Scientia Iter
ISSN:3072-9793

Volumen 2 Número: 1 Año: 2026

Gestión de calidad y seguridad informática en el desarrollo de software sostenible: un enfoque basado en la disponibilidad del sistema

Quality management and information security in sustainable software development: a system availability-based approach

Autor(es)

Ricardo M. Candanedo Yau[1*] https://orcid.org/0009-0002-5017-9830

[1] Universidad de Panamá. Panamá.

* Autor para correspondencia: ricardo.candanedo@up.c.pa

RESUMEN

La creciente dependencia de los sistemas de información en los procesos organizacionales ha convertido la gestión de la calidad y la seguridad informática en factores críticos para el desarrollo de software sostenible. En este contexto, la disponibilidad del sistema se posiciona como un atributo esencial, ya que garantiza la continuidad operativa, la confianza de los usuarios y la resiliencia tecnológica frente a fallos, amenazas y cambios del entorno. La problemática que aborda esta investigación radica en la insuficiente integración de prácticas sistemáticas de calidad y seguridad informática durante el ciclo de vida del software, lo cual afecta directamente la disponibilidad y sostenibilidad de los sistemas desarrollados. El objetivo general del estudio es analizar la gestión de la calidad y la seguridad informática en el desarrollo de software sostenible, con énfasis en su impacto sobre la disponibilidad del sistema. La metodología empleada corresponde a un enfoque cualitativo de tipo descriptivo y analítico, basado en la revisión sistemática de literatura científica, normas internacionales y modelos de buenas prácticas aplicables al desarrollo de software. Los principales resultados evidencian que la incorporación temprana de estrategias de gestión de la calidad, junto con controles de seguridad informática alineados a estándares reconocidos, contribuye significativamente a mejorar la disponibilidad del sistema y a fortalecer la sostenibilidad del software en el tiempo. Asimismo, se concluye que un enfoque integrado permite reducir riesgos operativos, optimizar recursos y promover el desarrollo de soluciones tecnológicas más confiables y sostenibles.

Palabras clave: Desarrollo de software, disponibilidad, gestión de la calidad, seguridad informática, sistemas de información, sostenibilidad

ABSTRACT

The increasing reliance on information systems in organizational processes has made quality management and information security critical factors for sustainable software development. In this context, system availability emerges as an essential attribute, as it ensures operational continuity, user trust and technological resilience in the face of failures, threats and environmental changes. The problem addressed in this research lies in the insufficient integration of systematic quality and information security practices throughout the software life cycle, which directly affects system availability and sustainability. The main objective of this study is to analyze quality management and

information security in sustainable software development, with an emphasis on their impact on system availability. The methodology follows a qualitative, descriptive and analytical approach, based on a systematic review of scientific literature, international standards and best practice models applicable to software development. The main results show that the early incorporation of quality management strategies, together with information security controls aligned with recognized standards, significantly improves system availability and strengthens software sustainability over time. It is concluded that an integrated approach reduces operational risks, optimizes resources and promotes the development of more reliable and sustainable technological solutions.

Keywords: *Availability, information security, information systems, quality management, software development, sustainability*

Fecha de Recibido: 26/12/2025

Fecha de Aceptado: 05/01/2026

INTRODUCCIÓN

En las últimas décadas, el desarrollo de software ha experimentado una evolución acelerada impulsada por el crecimiento de las tecnologías de la información y la comunicación, la digitalización de los procesos organizacionales y la creciente demanda de soluciones tecnológicas confiables, seguras y sostenibles. En este contexto, los sistemas de información se han consolidado como infraestructuras críticas para el funcionamiento de organizaciones públicas y privadas, incidiendo de manera directa en la productividad, la competitividad y la toma de decisiones estratégicas. Esta centralidad del software en los entornos organizacionales ha evidenciado la necesidad de garantizar no solo su funcionamiento técnico, sino también niveles adecuados y sostenidos de calidad, seguridad y disponibilidad, entendidos como factores esenciales para la continuidad operativa y la sostenibilidad de los sistemas (Venters et al., 2020; Lago et al., 2021).

La gestión de la calidad en el desarrollo de software se ha establecido como un enfoque fundamental para asegurar que los productos tecnológicos cumplan con requisitos funcionales, técnicos y organizacionales, al tiempo que satisfacen las expectativas de los usuarios y de las partes interesadas. Investigaciones recientes destacan que la incorporación de tecnologías emergentes y sistemas digitales avanzados exige la adaptación de los sistemas de gestión de la calidad a entornos cada vez más complejos y dinámicos, en los que la variabilidad tecnológica y organizacional demanda enfoques flexibles y sistemáticos de gestión (Cao & Alyousuf, 2025).

