante el tamaño, complejidad y dependencias del código	Ep1, ep4, ep13, ep28
P2	Uso de técnicas de ahorro de energía	Dynamic voltage and frequency scaling	Ep2
P3	Evaluación de energía en técnicas de prueba	Green-jexj	Ep6
P4	Uso de técnicas minimización en prueba	Test-suite minimization Hypervolume genetic algorithm for test case prioritization Energy-aware test-suite minimization problem can be represented as an ip model Energy-directed test suite optimizer (edtso) Hypervolume based search for test case prioritization Gtcm Generalized tree reduction algorithm (gtr) Delta Multi-criteria test case prioritization	Ep3, ep7, ep11, ep12 ep16, ep17. Ep20, ep24, ep25, ep26, ep29, ep30
P5	Uso de herramientas de evaluación energética	Mats tool Ct-3 powermeter, Microsft joulemeter Green-j3 model Greenabce Petra	Ep5, ep9, ep4, ep14, ep15, ep18, ep21, ep23 ,ep10
P6	Corrección de code smells	Adoctor Refactorización	Ep7, ep27

Fuente: elaboración propia

La práctica de evaluación energética se centra en analizar cómo el software consume energía durante su ejecución. Una de las técnicas más empleadas es *Energy Profiling*, que permite identificar las partes del código o los procesos que más recursos consumen. Esta técnica recopila datos sobre el uso del CPU, la memoria y el tiempo de ejecución, relacionándolos con el consumo energético total (EP4). Entre los métodos utilizados para el perfilado energético destaca el uso de *Random Decision Forests*, un enfoque basado en aprendizaje automático que permite predecir y clasificar patrones de consumo energético a partir de mediciones previas [25]. Complementariamente, el método de estimación de consumo energético mediante el tamaño, la complejidad y las dependencias del código, que consiste en calcular el gasto energético esperado de un programa en función de métricas estáticas del software, como el número de

líneas de código, la cantidad de llamadas entre módulos y la complejidad ciclomática (EP1). En conjunto, estos enfoques apoyan la detección temprana de ineficiencias y permiten aplicar optimizaciones dirigidas a reducir el consumo energético en la fase de prueba.

Técnicas en ahorro energía en la fase de prueba de software como optimizar el uso de los recursos, el ajuste dinámico de la frecuencia del procesador en función de la carga de trabajo. Una técnica destacada en este ámbito es el Escalado Dinámico de Voltaje y Frecuencia (DVFS), permite reducir el consumo de energía ajustando la velocidad de procesamiento según la demanda prevista. En particular, en las pruebas de regresión, donde los casos de prueba suelen ejecutarse repetidamente en diferentes versiones del software, se pueden aplicar enfoques basados en DVFS para minimizar la disipación energética sin afectar significativamente el rendimiento. Los algoritmos de asignación de frecuencia comparados en el estudio incluyen enfoques para pruebas y pruebas de regresión. PAST (P) ajusta la frecuencia dinámicamente según la utilización del CPU, aumentando si supera el 70% y disminuyendo si cae por debajo del 50%. Online (O) emplea estadísticas de ejecución y aprendizaje en línea para seleccionar la frecuencia más adecuada. EClass-Target (ET) crea un perfil de frecuencia basado en intervalos de ejecución, aunque introduce sobrecarga en las pruebas de regresión. Case Majority (CM) selecciona la frecuencia más eficiente para la mayoría de los casos de prueba sin necesidad de perfilado. Case Optimal (CO) optimiza aún más esta estrategia utilizando la frecuencia ideal previamente determinada para cada caso de prueba, representando el mejor rendimiento en técnicas no intrusivas. Las técnicas CO, CM y ET demostraron una reducción del consumo de energía en la prueba de software, siendo CO la mejor, logrando ahorros de hasta un 57.9 % en comparación con PAST y más del 30 % frente a la técnica aleatoria de referencia.

La evaluación de la energía mediante herramientas como JouleMeter, JPCT y JCUTE dentro del framework Green-ABCE. Este enfoque busca mejorar la cobertura de ramas en las pruebas concólicas mientras se monitorea y calcula el consumo de energía asociado [26, 27, 28]. Aunque la mejora en la cobertura de ramas conlleva un aumento en el consumo energético, el uso de JouleMeter permite medir y registrar el consumo de energía de forma precisa, lo que permite optimizar el proceso. Además, el empleo de técnicas como la transformación de programas con JPCT y la generación automática de casos de prueba con JCUTE contribuye a la eficiencia de las pruebas y la reducción del consumo energético, a pesar de que la generación de casos de prueba puede volverse más lenta debido al tiempo adicional requerido para la transformación del programa. Estas técnicas mostraron menor variabilidad en los consumos, lo que su eficiencia es consistente en diferentes casos de prueba.

Los métodos y técnicas de minimización en la fase de prueba y la reducción de entradas en los casos de prueba [29] y la reducción de casos de prueba con prioridad, se realizan a través del empleo de una técnica de priorización mediante una cola de prioridad que organiza los nodos por medio de criterios, como el orden de recorrido de los padres y nodos [15, 30, 31]. Esto permite procesar los nodos de

manera más eficiente, minimizando el tiempo de ejecución y el consumo de energía asociado con el procesamiento individual de cada nodo. Este enfoque de reducción basada en prioridades y agrupamiento eficiente contribuye a mejorar la eficiencia energética del proceso de prueba al disminuir los tiempos de cómputo sin comprometer la efectividad de las pruebas.

Por su parte, el marco de *GTCM* (*Green Test Case Minimization*) se centra en reducir el número de casos de prueba necesarios para cubrir los criterios MC/DC, utilizando una serie de herramientas integradas [32]. GTCM utiliza herramientas como jCUTE para generar casos de prueba y calcular la cobertura de ramas, mientras que Joulemeter mide el consumo de energía asociado con la ejecución de estos casos de prueba, como resultado presenta una disminución en el consumo de energía, ya que se reduce el número de casos de prueba como el consumo de energía del sistema.

El hipervolumen mide la calidad de un conjunto de soluciones como el tamaño total del espacio objetivo dominado por una o más soluciones, lo cual permite equilibrar la cobertura de declaraciones y minimizar el costo de ejecución de una suite de pruebas [33]. Este enfoque tiene como objetivo maximizar la cobertura y minimizar el costo de ejecución de los casos de prueba, lo que indirectamente contribuye a la reducción del consumo de energía durante las pruebas al optimizar el uso de recursos computacionales. La minimización de suites de prueba para aplicaciones móviles [34] esta técnica aborda la necesidad de gestionar eficientemente grandes suites de prueba diseñadas para evaluar el consumo energético de aplicaciones móviles.

El enfoque OPDD (Optimized Parallel Delta Debugging) optimiza la reducción de casos de prueba al evitar repeticiones innecesarias, logrando reducir significativamente el número de pruebas realizadas. La optimización ayudo a reducir el tiempo de respuesta de los casos de prueba entre un 1,3% y un 43%, dependiendo de los casos [15], y en algunos casos, el tiempo de respuesta se redujo hasta en un 74%. En conjunto, estos enfoques muestran el potencial de combinar técnicas de cobertura, minimización y optimización para lograr pruebas de software más eficientes y energéticamente sostenibles.

La priorización de casos de prueba utilizando el proceso *Analytic Hierarchy Process* (AHP) y su extensión con lógica difusa (FAHP) permite manejar la incertidumbre y mejorar la precisión en la toma de decisiones [35]. Este enfoque se basa en la identificación de criterios relevantes, la determinación de alternativas, la medición del impacto de los criterios en cada alternativa, la fuzificación de datos lingüísticos y la aplicación de AHP como técnica de apoyo a la toma de decisiones (DSS). Entre los criterios utilizados para la priorización se encuentran la eficiencia en costos y tiempo, la cobertura de requisitos, la probabilidad de detección de fallos, la conclusividad del veredicto y un indicador de desviación de los requisitos. La minimización del conjunto de pruebas utilizando criterios múltiples, como lo implementa la herramienta Nemo*: Multi-Criteria Test-Suite Minimization with Integer Nonlinear Programming* [36]. Este enfoque selecciona el mejor subconjunto del conjunto original de pruebas considerando criterios de

restricción, como mantener la cobertura de sentencias original, y criterios de optimización, como maximizar la detección de fallos.