Tradicionalmente, la calidad del software se ha asociado a atributos como funcionalidad, fiabilidad, usabilidad y mantenibilidad; sin embargo, en entornos digitales caracterizados por la interdependencia

de los sistemas y la exposición a riesgos crecientes, la calidad no puede concebirse de manera aislada de otros factores críticos, particularmente la seguridad informática y la disponibilidad del sistema. La falta de una gestión integrada de estos elementos incrementa la probabilidad de fallos, interrupciones del servicio y vulnerabilidades que afectan la continuidad operativa y comprometen la sostenibilidad del software en el tiempo (ISO, 2023; Wiesner et al., 2022; Shams & Petersen, 2021).

De forma paralela, la seguridad informática ha adquirido una relevancia estratégica debido al aumento sostenido de amenazas digitales, ataques cibernéticos y riesgos asociados a la integridad, confidencialidad y disponibilidad de la información. Las organizaciones enfrentan desafíos constantes para proteger sus sistemas frente a incidentes que pueden comprometer datos sensibles, deteriorar la confianza de los usuarios y generar impactos económicos y reputacionales significativos. En este escenario, la seguridad informática trasciende su dimensión puramente técnica y se consolida como un eje transversal de la gestión organizacional y del desarrollo de software, requiriendo una planificación sistemática y su integración coherente con los procesos de gestión de la calidad (Rashid et al., 2022; Seacord et al., 2020; Tøndel et al., 2021).

Dentro de los principios fundamentales de la seguridad informática, la disponibilidad del sistema ocupa un lugar central, al referirse a la capacidad de los sistemas de información para permanecer accesibles y operativos cuando son requeridos. La indisponibilidad de un sistema, ya sea por fallos técnicos, deficiencias de diseño, mantenimiento inadecuado o ataques informáticos, puede generar consecuencias significativas sobre los procesos organizacionales, afectando la prestación de servicios y comprometiendo la sostenibilidad de las soluciones tecnológicas. En este sentido, diversos estudios coinciden en que la disponibilidad debe concebirse como un objetivo estratégico que debe ser gestionado de manera proactiva desde las etapas iniciales del ciclo de vida del software y no únicamente como un resultado de la fase operativa (Zhang et al., 2023; Shams & Petersen, 2021).

El concepto de desarrollo de software sostenible surge como respuesta a la necesidad de crear sistemas que no solo sean funcionales y seguros en el corto plazo, sino que puedan mantenerse, evolucionar y adaptarse a lo largo del tiempo sin un consumo excesivo de recursos ni una degradación progresiva de su calidad. La sostenibilidad del software implica la integración de factores técnicos, organizacionales y humanos, así como la adopción de prácticas de gestión de la calidad y la seguridad informática que favorezcan la estabilidad, la escalabilidad y la resiliencia del sistema. Desde esta perspectiva, la disponibilidad del sistema se configura como un indicador clave de sostenibilidad, al reflejar la capacidad del software para responder de forma continua y eficaz a las demandas del entorno (Calero & Piattini, 2021; Penzenstadler et al., 2020; Alami et al., 2024).

A pesar del amplio desarrollo teórico y normativo en torno a la gestión de la calidad y la seguridad informática, en la práctica persiste una brecha significativa entre estos enfoques y su aplicación efectiva

en el desarrollo de software. Diversas investigaciones señalan que numerosas organizaciones continúan adoptando estrategias fragmentadas, en las que la calidad y la seguridad se gestionan de forma independiente o se incorporan de manera tardía, lo que limita su impacto positivo sobre la disponibilidad del sistema y la sostenibilidad del software. Esta situación pone de manifiesto una problemática relevante asociada a la ausencia de enfoques integrados que articulen de manera coherente la gestión de la calidad, la seguridad informática y los objetivos de sostenibilidad (Condori-Fernandez et al., 2021; Blandón-Jaramillo & Jaramillo-Becerra, 2023).

En este contexto, surge la necesidad de profundizar en el análisis de cómo la gestión de la calidad y la seguridad informática puede contribuir de manera efectiva al desarrollo de software sostenible, particularmente desde la perspectiva de la disponibilidad del sistema. A partir de esta necesidad, la presente investigación se articula en torno a la siguiente pregunta central: ¿cómo se gestiona la calidad y la seguridad informática en el desarrollo de software sostenible y de qué manera dicha gestión incide en la disponibilidad del sistema? De esta interrogante se derivan preguntas complementarias orientadas a identificar las prácticas más relevantes de gestión, los factores que influyen en la disponibilidad del sistema y el papel que desempeña la integración de estas dimensiones en el fortalecimiento de la sostenibilidad del software (Noman et al., 2024).

En coherencia con las preguntas planteadas, el objetivo general del estudio es analizar la gestión de la calidad y la seguridad informática en el desarrollo de software sostenible, con énfasis en su impacto sobre la disponibilidad del sistema. Para ello, se busca examinar los principales enfoques teóricos y normativos relacionados con la calidad y la seguridad informática, analizar los factores que condicionan la disponibilidad del sistema en los procesos de desarrollo de software y comprender cómo la integración de estas prácticas contribuye a la sostenibilidad del software a largo plazo (ISO, 2022; ISO, 2023).

La relevancia de esta investigación radica en su contribución al fortalecimiento del conocimiento científico en el ámbito de la ingeniería de software y los sistemas de información, al ofrecer una visión integral sobre la gestión de la calidad y la seguridad informática como elementos estratégicos para la disponibilidad del sistema. Asimismo, el estudio aporta implicaciones prácticas para las organizaciones, al proporcionar fundamentos que pueden orientar la toma de decisiones, la formulación de políticas y la implementación de estrategias orientadas al desarrollo de software sostenible en entornos digitales complejos y dinámicos (Behl et al., 2023; Sarker & Nihat, 2025). En este sentido, la investigación se posiciona como un aporte relevante para académicos, profesionales y gestores interesados en el diseño y la gestión de sistemas de información confiables, seguros y sostenibles en un contexto tecnológico en constante transformación.

MÉTODO

La presente investigación se desarrolló bajo un enfoque metodológico cualitativo, de carácter descriptivo y analítico, orientado a examinar de manera integral la gestión de la calidad y la seguridad informática en el desarrollo de software sostenible, con énfasis en su incidencia en la disponibilidad del sistema. Este enfoque resulta adecuado para el objeto de estudio, ya que permite una comprensión profunda de los conceptos, modelos, enfoques teóricos y marcos normativos que sustentan las prácticas actuales en el ámbito del desarrollo de software y los sistemas de información (Martínez-Fernández et al., 2021).

El diseño de la investigación se fundamentó en el análisis documental y en la revisión sistemática de literatura científica especializada, lo que posibilitó identificar, comparar y sintetizar aportes teóricos y empíricos relevantes relacionados con la gestión de la calidad, la seguridad informática, el desarrollo de software sostenible y la disponibilidad del sistema. Este tipo de diseño ha sido ampliamente empleado en estudios orientados a la construcción de marcos conceptuales y analíticos en ingeniería de software, debido a su capacidad para integrar evidencia procedente de múltiples fuentes y contextos organizacionales y tecnológicos (Condori-Fernandez et al., 2021; Gómez et al., 2025).

Como materiales principales de la investigación se utilizaron artículos científicos publicados en revistas indexadas, normas internacionales, informes técnicos y documentos institucionales vinculados con la ingeniería de software, la gestión de la calidad y la seguridad informática. Esta selección se alinea con revisiones recientes que analizan de manera sistemática la relación entre tecnologías de la información, sostenibilidad e ingeniería de software, subrayando la importancia de integrar criterios de eficiencia y sostenibilidad en los procesos de desarrollo de software (Gómez et al., 2025). Las fuentes documentales fueron identificadas a partir de bases de datos académicas reconocidas, como Scopus, Web of Science, IEEE Xplore y ScienceDirect, priorizando publicaciones recientes, de alto impacto y estándares vigentes aplicables al desarrollo de software (ISO, 2022; ISO, 2023).

El proceso de búsqueda de información se realizó mediante el uso de palabras clave y descriptores asociados a los ejes temáticos de la investigación, tanto en idioma español como en inglés, asegurando la correspondencia terminológica con el Tesauro de la UNESCO. Esta estrategia permitió ampliar el alcance de la revisión e incorporar estudios relevantes a nivel internacional sobre calidad del software, seguridad informática, disponibilidad del sistema y sostenibilidad (Sriraman & Raghunathan, 2023). Los criterios de inclusión contemplaron documentos que abordaran de manera explícita dichos ejes, mientras que se excluyeron aquellos trabajos sin relación directa con el objeto de estudio o que carecieran de rigor académico.