La estimación del consumo energético en pruebas de software puede abordarse mediante distintas herramientas, entre ellas los métodos basados en modelos estiman el consumo de energía mediante funciones matemáticas, pero también requieren calibración para obtener estimaciones confiables. Los métodos basados en software, como PETRA, presentan un costo más bajo asi como una mejor capacidad para estimar rápidamente el consumo de energía a nivel de método. PETRA mostró ser eficaz, alcanzando una precisión dentro del 5 % en comparación con herramientas de hardware, y permitiendo identificar métodos específicos en aplicaciones Android que consumen más energía. [37, 38].

El modelo Green-J3 propone una metodología para medir el consumo energético en pruebas de software basadas en cobertura de condiciones modificadas/decisiones (MC/DC) usando pruebas concólicas [25, 26]. Este enfoque consta de cinco módulos principales: JPCT, JCUTE, JCA, JouleMeter y Energy Calculator. La integración de estos módulos permite analizar el tiempo de ejecución, la energía consumida y el rendimiento del programa bajo prueba. El modelo ha demostrado una mejora en la cobertura de ramas en un 7.45 % y una reducción significativa del consumo energético, evidenciando su eficancia como herramienta para optimizar pruebas de software desde una perspectiva sostenible. El *framework* Green-ABCE utiliza herramientas como JouleMeter, JPCT y JCUTE, este enfoque busca mejorar la cobertura de ramas en las pruebas concolicas mientras se monitorea y calcula el consumo de energía asociado (EP6). Aunque la mejora en la cobertura de ramas conlleva un aumento en el consumo energético, el uso de JouleMeter permite medir y registrar el consumo de energía de forma precisa, lo que permite optimizar el proceso.

PI4. ¿Qué aportación tienen las herramientas de automatización en la reducción del consumo de energía en actividades de prueba?

Análisis de mutaciones de energía y generación automatizada de pruebas [22]. La herramienta MATS utiliza el análisis de mutaciones de energía y la generación automatizada de pruebas para evaluar la efectividad de los casos de prueba en la identificación de anomalías energéticas. El proceso comienza con la creación de un modelo abstracto del sistema bajo prueba (SUT) y una consulta para guiar la generación de casos de prueba. Este enfoque combina simulación, mutación controlada y criterios para optimizar las pruebas en sistemas basados en energía.

Aunque los *testers* cuentan con herramientas para verificar la funcionalidad y la lógica de las aplicaciones, no existen herramientas específicas para realizar pruebas desde una perspectiva de ingeniería de software verde y sostenible [39]. Por lo tanto, se destaca la importancia de contar con herramientas diseñadas específicamente para evaluar la eficiencia energética de las aplicaciones, lo que podría implicar la

integración de criterios de sostenibilidad en las fases de prueba. Además, se menciona que el aumento en la demanda de un alto rendimiento y nuevos modelos de uso continuará impulsando la necesidad de mejorar la eficiencia energética, especialmente en plataformas móviles y de escritorio.

Las herramientas de automatización contribuyen a reducir el consumo de energía en las pruebas de software optimizando la ejecución de casos de prueba y mejorando la cobertura del código. GreenJEXJ, que integra JEXJ para la cobertura de sucursales en Java con JouleMeter para medir el consumo de energía, lo que permite cuantificar y minimizar el consumo de energía de las pruebas (EP6). La adición de *Java Exclusive-NOR Code Transformer* (JEXNCT) aumentó la cobertura de la sucursal en un 7,45 % en promedio y redujo el consumo de energía en aproximadamente 75.945,1 julios.

Discusión

Esta investigación identificó las prácticas reportadas en la literatura. Las prácticas que tuvieron mayor representación fueron aquellas orientadas a la reducción del número de casos de prueba, sin comprometer la cobertura ni la detección de fallos, algunas como Test-Suite Minimization, EDTSO, GTCM, GTR, DELTA y enfoques multicriterio, que abarcaron la mayor cantidad de estudios analizados.

Estas prácticas se han reportado en dos contextos principales: entornos controlados y proyectos industriales, cada uno con características y desafíos distintivos. En entornos controlados, predominan los enfoques basados en herramientas automatizadas y algoritmos de optimización ILP, DVFS que se emplean en los estudios [16, 35], donde las métricas de eficiencia energética se validan en condiciones ideales. Estos estudios suelen enfatizar la reducción teórica del consumo (hasta un 95 % en suites de prueba optimizadas) pero con limitaciones en escalabilidad o integración con pipelines industriales (EP11; EP2). Por otro lado, en los proyectos industriales, las prácticas reportadas se centran en la integración con CI/CD (Jenkins), monitoreo continuo (tableros de energía) y refactorización de code smells (Leaking Thread), con ahorros más modestos pero aplicables a contextos reales (EP7).

La literatura reporta técnicas para reducir el consumo energético en pruebas de software, destacando enfoques como el Escalado Dinámico de Voltaje y Frecuencia (DVFS) con evidencia de ahorros del 34.2 % al ajustar dinámicamente la frecuencia del procesador según la carga de trabajo, particularmente efectivo en pruebas de regresión [16]. Los algoritmos de optimización como ILP (Programación Lineal Entera) y genéticos mostraron mayor versatilidad, logrando reducciones de hasta el 95 % en suites de prueba al priorizar casos críticos (EP11; EP7). Para aplicaciones móviles, herramientas como PETRA y Adoctor permitieron identificar y corregir olores de código (e.g., *Leaking Thread*) que incrementan hasta un 300 % el consumo, validando que la refactorización guiada por métricas energéticas es clave en este dominio (EP7). Sin embargo, técnicas emergentes como pruebas metamórficas o modelos predictivos

con ML enfrentan desafíos de generalización, evidenciando que las soluciones deben adaptarse al contexto específico [22, 40].

El análisis reveló que la ejecución de pruebas consume entre el 20 % y 88 % de la energía de una compilación completa, variando según la plataforma y frecuencia de ejecución [27]. Proyectos con alta actividad como Apache Flink registraron consumos anuales de 23,746 kWh (3,218 compilaciones), mientras que otros con menor actividad como LinkedIn Cruise-control mostraron solo 0.612 kWh (68 compilaciones), demostrando que la frecuencia de integración continua impacta significativamente la huella energética. Además, la preparación de entornos y datos de prueba surgió como una actividad crítica, donde la automatización de configuraciones y la gestión eficiente de recursos redujeron hasta un 15% el consumo en proyectos distribuidos (EP8).

El framework Green-J3 integró herramientas como JCUTE y JouleMeter para medir consumo durante pruebas concolicas, logrando un 7.45% más de cobertura con reducción energética (EP14). Técnicas como *Pardis Hybrid* (EP16) y OPDD (EP26) optimizaron la reducción de casos de prueba mediante agrupamiento, disminuyendo hasta un 74% el tiempo de ejecución. Destacan especialmente los enfoques basados en ILP, que resolvieron problemas de minimización energética en menos de 1 segundo, manteniendo la cobertura de código [41). No obstante, métodos avanzados como el análisis de mutaciones energéticas (MATS) requieren mayor validación industrial, pues, aunque detectan eficientemente anomalías, su configuración es compleja (EP5).

Las herramientas automatizadas demostraron ser esenciales para escalar las prácticas de eficiencia energética. Green-JEXJ redujo 75,945 Joules al integrar mediciones energéticas en pruebas de cobertura (EP6), mientras que tableros de energía en CI/CD (Jenkins) permitieron monitorear reducciones del 2.15% entre versiones de software (EP9). PETRA destacó por su precisión del 5% frente al hardware especializado, siendo clave para perfilar aplicaciones móviles (EP7). Sin embargo, persiste una brecha en las herramientas para pruebas sostenibles, ya que el 83% de las soluciones analizadas son académicas y pocas se integran con ecosistemas industriales como Selenium o TestNG (EP23).

Amenazas a la validez

Esta investigación se enfocó en identificar y analizar las prácticas, técnicas y herramientas orientadas a la reducción del consumo energético durante la etapa de prueba de software, sin pretender constituir una guía exhaustiva de aplicación. Su alcance se limita a la recopilación y síntesis de hallazgos documentados en la literatura académica, con el propósito de comprender los beneficios y desafíos asociados a las prácticas sostenibles en pruebas de software.

Entre las principales limitaciones, se reconoce que si bien el estudio se apoya en bases teóricas del área de prueba, no profundiza completamente en todos los niveles y tipos de prueba existentes, debido a las restricciones de tiempo y recursos disponibles. Limitó la inclusión de un mayor número de prácticas y técnicas reportadas en la literatura, enfocando el análisis en aquellas con evidencia y relevancia en la etapa de prueba.

Respecto a las amenazas este estudio, el acceso limitado a bibliotecas digitales y bases de datos de publicaciones. En consecuencia, se excluyeron estudios potencialmente relevantes, lo que puede haber afectado la profundidad del análisis. Esta limitación podría haber llevado a la omisión de ideas valiosas y contribuciones recientes que podrían haber enriquecido los resultados de esta revisión. Por otro lado, la fiabilidad de la selección del estudio radica en la subjetividad del investigador encargado de realizarlo manualmente.

Finalmente, la lengua materna del investigador es el español, no el inglés, lo que puede haber influido en la interpretación de los textos, la extracción de datos y la síntesis de la información. Sin embargo, este sesgo se mitigó mediante la supervisión parcial de los coautores de la investigación durante el desarrollo de la síntesis narrativa. En conjunto, estas consideraciones permiten establecer análisis transparente y riguroso, delimitando claramente los alcances, limitaciones y posibles fuentes de sesgo, al tiempo que fortalecen la credibilidad y consistencia de la revisión sistemática realizada.

Conclusiones

En conclusión, esta investigación resalta la importancia de utilizar prácticas que contribuyen a minimizar el consumo energético durante la fase de pruebas de software. La revisión permitió identificar enfoques, entre los que destacan las técnicas de minimización de pruebas, los métodos de evaluación y estimación del consumo energético, el uso de herramientas especializadas, la optimización de recursos mediante ajustes de voltaje y frecuencia, y la corrección de code smells. Esta revisión siguió una metodología establecida con fines académicos y de investigación, evaluando estudios primarios publicados entre 2013 y 2024. Asimismo, se documentaron las actividades específicas del proceso de estas prácticas.

En cuanto a los métodos utilizados, la investigación evidenció que los enfoques de reducción y priorización de casos de prueba son los más ampliamente explorados. Estos incluyen técnicas como *Test-Suite Minimization*, *Energy-Directed Test Suite Optimizer* (EDTSO), *Green Test Case Minimization* (GTCM) y *Generalized Tree Reduction* (GTR). Estas técnicas buscan mantener la cobertura y la detección de fallos con el mínimo número de ejecuciones, logrando reducciones de energía de entre 30% y 58% en los estudios revisados.

La optimización de recursos en la ejecución de pruebas se logra mediante métodos como el *Dynamic Voltage and Frequency Scaling* (DVFS), que ajusta dinámicamente la frecuencia y el voltaje del procesador según la carga de trabajo. Este enfoque demostró ahorros energéticos promedio del 34,2 %, alcanzando en algunos casos reducciones de hasta 57,9 % al aplicar algoritmos como *Case Optimal* (CO) *y Case Majority* (CM) en entornos de integración continua. Estos métodos confirman que es posible disminuir el consumo de energía sin comprometer el rendimiento del sistema ni la cobertura de las pruebas.

Respecto a las técnicas de evaluación energética, se identificaron métodos de perfilado como *Energy Profiling y Random Decision Forests for Profiling Energy Usage*, así como herramientas como PETRA, Softwatt, Green-J3, MATS, GreenABCE y Microsoft JouleMeter, que permiten estimar y monitorear el consumo energético con una precisión del 5 % en comparación con dispositivos de medición por hardware. En particular, el modelo Green-J3 integró módulos de cobertura (JPCT, JCUTE, JCA) con medición energética (JouleMeter y Energy Calculator), logrando una mejora del 7,45 % en cobertura y una reducción significativa en el consumo energético durante las pruebas basadas en cobertura MC/DC.

Por otra parte, la refactorización de *code smells* mediante herramientas como ADOCTOR también se consolidó como una práctica efectiva para reducir el consumo de energía, ya que mejora la estructura del código, reduce operaciones redundantes y optimiza la eficiencia en pruebas de regresión y mantenimiento. No obstante, los hallazgos también revelan desafíos importantes. Entre ellos, la falta de estandarización en las métricas de medición energética donde persiste una brecha de conciencia y formación en torno a la ingeniería de software verde, lo que limita la adopción de prácticas sostenibles en entornos productivos.

En síntesis, esta revisión demuestra que es posible mejorar la eficiencia energética de la fase de prueba mediante la combinación de técnicas de reducción, optimización y medición, apoyadas por herramientas y algoritmos especializados. Este trabajo ofrece una visión general de las prácticas existentes y sirve como referencia para investigadores y profesionales que buscan tratar la eficiencia energética en las pruebas de software.

Referencias

[1] H. Münzel, "Towards an ethical foundation of green software engineering," in *Proc. 10th IEEE Int. Conf. Global Softw. Eng. Workshops (ICGSEW)*, Ciudad Real, Spain, 2015, pp. 23–26. https://doi.org/10.1109/ICGSEW.2015.17 ↑

[2] S. Murugesan, "Harnessing green IT: Principles and practices," in *Green IT: Technologies and Applications*. Berlin, Germany: Springer, 2012, pp. 3–26. https://doi.org/10.1109/MITP.2008.10 ↑

[3] E. Jagroep *et al.*, "Awakening awareness on energy consumption in software engineering," in *Proc. 39th IEEE/ACM Int. Conf. Softw. Eng.: Softw. Eng. Soc. Track (ICSE-SEIS)*, Buenos Aires, Argentina, 2017, pp. 76–85. https://doi.org/10.1109/ICSE-SEIS.2017.10 ↑

[4] K. J. Valle-Gómez, P. Delgado-Pérez, I. Medina-Bulo, and J. Magallanes-Fernández, "Software testing: Cost reduction in Industry 4.0," in *Proc. 14th IEEE/ACM Int. Workshop Autom. Softw. Test (AST)*, Montreal, QC, Canada, 2019, pp. 69–70. https://doi.org/10.1109/AST.2019.00018 ↑

[4] I. Manotas *et al.*, "An empirical study of practitioners' perspectives on green software engineering," in *Proc. 38th IEEE/ACM Int. Conf. Softw. Eng. (ICSE)*, Austin, TX, USA, 2016, pp. 237–248. https://doi.org/10.1145/2884781.2884810 ↑

[5] S. Asadi, A. R. C. Hussin, and H. M. Dahlan, "Organizational research in the field of green IT: A systematic literature review from 2007 to 2016," *Telemat. Inform.*, vol. 34, no. 7, pp. 1191–1249, Nov. 2017. https://doi.org/10.1016/j.tele.2017.05.009 ↑

[6] R. Jabbarvand and S. Malek, "Advancing energy testing of mobile applications," in *Proc. 39th IEEE/ACM Int. Conf. Softw. Eng. Companion (ICSE-C)*, Buenos Aires, Argentina, 2017, pp. 491–492. https://doi.org/10.1109/ICSE-C.2017.45 ↑

[7] B. R. Bruce, J. Petke, and M. Harman, "Reducing energy consumption using genetic improvement," in *Proc. 2015 Annu. Conf. Genetic Evol. Comput. (GECCO '15)*, New York, NY, USA: ACM, 2015, pp. 1327–1334. https://doi.org/10.1145/2739480.2754752 ↑

[8] A. C. Moises, A. Malucelli, and S. Reinehr, "Prácticas de consumo energético para la ingeniería de software sostenible," in *Proc. 9th Int. Green Sustain. Comput. Conf. (IGSC)*, Pittsburgh, PA, USA, 2018, pp. 1–6. https://doi.org/10.1109/IGCC.2018.8752151 ↑

[9] B. A. Kitchenham, D. Budgen, and P. Brereton, *Evidence-Based Software Engineering and Systematic Reviews*, vol. 4. Boca Raton, FL, USA: CRC Press, 2015. https://doi.org/10.5555/2994449 ↑

[10] H. Zhang, M. A. Babar, and P. Tell, "Identifying relevant studies in software engineering," *Inf. Softw. Technol.*, vol. 53, no. 6, pp. 625–637, Jun. 2011. https://doi.org/10.1016/j.infsof.2010.12.010 ↑