Una vez recopilada la información, se llevó a cabo un proceso sistemático de organización y análisis de los documentos seleccionados. Esta etapa incluyó una lectura exhaustiva y crítica de las fuentes, orientada a identificar conceptos clave, enfoques metodológicos, modelos de gestión y hallazgos relevantes. El análisis se desarrolló mediante técnicas de análisis de contenido cualitativo, lo que permitió categorizar la información en función de los principales ejes temáticos del estudio y establecer relaciones conceptuales entre la gestión de la calidad, la seguridad informática, la disponibilidad del sistema y el desarrollo de software sostenible (Qiang et al., 2024).

Con el fin de fortalecer la consistencia metodológica del estudio, se aplicó un proceso de triangulación teórica, contrastando las distintas perspectivas propuestas por autores y organismos internacionales. Esta triangulación contribuyó a reducir sesgos interpretativos y a consolidar una visión integral del fenómeno analizado, facilitando la identificación de convergencias, divergencias y vacíos en la literatura existente (Lago et al., 2021; Venters et al., 2020). Asimismo, se consideraron modelos y estándares internacionales ampliamente reconocidos en el ámbito de la calidad y la seguridad informática como referentes conceptuales para el análisis y la discusión de los resultados (ISO, 2022; ISO, 2023).

El análisis de la disponibilidad del sistema se abordó desde una perspectiva cualitativa, considerando su relación con las prácticas de gestión de la calidad y la seguridad informática a lo largo del ciclo de vida del software. Se examinó cómo las decisiones adoptadas durante las fases de planificación, diseño, implementación, pruebas, mantenimiento y mejora continua influyen en la capacidad del sistema para mantenerse operativo y accesible de manera sostenida (Zhang et al., 2023). Este enfoque permitió comprender la disponibilidad no solo como un atributo técnico, sino como el resultado de decisiones estratégicas y de gestión adoptadas durante el desarrollo del software.

La validez y la confiabilidad del estudio se garantizaron mediante la selección rigurosa de las fuentes, la aplicación sistemática de los criterios de inclusión y exclusión, y la coherencia entre los objetivos de la investigación, las preguntas planteadas y la metodología empleada. El uso de literatura científica reconocida y de estándares internacionales contribuyó a reforzar la credibilidad y solidez del análisis realizado (Noman et al., 2024; Wiesner et al., 2022).

Desde el punto de vista ético, la investigación respetó los principios de integridad académica, asegurando la correcta citación de todas las fuentes utilizadas y evitando cualquier forma de plagio o uso indebido de la información. Al tratarse de un estudio de carácter documental, no se requirió la participación directa de sujetos humanos ni la recolección de datos sensibles, lo que garantiza el cumplimiento de las normas éticas de la investigación científica.

En síntesis, los materiales y métodos empleados permitieron desarrollar un análisis riguroso y coherente de la gestión de la calidad y la seguridad informática en el desarrollo de software sostenible, proporcionando una base metodológica sólida para la interpretación de los resultados y la formulación

de conclusiones fundamentadas. Esta metodología resulta pertinente para aportar conocimiento científico relevante y para orientar futuras investigaciones y aplicaciones prácticas en el ámbito del desarrollo de software y los sistemas de información.

RESULTADOS

Los resultados de la presente investigación se derivan del análisis sistemático de la literatura científica, normativa y técnica relacionada con la gestión de la calidad, la seguridad informática, el desarrollo de software sostenible y la disponibilidad del sistema. A partir del proceso metodológico desarrollado, fue posible identificar patrones conceptuales, enfoques recurrentes y relaciones significativas entre los ejes analizados, lo que permitió estructurar los hallazgos de manera coherente en función de los objetivos del estudio.

En primer lugar, el análisis de las fuentes documentales permitió caracterizar los enfoques predominantes de gestión de la calidad y la seguridad informática en el desarrollo de software. Los resultados evidencian una tendencia progresiva hacia modelos de gestión integrados; sin embargo, también se observa la persistencia de aproximaciones fragmentadas que limitan su impacto sobre la disponibilidad del sistema. La tabla 1 sintetiza los enfoques identificados en la literatura analizada, considerando su nivel de integración y su relación con la disponibilidad del sistema.

Tabla 1. Enfoques de gestión de la calidad y seguridad informática identificados en la literatura

Enfoque identificado	**Dimensión de calidad**	**Dimensión de seguridad informática**	**Relación con la disponibilidad del sistema**	**Nivel de integración**
Enfoque tradicional	Parcial	Reactiva	Baja	Bajo
Enfoque normativo	Estandarizada	Preventiva	Media	Medio
Enfoque integrado	Sistémica	Proactiva	Alta	Alto

Fuente o Nota:

La clasificación se realizó a partir del análisis de contenido cualitativo de las fuentes revisadas.

Elaboración propia a partir de la revisión documental.