[11] J. Popay *et al.*, "Guidance on the conduct of narrative synthesis in systematic reviews: A product from the ESRC Methods Programme," ESRC Methods Programme, Technical Report, 2006. https://doi.org/10.13140/2.1.1018.4643 ↑

[12] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng. (EASE '14)*, New York, NY, USA: ACM, 2014. https://doi.org/10.1145/2601248.2601268 ↑

[13] F. Wedyan, R. Morrison, and O. S. Abuomar, "Integration and unit testing of software energy consumption," in *Proc. 10th Int. Conf. Softw. Defined Syst. (SDS)*, San Antonio, TX, USA, 2023, pp. 60–64. https://doi.org/10.1109/SDS59856.2023.10329262 ↑

[14] G. Gharachorlu and N. Sumner, "Avoiding the familiar to speed up test case reduction," in *Proc. IEEE Int. Conf. Softw. Quality, Reliab. Secur. (QRS)*, Lisbon, Portugal, 2018, pp. 426–437. https://doi.org/10.1109/QRS.2018.00056 ↑

[15] E. Y. Y. Kan, "Energy efficiency in testing and regression testing — A comparison of DVFS techniques," in *Proc. 13th Int. Conf. Quality Softw. (QSIC)*, Nanjing, China, 2013, pp. 280–283. https://doi.org/10.1109/QSIC.2013.21 ↑

[16] S. Godboley, A. Dutta, B. Besra, and D. P. Mohapatra, "Green-JEXJ: A new tool to measure energy consumption of improved concolic testing," in *Proc. Int. Conf. Green Comput. Internet of Things (ICGCIoT)*, Greater Noida, India, 2015, pp. 36–40. https://doi.org/10.1109/ICGCIoT.2015.7380424 ↑

[17] R. Verdecchia, P. Lago, C. Ebert, and C. de Vries, "Green IT and green software," *IEEE Softw.*, vol. 38, no. 6, pp. 7–15, Nov.–Dec. 2021. https://doi.org/10.1109/MS.2021.3102254 ↑

[18] D. Di Nucci, A. Panichella, A. Zaidman, and A. De Lucia, "Hypervolume-based search for test case prioritization," in *Search-Based Software Engineering (SSBSE 2015)*, Lecture Notes in Computer Science, vol. 9275, M. Barros and Y. Labiche, Eds. Cham, Switzerland: Springer, 2015. https://doi.org/10.1007/978-3-319-22183-0_11↑

[19] G. Gharachorlu and N. Sumner, "Pardis: Priority aware test case reduction," in *Fundamental Approaches to Software Engineering (FASE 2019)*, Lecture Notes in Computer Science, vol. 11424, R. Hähnle and W. van der Aalst, Eds. Cham, Switzerland: Springer, 2019. https://doi.org/10.1007/978-3-030-16722-6_24 ↑

[20] M. Dick, J. Drangmeister, E. Kern, and S. Naumann, "Green software engineering with agile methods," in *Proc. 2nd Int. Workshop Green Sustain. Softw. (GREENS)*, San Francisco, CA, USA, 2013, pp. 78–85. https://doi.org/10.1109/GREENS.2013.6606425 ↑

[21] J. Larsson and E. P. Enoiu, "Test generation and mutation analysis of energy consumption using UPPAAL SMC and MATS," in *Proc. IEEE Int. Conf. Softw. Test. Verif. Validation Workshops (ICSTW)*, Dublin, Ireland, 2023, pp. 186–189. https://doi.org/10.1109/ICSTW58534.2023.00042 ↑

[22] Md. R. H. Misu, J. Li, A. Bhattiprolu, Y. Liu, E. S. de Almeida, and I. Ahmed, "Test smell: A parasitic energy consumer in software testing," *Inf. Softw. Technol.*, vol. 181, art. 107671, May 2025. https://doi.org/10.1016/j.infsof.2025.107671 ↑

[23] C. Camacho, S. Marczak, and T. Conte, "On the identification of best practices for improving the efficiency of testing activities in distributed software projects: Preliminary findings from an empirical study," in *Proc. 8th IEEE Int. Conf. Global Softw. Eng. Workshops (ICGSEW)*, Bari, Italy, 2013, pp. 1–4. https://doi.org/10.1109/ICGSEW.2013.7 ↑

[24] M. A. Beghoura, A. Boubetra, and A. Boukerram, "Green software requirements and measurement: Random decision forests-based software energy consumption profiling," *Requir. Eng.*, vol. 22, no. 1, pp. 27–40, Mar. 2017. https://doi.org/10.1007/s00766-015-0234-2 ↑

[25] A. Hindle, "Green mining: A methodology of relating software change and configuration to power consumption," *Empir. Softw. Eng.*, vol. 20, pp. 374–409, 2015. https://doi.org/10.1007/s10664-013-9276-6 ↑

[26] A. Zaidman, "An inconvenient truth in software engineering? The environmental impact of testing open source Java projects," in *Proc. IEEE/ACM Int. Conf. Autom. Softw. Test (AST)*, Lisbon, Portugal, 2024, pp. 214–218. https://doi.org/10.1145/3644032.3644461 ↑

[27] S. Godboley, S. Panda, A. Dutta *et al.*, "An automated analysis of the branch coverage and energy consumption using concolic testing," *Arab. J. Sci. Eng.*, vol. 42, pp. 619–637, 2017. https://doi.org/10.1007/s13369-016-2284-2 ↑

[28] S. Herfert, J. Patra, and M. Pradel, "Automatically reducing tree-structured test inputs," in *Proc. 32nd IEEE/ACM Int. Conf. Autom. Softw. Eng. (ASE)*, Urbana, IL, USA, 2017, pp. 861–871. https://doi.org/10.1109/ASE.2017.8115697 ↑

[29] D. Li, C. Sahin, J. Clause, and W. G. J. Halfond, "Energy-directed test suite optimization," in *Proc. 2nd Int. Workshop Green Sustain. Softw. (GREENS)*, San Francisco, CA, USA, 2013, pp. 62–69. https://doi.org/10.1109/GREENS.2013.6606423 ↑

[30] L. V. Povoa, P. W. Bignatto, C. E. Monteiro, D. Mueller, C. A. C. Marcondes, and H. Senger, "A model for estimating energy consumption based on resources utilization," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Split, Croatia, 2013, pp. 1–6. https://doi.org/10.1109/ISCC.2013.6754957 ↑

[31] S. Godboley, A. Dutta, and D. P. Mohapatra, "Reduced energy consumption for MC/DC testing," *Int. J. Bus. Inf. Syst.*, vol. 28, no. 4, pp. 447–467, 2018. https://doi.org/10.1504/IJBIS.2018.093657 ↑

[32] D. Di Nucci, "Methods and tools for focusing and prioritizing the testing effort," in *Proc. IEEE Int. Conf. Softw. Maintenance Evol. (ICSME)*, Madrid, Spain, 2018, pp. 722–726. https://doi.org/10.1109/ICSME.2018.00089 ↑

[33] R. Jabbarvand, A. Sadeghi, H. Bagheri, and S. Malek, "Energy-aware test-suite minimization for Android apps," in *Proc. 25th Int. Symp. Softw. Test. Analysis (ISSTA 2016)*, New York, NY, USA: ACM, 2016, pp. 425–436. https://doi.org/10.1145/2931037.2931067 ↑

[34] Sahar Tahvili, Mehrdad Saadatmand, and M. Bohlin, "Multi-Criteria Test Case Prioritization Using Fuzzy Analytic Hierarchy Process," *ResearchGate*, Nov. 15, 2015. https://www.researchgate.net/publication/281593743_Multi-Criteria_Test_Case_Prioritization_Using_Fuzzy_Analytic_Hierarchy_Process (accessed May 28, 2026)

[35] J.-W. Lin, R. Jabbarvand, J. Garcia, and S. Malek, "Nemo: Multi-criteria test-suite minimization with integer nonlinear programming," in *Proc. 40th IEEE/ACM Int. Conf. Softw. Eng. (ICSE)*, Gothenburg, Sweden, 2018, pp. 1039–1049. https://doi.org/10.1145/3180155.3180174 ↑

[36] D. Di Nucci, F. Palomba, A. Prota, A. Panichella, A. Zaidman, and A. De Lucia, "PETRA: A software-based tool for estimating the energy profile of Android applications," in *Proc. 39th IEEE/ACM Int. Conf. Softw. Eng. Companion (ICSE-C)*, Buenos Aires, Argentina, 2017, pp. 3–6. https://doi.org/10.1109/ICSE-C.2017.18 ↑