Los resultados muestran que los enfoques integrados presentan una relación más consistente con la disponibilidad del sistema, lo que refuerza la importancia de adoptar modelos sistémicos en el desarrollo de software sostenible y de superar enfoques parciales o reactivos.

En un segundo momento, se analizaron los factores metodológicos que influyen en la disponibilidad del sistema a lo largo del ciclo de vida del software. Este análisis permitió identificar cómo las decisiones adoptadas en cada fase condicionan de manera directa o indirecta la sostenibilidad del sistema. La tabla 2 presenta una síntesis de los factores identificados y su incidencia en la disponibilidad.

Tabla 2. Factores metodológicos que influyen en la disponibilidad del sistema

Fase del ciclo de vida	Factor identificado	Impacto en la disponibilidad	Relación con calidad	Relación con seguridad
Análisis y diseño	Definición de requisitos	Alto	Alta	Media
Desarrollo	Control de procesos	Medio	Alta	Media
Pruebas	Verificación sistemática	Alto	Alta	Alta
Mantenimiento	Gestión de cambios	Alto	Media	Alta

Fuente o Nota:

Los factores fueron categorizados según su recurrencia y relevancia en la literatura analizada.

Elaboración propia con base en fuentes académicas y normativas.

Los resultados evidencian que la disponibilidad del sistema se configura de manera progresiva desde las fases iniciales del desarrollo, lo que confirma que no depende exclusivamente de la etapa operativa, sino de una gestión anticipada y coherente de la calidad y la seguridad informática.

Asimismo, el análisis documental permitió identificar los principales estándares y modelos utilizados como referentes metodológicos para garantizar la calidad, la seguridad informática y la disponibilidad del sistema. La tabla 3 resume los estándares más citados en la literatura y su aporte al desarrollo de software sostenible.

Tabla 3. Estándares y modelos relevantes para la gestión de calidad y seguridad informática

Estándar o modelo	Enfoque principal	Aporte a la calidad	Aporte a la seguridad	Contribución a la disponibilidad
ISO 9001	Gestión de calidad	Alta	Indirecta	Media
ISO/IEC 27001	Seguridad informática	Indirecta	Alta	Alta
ISO/IEC 25010	Calidad del software	Alta	Media	Alta
ITIL	Gestión de servicios	Media	Media	Alta

Fuente o Nota:

Los aportes se determinaron a partir del análisis cualitativo del contenido normativo.

Elaboración propia basada en normas internacionales.

Los resultados ponen de manifiesto que la aplicación complementaria de estándares de calidad y seguridad informática fortalece la disponibilidad del sistema, especialmente cuando se integran dentro de un enfoque metodológico orientado a la sostenibilidad del software.

Por otra parte, se identificaron prácticas de gestión recurrentes asociadas al desarrollo de software sostenible y a su impacto sobre la disponibilidad del sistema. Estas prácticas emergen como resultados directos de la integración metodológica analizada. La tabla 4 presenta dichas prácticas y su relación con los objetivos del estudio.

Tabla 4. Prácticas de gestión asociadas al desarrollo de software sostenible

Práctica de gestión	**Dimensión principal**	**Impacto en sostenibilidad**	**Impacto en disponibilidad**
Gestión de riesgos	Seguridad	Alto	Alto
Mejora continua	Calidad	Alto	Medio
Monitoreo del sistema	Seguridad	Medio	Alto
Documentación técnica	Calidad	Medio	Medio

Fuente o Nota:

Las prácticas se agruparon según su contribución a los objetivos de la investigación.

Elaboración propia a partir del análisis de la literatura.

Los hallazgos confirman que las prácticas orientadas a la prevención, el monitoreo y la mejora continua inciden positivamente tanto en la sostenibilidad del software como en la disponibilidad del sistema.

Como resultado integrador del análisis, se establecieron relaciones entre los componentes de calidad, seguridad informática y disponibilidad del sistema, permitiendo visualizar su contribución conjunta al desarrollo de software sostenible. La tabla 5 sintetiza dichas relaciones.

Tabla 5. Relación entre calidad, seguridad informática y disponibilidad del sistema

Componente	**Rol en el desarrollo de software**	**Relación con sostenibilidad**	**Resultado metodológico**
Calidad	Optimización de procesos	Alta	Reducción de fallos
Seguridad informática	Protección del sistema	Alta	Continuidad operativa
Disponibilidad	Accesibilidad y operación continua	Muy alta	Software sostenible

Fuente o Nota:

La relación se estableció a partir de la triangulación teórica de los hallazgos. Elaboración propia.