[37] S. Song, F. Wedyan, and Y. Jararweh, "Empirical evaluation of energy consumption for mobile applications," in *Proc. 12th Int. Conf. Inf. Commun. Syst. (ICICS)*, Valencia, Spain, 2021, pp. 352–357. https://doi.org/10.1109/ICICS52457.2021.9464579 ↑

[38] M. Mohankumar and M. Anand Kumar, "An empirical study on green and sustainable software engineering," 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:36428799. ↑

[39] A. Dutta, "Green-J3 model: A novel approach to measure energy consumption of modified condition/decision coverage using concolic testing," *CSI Trans. ICT*, 2017. https://doi.org/10.1007/S40012-017-0157-9 ↑

[40] D. Li, Y. Jin, C. Sahin, J. Clause, and W. G. J. Halfond, "Integrated energy-directed test suite optimization," in *Proc. Int. Symp. Softw. Test. Analysis (ISSTA 2014)*, New York, NY, USA: ACM, 2014, pp. 339–350. https://doi.org/10.1145/2610384.2610414 ↑

CONTENIDO

ALCANCE Y POLÍTICA EDITORIAL DE LA REVISTA

La revista Tecnura es una publicación institucional de la Facultad Tecnológica de la Universidad Francisco José de Caldas, de carácter científico-tecnológico con periodicidad trimestral, que se publica los meses de enero, abril, julio y octubre. Su primer número apareció en el segundo semestre del año 1997 y hasta la fecha ha mantenido su regularidad.

Las áreas temáticas de interés de la revista Tecnura están enfocadas a todos los campos de la ingeniería, como la electrónica, telecomunicaciones, electricidad, sistemas, industrial, mecánica, catastral, civil, ambiental, entre otras. Sin embargo, no se restringe únicamente a estas, también tienen cabida los temas de educación y salud, siempre y cuando estén relacionados con la ingeniería. La revista publica únicamente artículos de investigación científica y tecnológica, de reflexión y de revisión. En consecuencia, durante la fase de evaluación editorial inicial se rechazarán los artículos cortos y reportes de caso.

La revista Tecnura está dirigida a docentes, investigadores, estudiantes y profesionales interesados en la actualización permanente de sus conocimientos y el seguimiento de los procesos de investigación científico-tecnológica, en el campo de las ingenierías. Tiene como misión divulgar resultados de proyectos de investigación realizados en el área de las ingenierías, a través de la publicación de artículos originales e inéditos, realizados por académicos y profesionales pertenecientes a instituciones nacionales o extranjeras del orden público o privado. Los artículos presentados deben ser trabajos inéditos escritos en español o inglés; sin embargo, tendrán preferencia los artículos que muestren conceptos innovadores de gran interés, que traten sobre asuntos relacionados con el objetivo y cobertura temática de la revista.

Instrucciones para los autores

https://revistas.udistrital.edu.co/index.php/Tecnura/about/submissions

Tecnura es una publicación de carácter académico indexada en los Índices Regionales Scielo Colombia (Colombia) y Redalyc (México), además de las siguientes bases bibliográficas: INSPEC del Institution of Engineering and Technology (Inglaterra), Fuente Académica Premier de EBSCO (Estados Unidos), CABI (Inglaterra), Index Corpernicus (Polonia), Informe Académico de Gale Cengage Learning (México), Periódica de la Universidad Nacional Autónoma de México (México), Oceanet (España) y Dialnet de la Universidad de la Rioja (España). También hace parte de los siguientes directorios: Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal Latindex (México), Índice Bibliográfico Actualidad Iberoamericana (Chile), e-Revistas (España), DOAJ (Suecia), Ulrich de Proquest (Estados Unidos).

Tecnura es una revista arbitrada mediante un proceso de revisión entre pares de doble ciego. La periodicidad de la conformación de sus comités Científico y Editorial está sujeta a la publicación de artículos en revistas indexadas internacionalmente por parte de sus respectivos miembros.

La Universidad Distrital Francisco José de Caldas, sus directivas, el Editor, el Comité Editorial y Científico no son responsables por la opinión y criterios expresados en el contenido de los artículos y estos se publican bajo la exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento del Comité Editorial.

La revista Tecnura se edita exclusivamente en formato digital y se publica en su página web: http://revistas.udistrital.edu.co/ojs/index.php/Tecnura

TIPOS DE ARTÍCULOS ACEPTADOS

De acuerdo con la clasificación del Índice Nacional de Publicaciones Científicas y Tecnológicas (Publindex-Colciencias), la revista Tecnura recibe postulaciones de artículos inéditos de los siguientes tipos:

Artículos de investigación científica y tecnológica: documento que presenta, de manera detallada, los resultados originales de proyectos de investigación. La estructura generalmente utilizada contiene cuatro apartes importantes: introducción, metodología, resultados y conclusiones.

Artículo de revisión: documento resultado de una investigación donde se analizan, sistematizan e integran los resultados de las investigaciones publicadas o no publicadas, sobre un campo en ciencia o tecnología, con el fin de dar cuenta de los avances y las tendencias de desarrollo. Se caracteriza por presentar una cuidadosa revisión bibliográfica de al menos 50 referencias.

FORMATO DEL ARTÍCULO

Del lenguaje y estilo apropiado para la redacción de artículos

- Deben emplearse estructuras de oraciones simples, evitando las que sean demasiado largas o complejas.
- El vocabulario empleado debe ser básico y común. Los términos técnicos deben explicarse brevemente; asimismo, el significado de las siglas debe presentarse la primera vez que estas aparecen en el texto.
- Los autores son responsables de que su trabajo sea conducido de una manera profesional y ética.

De la extensión de los documentos

Los artículos no deben tener una extensión de más de 25 páginas en tamaño carta y a doble espacio, con márgenes simétricas de 3 cm. Solo en el caso de los artículos de revisión las 25 páginas no incluyen las referencias bibliográficas.

Del formato de presentación

Los artículos presentados deben ser trabajos inéditos escritos en español o inglés y deben digitarse en Microsoft Word (2003 en adelante), cumpliendo con las siguientes indicaciones:

Letra *Times New Román* de 12 puntos (a excepción de que se requiera lo contrario para algunos apartados).

- Una columna a doble espacio.
- Todas las márgenes de 3 cm.
- Los párrafos se justifican, y no debe haber espacio entre los consecutivos.
- No incluir saltos de página o finales de sección.
- Si se desea resaltar palabras o frases del texto, no usar letra negrita sino letra cursiva.
- Los decimales se deben señalar con coma (,) y no con un punto.
- Los millares y millones se deben señalar con un espacio fino.
- Evitar las notas de pie de página.
- Se debe utilizar nomenclatura arábiga hasta el tercer nivel únicamente.

De la estructura del documento

Los trabajos deben tener la siguiente estructura y cumplir con los siguientes requisitos:

Composición de un artículo

Todos los artículos remitidos para su evaluación y posible publicación por parte de la revista Tecnura deben tener por lo menos los siguientes componentes:

- Título en español e inglés.
- Información de los autores.
- Resumen en español e inglés.
- Palabras clave en español e inglés.
- Introducción.
- Conclusiones.
- Trabajo futuro (opcional).
- Agradecimientos (opcional).
- Referencias bibliográficas.

Si el artículo es de investigación científica y tecnológica deben tener, además de lo anterior, los siguientes componentes:

- Metodología.
- Resultados.
- Financiamiento.

Título

Título El título del artículo deberá ser corto o dividido en título y subtítulo, atractivo para el lector potencial y escrito en mayúscula sostenida. Este debe aparecer centrado entre las márgenes, escrito con letra *Times New Roman*, en negrita, tamaño de fuente 18. El título del artículo debe ir en español e inglés separado por un espacio doble. Máximo 20 palabras.

Autores

Después del título debe escribirse el (los) nombre(s) completo(s) del (los) autor(es), acompañado de los datos biográficos básicos: título de pregrado, título de posgrado, ocupación o cargo, afiliación institucional (institución donde labora), dependencia, ciudad, país y correo electrónico. La información anterior debe ir inmediatamente debajo del nombre del autor.

Resumen

Debe establecer el objetivo y alcance del trabajo, una descripción clara y concisa de la metodología, los resultados y las conclusiones obtenidas. Máximo 250 palabras.

Palabras clave

Debe escogerse entre tres y diez palabras clave, escritas en español con letra *Times New Roman*, en negrita y cursiva.

Las palabras clave deben estar escritas en orden alfabético y ser de uso estandarizado, para lo cual se sugiere utilizar bases de datos internacionales según el área del conocimiento. Por ejemplo, en el área de Eléctrica y Electrónica se sugiere utilizar el tesauro de la UNESCO que se pueden encontrar en la página: http://databases.unesco.org/thessp.

Abstract

Debe ser una traducción correcta y precisa al idioma inglés del texto que aparece en el resumen en español.

Keywords

Debe ser una traducción correcta y precisa al idioma inglés de la lista de palabras clave en español. Las *keywords* deben estar escritas en el orden de las palabras clave y ser de uso estandarizado, para lo cual se sugiere utilizar bases de datos internacionales según el área del conocimiento. Por ejemplo, en el área de Eléctrica y Electrónica se sugiere utilizar los Tesauros de la IEEE y/o World Bank que se pueden encontrar en las siguientes páginas respectivamente: http://www.ieee.org/documents/2009Taxonomy_v101.pdf,http://multites.net/mtsql/wb/site/default.asp

Introducción

Debe describir el planteamiento general del trabajo, así como contexto, antecedentes, estado de arte de la temática abordada, objetivo y posible alcance del trabajo.

Metodología

La redacción de este apartado debe permitir a cualquier profesional especializado en el tema replicar la investigación.

Resultados

Explicación e interpretación de los hallazgos. Si es necesario, se puede presentar una discusión breve y enfocada a la interpretación de los resultados.

Conclusiones

Implicación de los resultados y su relación con el objetivo propuesto.

Financiamiento

Mencionar la investigación asociada de la cual se derivó el artículo y la entidad que avaló y financió dicha investigación.

Agradecimientos

Preferiblemente deben ser breves y deben incluir los aportes esenciales para el desarrollo del trabajo.

Ecuaciones

Deben aparecer centradas con respecto al texto principal. Las ecuaciones deben ser referenciadas con números consecutivos (escritos entre paréntesis cerca al margen derecho). Las ecuaciones se citan en el texto principal empleando la palabra ecuación y seguida del número entre paréntesis. Las ecuaciones deben ser elaboradas en un editor de ecuaciones apropiado y compatible con el paquete de software InDesign, por ejemplo, el editor de ecuaciones de Windows.

Tablas

Para el caso de realización de tablas se recomienda que estas no sean insertadas como imágenes, considerando que en este formato no pueden ser modificadas. El encabezado de cada tabla debe incluir la palabra Tabla (en negrita) seguida del número consecutivo correspondiente y de un breve nombre de la tabla. El encabezado debe estar escrito con letra Times New Roman, en cursiva y tamaño de fuente 9.

No se presentan cuadros sino tablas y estas se deben levantar automáticamente desde el procesador de textos. Las tablas deben ir nombradas y referenciadas en el artículo, en estricto orden. Toda tabla debe tener en su parte inferior la fuente de la que fue tomada, o mencionar que es autoría de los autores si es el caso.

Figuras

Todas las figuras o fotografías deben enviarse en formato PNG o TIFF con una resolución mínima de 300 DPI, adaptadas a escala de grises.

El pie o rótulo de cada figura debe incluir la palabra Figura (en negrita) seguida del número consecutivo correspondiente y de una breve descripción del contenido de la figura. El pie de figura debe estar escrito con letra Times New Roman, en cursiva y tamaño de fuente 9. Las figuras deben ir nombradas y referenciadas en el artículo, en estricto orden. Toda figura debe tener también la fuente de la que fue tomada, o mencionar que es autoría de los autores si es el caso.

Símbolos

Los símbolos de las constantes, variables y funciones en letras latinas o griegas –incluidos en las ecuaciones– deben ir en cursiva; los símbolos matemáticos y los números no van en cursiva. Se deben identificar los símbolos inmediatamente después de la ecuación. Se deben utilizar las unidades, dimensiones y símbolos del sistema internacional.

Cuando se empleen siglas o abreviaturas, se debe anotar primero la equivalencia completa, seguida de la sigla o abreviatura correspondiente entre paréntesis y en lo subsecuente se escribe solo la sigla o abreviatura respectiva.

Referencias bibliográficas

Todas las referencias bibliográficas citadas dentro del texto se encuentran listadas en la sección Referencias. El formato en que se cita es el establecido por el Institute of Electrical and Electronics Engineers (IEEE). Puede consultar los materiales que pone a disposición el sistema de bibliotecas de la Universidad Distrital Francisco José de Caldas o el documento oficial de la IEEE

ENVÍO DE ARTÍCULOS

Los autores deben enviar sus artículos a través de la aplicación para tal fin del Open Journal System en formato digital, adjuntando la carta de presentación y el formato de información artículo-autores.

Carta de presentación

El artículo debe ir acompañado de una carta de presentación dirigida al director y editor de la revista, Ing. Lely Adriana Luengas Contreras, donde incluya:

- Solicitud expresa de considerar su artículo para publicarlo en la revista Tecnura.

- Título completo del trabajo.
- Nombres completos de todos los autores del trabajo.
- Certificación de la originalidad y el carácter inédito del trabajo.
- Exclusividad de su remisión a la revista Tecnura.
- Confirmación de la autoría con la firma de todos los autores.

Esta carta deberá estar firmada por todos los autores, escanearse y enviarse junto con los demás documentos solicitados.

Formato de información artículo-autores

El artículo además debe ir acompañado de un formato de información sobre el artículo y sus autores, el cual se puede descargar de la página web de la revista Tecnura: http://revistas.udistrital.edu.co/ojs/index.php/Tecnura, en la sección "Formatos y Documentos". Es importante completar todos los campos de información solicitados, algunos de ellos tienen comentarios para aclarar mejor lo que se está solicitando. El formato no debe escanearse.

Artículo

Artículo en formato digital (Word 2003 en adelante) que cumpla con todas las normas de presentación descritas en el capítulo 3, "Formato del artículo", de la presente en las instrucciones a los autores.

PROCEDIMIENTO PARA LA PUBLICACIÓN

El procedimiento que sigue la revista Tecnura para la evaluación y posible publicación de los trabajos enviados por los autores es el siguiente en orden cronológico:

1. Envío del articulo acompañado de la carta de presentación y el formato de información por parte de los autores.
2. Notificación al autor de correspondencia de la recepción del artículo.
3. Verificación del tema del artículo con respecto a las áreas de interés de la revista.
4. Verificación de las normas de presentación por parte del monitor de la revista.
5. Notificación al autor de correspondencia de la evaluación de las normas de presentación.
6. Envío de las correcciones realizadas por los autores con respecto a la evaluación de las normas de presentación

7. Envío del artículo a los árbitros seleccionados.
8. Notificación del inicio del proceso de arbitraje del artículo.
9. Notificación a los autores de la decisión tomada por el Comité Editorial y de las evaluaciones hechas por los árbitros.
10. Envío de las correcciones realizadas por los autores con respecto a las evaluaciones de los árbitros.
11. Estudio de la versión final del artículo y de las evaluaciones de los árbitros por parte del Comité Editorial.
12. Envío por parte de los autores de la carta de cesión de derechos al editor de la revista.
13. Envío de la versión con corrección de estilo y diagramada a los autores.
14. Verificación de errores y aprobación final de la versión con corrección de estilo y diagramada por parte de los autores.
15. Publicación del artículo en el número correspondiente de la revista Tecnura.
16. Notificación a los autores de la publicación del número de interés.
17. Envío de un ejemplar de la revista a cada autor del artículo publicado.

PROCESO DE ARBITRAJE DE ARTÍCULOS

Considerando la periodicidad trimestral de la revista, el Comité Editorial realiza cuatro convocatorias anuales para la recepción de artículos, aproximadamente en los meses de febrero, mayo, agosto y noviembre. Los artículos serán recibidos hasta la fecha máxima establecida en cada convocatoria.

Una vez recibidos los artículos el monitor de la revista realizará una primera evaluación de forma para verificar que cumplan con todos los elementos mencionados en esta guía de instrucciones a los autores. Luego de recibir nuevamente el articulo con las correcciones de forma solicitadas por el monitor de la revista, este será sometido a evaluación por tres pares académicos (paulatinamente se espera incorporar un mayor número de pares externos que participen en el proceso).