Los resultados indican que la disponibilidad del sistema actúa como un elemento articulador entre la gestión de la calidad y la seguridad informática, consolidándose como un indicador central del desarrollo de software sostenible.

De manera complementaria, el análisis permitió identificar debilidades recurrentes en la gestión de la calidad y la seguridad informática que afectan directamente la disponibilidad del sistema y la sostenibilidad del software. Estas debilidades se presentan de forma reiterada en la literatura revisada. La tabla 6 sintetiza los principales hallazgos.

Tabla 6. Debilidades identificadas en la gestión de calidad y seguridad informática

Debilidad identificada	**Dimensión afectada**	**Consecuencia principal**	**Impacto en la disponibilidad**	**Implicación para la sostenibilidad**
Gestión fragmentada	Calidad y seguridad	Falta de coherencia	Alto	Software poco sostenible
Seguridad reactiva	Seguridad informática	Respuesta tardía	Alto	Riesgo operativo elevado
Escasa documentación	Calidad	Pérdida de conocimiento	Medio	Dificultad de mantenimiento
Ausencia de monitoreo continuo	Seguridad	Fallos no detectados	Alto	Interrupciones frecuentes

Fuente o Nota:

Las debilidades se identificaron mediante análisis de recurrencia y convergencia temática en las fuentes revisadas. Elaboración propia a partir de la revisión documental.

Estos resultados evidencian que las principales limitaciones no se originan exclusivamente en aspectos técnicos, sino en deficiencias de gestión y planificación metodológica, lo que refuerza la necesidad de adoptar enfoques integrados.

Finalmente, se identificaron beneficios metodológicos derivados de la implementación integrada de la gestión de la calidad y la seguridad informática en el desarrollo de software sostenible. La tabla 7 presenta dichos beneficios y su contribución a la disponibilidad del sistema.

Tabla 7. Beneficios metodológicos de la gestión integrada de calidad y seguridad informática

Beneficio identificado	**Enfoque metodológico**	**Efecto en la calidad**	**Efecto en la seguridad**	**Resultado en la disponibilidad**
Reducción de fallos	Preventivo	Alto	Medio	Alta
Continuidad operativa	Sistémico	Medio	Alto	Muy alta
Optimización de recursos	Estratégico	Alto	Alto	Alta

Beneficio identificado	Enfoque metodológico	Efecto en la calidad	Efecto en la seguridad	Resultado en la disponibilidad
Mejora de la sostenibilidad	Integral	Alto	Alto	Muy alta

Fuente o Nota:

Los beneficios se determinaron a partir de la triangulación teórica de los hallazgos. Elaboración propia.

En conjunto, los resultados obtenidos evidencian que una gestión integrada de la calidad y la seguridad informática, alineada con estándares internacionales y aplicada de manera sistemática, contribuye de forma significativa a mejorar la disponibilidad del sistema y a fortalecer la sostenibilidad del software. Estos hallazgos proporcionan una base sólida para la discusión teórica y la formulación de conclusiones, así como para futuras investigaciones orientadas a la optimización de los procesos de desarrollo de software.

DISCUSIÓN

El análisis de los resultados obtenidos en la presente investigación permite profundizar en la comprensión de la gestión de la calidad y la seguridad informática como pilares fundamentales del desarrollo de software sostenible, evidenciando que la disponibilidad del sistema actúa como un elemento transversal que articula ambas dimensiones. Desde una perspectiva interpretativa, los hallazgos confirman que la sostenibilidad del software no puede concebirse únicamente como la permanencia funcional del sistema, sino como el resultado de una gestión integrada que combina prácticas de calidad, estrategias de seguridad informática y decisiones metodológicas adoptadas a lo largo de todo el ciclo de vida del software, tal como lo plantean Venters et al. (2020) y Lago et al. (2021).

Los resultados ponen de manifiesto que los enfoques fragmentados de gestión de la calidad y la seguridad informática continúan presentes en diversos contextos organizacionales, lo que limita la efectividad de las acciones orientadas a garantizar la disponibilidad del sistema. Esta fragmentación se evidencia cuando las prácticas de calidad se restringen al cumplimiento de requisitos funcionales, mientras que la seguridad informática se aborda de forma reactiva, generalmente tras la ocurrencia de incidentes o fallos. Esta separación conceptual y operativa reduce la capacidad del sistema para responder de manera continua y confiable a las exigencias del entorno, afectando directamente su sostenibilidad, en concordancia con lo señalado por Rashid et al. (2022) y Seacord et al. (2020) respecto a los riesgos asociados al ciclo de vida del software.

En contraste, los resultados del estudio evidencian que la adopción de enfoques integrados de gestión favorece una visión sistémica del desarrollo de software, en la que la calidad y la seguridad informática

se conciben como componentes interdependientes. Esta integración permite anticipar riesgos, fortalecer la planificación de los procesos y mejorar la disponibilidad del sistema desde las etapas iniciales del desarrollo. En este sentido, la disponibilidad no se interpreta como un atributo aislado, sino como un indicador del nivel de madurez alcanzado en la gestión de la calidad y la seguridad informática, lo cual coincide con los planteamientos de Penzenstadler et al. (2020) y Martínez-Fernández et al. (2021) sobre modelos holísticos en la ingeniería de software sostenible.

Otro aspecto relevante derivado del análisis es la comprensión de la disponibilidad del sistema como un resultado que se construye de manera progresiva a lo largo del ciclo de vida del software. Las decisiones adoptadas durante las fases de análisis y diseño, la implementación de controles durante el desarrollo, la rigurosidad de las pruebas y la eficacia de la gestión del mantenimiento influyen directamente en la capacidad del sistema para mantenerse operativo y accesible de forma sostenida. Esta interpretación amplía la concepción tradicional de la disponibilidad, superando un enfoque exclusivamente técnico y reconociéndola como una consecuencia acumulativa de prácticas metodológicas coherentes, tal como lo señalan Shams y Petersen (2021) y Zhang et al. (2023).

Desde la perspectiva de la sostenibilidad del software, los resultados indican que la gestión de la calidad contribuye a la reducción de errores, a la estandarización de procesos y a la mejora continua, mientras que la seguridad informática aporta mecanismos de protección que fortalecen la continuidad operativa y la resiliencia del sistema. La interacción entre ambas dimensiones genera un efecto sinérgico que se traduce en una mayor disponibilidad del sistema y en una optimización del uso de recursos, lo que coincide con los planteamientos de Calero y Piattini (2021) y Alami et al. (2024). Estos hallazgos son consistentes con revisiones conceptuales recientes que destacan que el desarrollo de software sostenible requiere la integración explícita de calidad, seguridad y gestión organizacional para garantizar resultados duraderos en el tiempo (Kamboj, 2025).

Asimismo, los resultados evidencian que la aplicación aislada de estándares o modelos normativos resulta insuficiente para garantizar la sostenibilidad del software si estos no se integran dentro de una estrategia común orientada a la disponibilidad del sistema. Los estándares de calidad y seguridad informática adquieren mayor efectividad cuando se aplican de manera complementaria, permitiendo alinear los procesos de desarrollo con objetivos estratégicos de continuidad, confiabilidad y adaptación al cambio, tal como lo plantean las normas ISO (2022; 2023). En este contexto, la disponibilidad del sistema emerge como un criterio integrador para evaluar la efectividad de la implementación normativa, en concordancia con los aportes de Nurbojatmiko et al. (2025).

En relación con las prácticas de gestión identificadas, los hallazgos permiten interpretar que aquellas orientadas a la prevención, el monitoreo continuo y la mejora sistemática generan impactos positivos sostenidos en la disponibilidad del sistema. Estas prácticas favorecen la detección temprana de fallos, la

gestión eficiente de cambios y la conservación del conocimiento técnico, aspectos esenciales para la sostenibilidad del software, como lo señalan Noman et al. (2024) y Wiesner et al. (2022). En contraste, la ausencia de estos enfoques se asocia con mayores niveles de riesgo operativo, interrupciones frecuentes y dificultades para el mantenimiento evolutivo del sistema.

De manera complementaria, los resultados muestran que las principales debilidades que afectan la disponibilidad del sistema no se originan exclusivamente en limitaciones tecnológicas, sino en deficiencias de gestión y planificación. La fragmentación de procesos, la falta de coordinación entre calidad y seguridad informática y la ausencia de mecanismos de seguimiento continuo emergen como factores críticos que comprometen la sostenibilidad del software, reforzando la necesidad de enfoques organizacionales integrados, tal como lo indican Sriraman y Raghunathan (2023).

CONCLUSIONES

En conclusión, el desarrollo de la presente investigación permitió analizar de manera integral la gestión de la calidad y la seguridad informática en el contexto del desarrollo de software sostenible, evidenciando la relevancia de la disponibilidad del sistema como un elemento articulador entre ambas dimensiones. A partir del enfoque cualitativo y del análisis documental realizado, se concluye que la sostenibilidad del software no depende únicamente de su correcto funcionamiento técnico, sino de la adopción de estrategias de gestión coherentes, sistemáticas e integradas que garanticen su continuidad operativa y su capacidad de adaptación a lo largo del tiempo (Venters et al., 2020; Lago et al., 2021).