Cada artículo remitido a la revista Tecnura es revisado por dos pares académicos externos a la institución de los autores, mediante un proceso de "revisión entre pares" (*Peer-review*) de doble-ciego, garantizando el anonimato de los autores y evaluadores; se considera confidencial todo trabajo recibido y así se le exige a sus evaluadores.

Las posibles conclusiones de los resultados de la evaluación por parte de los árbitros son únicamente tres: publicar el artículo sin modificaciones, publicar el artículo con modificaciones o no publicar el artículo.

Posteriormente, el Comité Editorial toma la decisión de publicar o no los artículos, con base en los resultados de las evaluaciones realizadas por los árbitros asignados. En caso de existir contradicciones en las evaluaciones con respecto a la publicación de un artículo, el Comité Editorial enviará el artículo a un tercer árbitro y se inclinará por las dos evaluaciones que tengan el mismo concepto respecto a la publicación del artículo.

En cada convocatoria el autor de correspondencia debe sugerir al menos cuatro posibles evaluadores externos a su institución laboral, los cuales deben ser especialistas en el tema específico del artículo remitido, tener al menos maestría y por lo menos dos deben ser internacionales. Los posibles evaluadores pueden pertenecer a una universidad o industria, pública o privada; de estos se debe proporcionar el nombre completo, su formación académica más alta, su afiliación institucional y su correo electrónico. Estos cuatro potenciales evaluadores serán analizados por el Comité Editorial a fin de ampliar la base de datos de los árbitros de la revista Tecnura.

El Comité Editorial de la revista Tecnura se reserva los derechos de impresión, reproducción total o parcial del artículo, así como el de aceptarlo o rechazarlo. Igualmente, se reserva el derecho de hacer cualquier modificación editorial que estime conveniente; en tal caso el autor recibirá por escrito recomendaciones de los evaluadores. Si las acepta, deberá entregar el artículo con los ajustes sugeridos dentro de las fechas fijadas por la revista para garantizar su publicación dentro del número programado.

CONTACTO

Para cualquier solicitud de información adicional puede comunicarse a través del correo electrónico de la revista Tecnura: tecnura@udistrital.edu.co, tecnura@gmail.com, o por mensajería con el Ing. Lely Adriana Luengas Contreras, Director y Editor de la revista Tecnura, a la dirección:

Revista Tecnura
Sala de Revistas, Bloque 5, Oficina 305. Facultad Tecnológica
Universidad Distrital Francisco José de Caldas Transversal 70 B N. 73 a 35 sur
Teléfono: 571 – 3239300 Extensión: 5003
Celular: 57–3153614852
Bogotá D.C., Colombia
Email: tecnura.ud@correo.udistrital.edu.co, tecnura@gmail.com
Página web: https://revistas.udistrital.edu.co/ojs/index.php/Tecnura

Instructions for authors

https://revistas.udistrital.edu.co/index.php/Tecnura/about/submissions

CONTENT

Tecnura journal is an institutional publication of the Faculty of Technology from University Francisco José de Caldas. It is a scientific and technological publication with quarterly periodicity, which is published in January, April, July and October. The first issue appeared in the second semester of 1997 and up to now it has maintained its regularity.

The areas of interest of Tecnura journal are focused on all engineering fields such as electronics, telecommunications, electricity, systems, industrial, mechanics, cadastral, civil, environmental, among others. However, it is not restricted to those; it also has room for education and health issues, as long as they are related to engineering. The journal will only publish concerning scientific and technological research, reflection and revision. In consequence, during the initial editorial evaluation, short articles and case reports will be rejected.

Tecnura Journal is addressed for professors, researchers, students and professionals interested in permanent update of their knowledge and follow-up of scientific-technologic processes in the field of engineering. Tecnura Journal has as mission to disseminate results of research projects in the areas of engineering, through the publication of original and unpublished articles, conducted by academics and professionals accredited by public or private national or foreign institutions. Articles submitted to Tecnura journal must be unpublished works written in Spanish or English; nevertheless, preference will be given to articles that show innovative concepts of great interest, related to the objective and scope of the journal.

Tecnura is an academic publication indexed in the Regional Index Scielo Colombia (Colombia) and Redalyc (México); as well as of the following bibliographic databases: INSPEC of the Institution of Engineering and Technology (England), Fuente Académica Premier of EBSCO (United States), CABI (England), Index Copernicus (Poland), Informe Académico of Gale Cengage Learning (México), Periódica from the Universidad Nacional Autónoma de México (México), Oceanet (Spain) and Dialnet from the

Universidad de la Rioja (Spain). It is also part of the following directories: Online Regional Information System for Scientific journals from Latin America, Caribbean, Spain and Portugal Latindex (México), Bibliographic Index Actualidad Iberoamericana (Chile), e-Revistas (Spain) , DOAJ (Sweden) and Ulrich of Proquest (United States).

Tecnura is a journal arbitrated by a revision process among double blind peers. The schedule of the conformation of its scientific and editorial committee is subject to the publication of articles in internationally indexed journals by their members.

District University Francisco José de Caldas, its directors, the editor, the editorial and scientific committee are not responsible for the opinions and the criteria expressed in the content of the articles and they are published under the exclusive responsibility of the authors and do not necessarily reflect the ideas of the editorial committee.

Tecnura journal is published exclusively in digital format and is available on its website: http://revistas.udistrital.edu.co/ojs/index.php/Tecnura/index

TYPE OF ARTICLES ACCEPTED

According to the classification of the Scientific and Technological Publications National Index (Publindex-Colciencias), Tecnura journal receives nominations of unpublished articles on the following topics:

- **Scientific and technological research articles:** document that presents, in a detailed manner, the original results of research projects. The generally used structure contains four main parts: introduction, methodology, results and conclusions.
- **Reflection articles:** document that presents research results from an analytic, interpretative or critic perspective from the author, dealing with a specific topic and adopting original sources.
- **Review article:** document that results from a research where the results of published or unpublished research on a science or technology field are analyzed, systematized and integrated, in order to state the advances and tendencies in development. It is characterized for presenting a careful bibliographical review of at least 50 references.

ARTICLE FORMAT

About the appropriate language and style for articles writing

- Authors must use simple sentence structures, avoiding those too long or complex.

- The vocabulary used must be basic and common. Technical language must be briefly explained; also, the meaning of the acronyms must be given the first time they appear in the text.
- The authors are responsible for their work to be conducted in a professional and ethic manner.

About the length of articles

The articles should not exceed 25 pages in letter size and double space, with symmetric margins of 3 cm. Only in the case of review articles, these 25 pages do not include references.

About the presentation format

Submitted articles must be unpublished works written in Spanish or English, and must be typed in Microsoft Word (2003 and beyond), complying with the following indications:

- *Times New Roman* letter, 12 point (except it is required for some sections).
- One column, double-spaced.
- All the margins 3 cm.
- Paragraphs should be justified without spaces between consecutives and without cutting words.
- Do not include page breaks or section finals.
- If you want to emphasize words or phrases from the text, do not use bold letters but italic.
- Decimals should be pointed with comma (,) and not with period (.).
- Thousands and millions should be pointed with a fine space.
- Avoid footnotes.
- Arabic nomenclature must be used only until the third level.

About the article structure

The papers must have the following structure and comply with the following requirements:

Composition of an article

All the articles submitted for evaluation and possible publication by the Tecnura Journal must have at least the following components:

- Title in Spanish and English.
- Information about the authors.

- Abstract in Spanish and English.
- Key words in Spanish and English.
- Introduction.
- Conclusions.
- Future work (optional).
- Acknowledgements (optional).
- Bibliographical references.

If the article is related to scientific and technological research must have, in addition to the above, the following components:

- Methodology.
- Results.
- Financing.

Title

The title of the article must be short or divided in title and subtitle, attractive for the potential reader and written in capital letters. It should appear centered between the margins, written in *Times New Roman* letter, in bold, font size 18. The title of the article has to be in Spanish and English separated by double space. Maximum 20 words.

Authors

After the title the complete name(s) of the author(s) must be written, with their basic biographical data: undergraduate degree, graduate degree, occupation or position, institutional affiliation (institution where they work), dependency, city, country and e-mail. The above information must be immediately below the author's name.

Abstract

The scope and purpose of the work must be established giving a clear and concise description of the methodology, results presented and the conclusions obtained. Maximum of 250 words.

Keywords

Between three and ten keywords must be chosen, written in English with *Times New Roman* letter in bold and italic.

Key words must be written in alphabetic order and must be as standard as possible, for which it is suggested the use of international databases according to the area of knowledge. For example, in the area of Electrics and Electronics it is suggested to use the IEEE thesaurus and World Bank thesaurus that can be accessed at the following web pages respectively: http://www.ieee.org/documents/2009Taxonomy_v101.pdf, http://multites.net/mtsql/wb/site/default.asp

Abstract in Spanish

Translation to the Spanish language of the text that appears in the abstract, it must be correct and precise.

Keywords in Spanish

Translation to the English language of the keywords in Spanish, they must be correct and precise.

Keywords must be written in the order of the English version and must be as standard as possible, for which it is suggested the use of international databases according to the area of knowledge. For example, in the area of Electrics and Electronics it is suggested to use the UNESCO thesaurus that can be found at the following web pages: http://databases.unesco.org/thessp

Introduction

The general idea of the work must be described, its context, backgrounds, state of the art of the topic, objectives and possible scope of the work.

Methodology

The writing of this part must allow any specialized professional in the topic to replicate the research.

Results

Explanation and interpretation of the findings. If necessary, a brief discussion focused on the interpretation of the results can be presented.

Conclusions

Implication of the results and their relation to the proposed objective.

Financing

Mention the associated research from which the article was derived and the entity that endorsed and financed the research.

Acknowledgments

They should preferably be brief and include the essential contributions for the development of the paper.

Equations

Equations must appear centered with respect to the main text. They must be referenced with consecutive numbers (written in parenthesis close to the right margin). Equations are cited in the main text employing the word equation, and followed by the number in parenthesis. Equations must be made in an appropriate equation editor and compatible with "InDesign" software, as for example the equation editor of Windows.

Tables

In the case of implementation of tables, it is recommended that these are not inserted as images, considering that in that format they cannot be modified. The title of each table must include the word table (in italic) followed by the corresponding consecutive number and a brief name of the table. The heading must be written in TNR letter, italic and font size 9.

Charts are not presented but tables and they should be automatically raised from the text processor. Tables should be named and referenced in the article, in strict order. Every table must have at the bottom the source from which it was taken, or to mention self-authorship if it is the case.

Figures

All the figures or pictures have to be sent in JPG or PNG format with a minimum resolution of 300 DPI, adapted to gray scale.

The footnote or name of each figure must include the word figure (in italic) followed by the corresponding consecutive number and a brief description of the content of the figure. The footnote of the figure must be written in Times New Roman letter, italic and font size 9. Figures must be named and referenced in the article, in strict order. Every figure must have at the bottom the source from which it was taken, or to mention self-authorship if it is the case.

Symbols

The symbols of the constants, variables and functions in Latin or Greek letters –included in the equations- must be in italic; the mathematical symbols and the numbers do not go in italic. The symbols must be identified immediately after the equation. Units, dimensions and symbols of the international system must be used.

When using acronyms or abbreviations, the complete equivalence should be written first, followed by the corresponding acronym or abbreviation in parenthesis and from there it is only written the respective acronym or abbreviation.

Bibliographic references

All bibliographic references cited in the text must be listed in the References section. Citations must follow the IEEE (Institute of Electrical and Electronics Engineers) format.

You may consult the materials provided by the Francisco José de Caldas District University Library System or the official IEEE documentation.

ARTICLE SUBMISSION

Authors must submit their articles through the application Open Journal System in digital format, attaching the cover letter and the article-authors format.

Cover letter

The article must be submitted with a cover letter addressed to the director and editor of the journal, Engineer Lely Adriana Luengas Contreras, including:

- Specific request to consider your article to be published in Tecnura journal.
- Full title of the article.
- Full names of all the authors of the paper.
- Certification of the originality and unpublished character of the paper.
- Exclusivity of submission to Tecnura journal.
- Authoring confirmation with signature of all the authors.

This letter must be signed by all the authors, scanned and sent with the remaining requested documents.

Article-authors information format

The article has to be submitted with an information format about the article and its authors which can be downloaded from the web page of Tecnura journal http://revistas.udistrital.edu.co/ojs/index.php/Tecnura/index, in the section “Forms and Documents”. It is important to complete all the fields of information requested, some of them have comments to clarify better what is being requested. The format must not be scanned.

Article

Article in digital format (Word 2003 and later editions) that complies with all the presentation rules described in chapter three, "Article structure", of this guide of instructions for authors.

PUBLICATION PROCEDURE

The procedure to be followed by Tecnura journal for the evaluation and possible publication of the papers sent by the authors is the following in chronological order:

1. Delivery of the article with the cover letter and the information format by the authors.
2. Notification to the author about the reception of the article.
3. Verification of the presentation rules by the monitor of the journal.
4. Notification to the author about the evaluation of the presentation rules.
5. Submission of corrections made by the authors related to the evaluation of presentation rules.
6. Submission of the articles to the selected arbitrators.
7. Notification of the beginning of the arbitration process of the article.
8. Notification to the authors about the decision made by the editorial committee, and about the evaluations made by the arbitrators.
9. Delivery of the corrections made by the authors with respect to the evaluations made by the arbitrators.
10. Study of the final version of the article and the evaluations of the arbitrators by the editorial committee.
11. Delivery by the authors of the letter that surrenders right to the editor of the journal.
12. Submission of the version with style corrections and diagramed to the authors.
13. Verification of errors and final approval of the version with style corrections and diagrammed by the authors.
14. Publication of the article in the corresponding number of Tecnura journal.
15. Notification to the authors of the number of interest.
16. Delivery of a copy of the journal to each one of the authors of the published article.

ARTICLE ARBITARION PROCESS

Considering the quarterly periodicity of the journal, the Editorial Committee makes four calls every year for the submission of articles, approximately in the months of February, May, August and November. The articles will be received until the date established in the call.

Once received the articles, the monitor of the journal will make an initial form evaluation to verify the completion of the elements mentioned in this guide of instructions to authors. After receiving again the article with the requested corrections by the journal's monitor, the paper will be submitted to evaluation by three academic peers (through time it is expected to include more external peers to participate in the process).

Each article sent to Tecnura journal is checked by two expert academic peers external to the institution of the authors, by a process of "*Peer-review*" of double blind, guaranteeing the anonymity of authors and evaluators; every paper sent is considered confidential and so it is demanded to evaluators.

Possible conclusions of the result of the evaluation by the judges are only three: publish the article without modifications, publish the article with modifications and not publish the article.

Subsequently, the Editorial Committee takes the decision to publish or not the articles, based on the results of the evaluations made by the assigned arbitrators. In case of contradictions in the evaluations with respect to the publication of an article, the editorial committee will send the article to a third peer and will be inclined for the two evaluations that have the same concept with respect to the publication of the article.

In each call the main author must suggest at least four possible external arbitrators to his work institution evaluators, who must be specialists in the specific topic of the article sent and must have at least Masters level, and at least two must to be international. Potential evaluators can belong to a university or industry, public or private; their complete names must be provided, highest academic formation, institutional affiliation and e-mail. The editorial committee will analyze these four potential evaluators in order to enrich the database of arbitrators of Tecnura journal.

The Editorial Committee of Tecnura journal reserves the right to print, reproduce total or partially the article, as the right to accept or reject it. In the same way, it has the right to make any editorial modification that considers necessary; in this case the author will receive written recommendations from the evaluators. If accepted, authors must deliver the article with the suggested adjustments within the dates given by the journal to guarantee its publication in the programmed number.

CONTACT

For any additional information request, please send an e-mail to Tecnura journal tecnura@udistrital.edu.co, tecnura@gmail.com or by mail to Lely Adriana Luengas Contreras, Director and Publisher of Tecnura Journal, to the following address:

Tecnura Journal
Journals Room, Block 5, Office 305. Faculty of Technology
Universidad Distrital Francisco José de Caldas Transversal 70 B N. 73 a 35 sur
Phone: 571–3239300 Extension: 5003
Mobile: 57–3153614852
Bogotá D.C., Colombia
Email: tecnura.ud@correo.udistrital.edu.co, tecnura@gmail.com
Web page: https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/index