Se concluye, además, que la gestión de la calidad y la seguridad informática no deben concebirse como procesos independientes, sino como componentes interdependientes que influyen directamente en la disponibilidad del sistema. Los enfoques fragmentados limitan la capacidad del software para mantenerse operativo y confiable, mientras que los enfoques integrados fortalecen la estabilidad del sistema y favorecen su sostenibilidad, consolidando la disponibilidad como un indicador del nivel de madurez del desarrollo de software (ISO, 2023; Wiesner et al., 2022).

Asimismo, se establece que la disponibilidad del sistema es el resultado de decisiones metodológicas adoptadas a lo largo de todo el ciclo de vida del software, desde el análisis y diseño hasta el mantenimiento y la mejora continua. La incorporación temprana de prácticas de calidad y seguridad informática contribuye significativamente a la prevención de fallos, a la reducción de riesgos operativos y a la continuidad del servicio, reforzando la necesidad de enfoques proactivos orientados a la sostenibilidad del software (Shams & Petersen, 2021; Zhang et al., 2023).

Desde una perspectiva estratégica, la seguridad informática se consolida como un factor determinante para garantizar la disponibilidad del sistema y la resiliencia tecnológica. Más allá de la protección de la información, su integración con prácticas de calidad fortalece la capacidad del software para enfrentar amenazas, fallos y cambios del entorno, contribuyendo a su confiabilidad y permanencia en el tiempo (Rashid et al., 2022; Tøndel et al., 2021).

En relación con la gestión de la calidad, se concluye que la estandarización de procesos, la mejora continua y la adecuada documentación técnica son elementos fundamentales para la sostenibilidad del software, ya que optimizan el desempeño del sistema y facilitan su mantenimiento evolutivo y la transferencia de conocimiento, aspectos esenciales para garantizar la disponibilidad del sistema en entornos dinámicos y complejos (Calero & Piattini, 2021; Alami et al., 2024; Yılmaz & Şenvar, 2025).

En términos generales, la investigación confirma que el desarrollo de software sostenible requiere una visión holística que integre aspectos técnicos, organizacionales y de gestión. La disponibilidad del sistema se configura como un criterio central para evaluar la efectividad de la gestión de la calidad y la seguridad informática, aportando un enfoque conceptual que concibe la sostenibilidad del software como un proceso continuo y articulado (Penzenstadler et al., 2020).

Desde una perspectiva académica, el estudio contribuye al fortalecimiento del conocimiento científico al ofrecer un marco analítico que vincula calidad, seguridad informática y disponibilidad del sistema dentro del desarrollo de software sostenible, estableciendo bases conceptuales susceptibles de ser ampliadas y contrastadas en distintos contextos organizacionales y tecnológicos. Desde una perspectiva práctica, los resultados evidencian que las organizaciones que adopten enfoques integrados de gestión de la calidad y la seguridad informática estarán en mejores condiciones para desarrollar software sostenible, reducir riesgos operativos y garantizar la continuidad de sus sistemas de información (Behl et al., 2023; Sarker & Nihat, 2025).

A partir de las conclusiones alcanzadas, se recomienda que las organizaciones incorporen la gestión integrada de la calidad y la seguridad informática como un eje estratégico del desarrollo de software, asegurando su aplicación desde las fases iniciales del ciclo de vida del sistema. Asimismo, se sugiere promover la adopción complementaria de estándares internacionales, alineándolos con objetivos explícitos de disponibilidad y sostenibilidad del software. Para futuras investigaciones, se recomienda profundizar en estudios empíricos que permitan validar los hallazgos en contextos organizacionales específicos y desarrollar métricas que faciliten la evaluación cuantitativa de la disponibilidad del sistema como componente del desarrollo de software sostenible.

REFERENCIAS BIBLIOGRÁFICAS

Alami, A., Pardo, R., & Linåker, J. (2024). Free and open source software communities sustainability: Does it make a difference in software quality? *Journal of Systems and Software*, *210*, 111937. https://doi.org/10.1016/j.jss.2023.111937

Behl, A., Pereira, V., & Clegg, S. (2023). Cybersecurity and digital sustainability: A resource-based view of secure information systems. *Technological Forecasting and Social Change, 186*, 122149. https://doi.org/10.1016/j.techfore.2022.122149

Blandón-Jaramillo, C. A., & Jaramillo-Becerra, J. S. (2023). Calidad del software y seguridad de aplicaciones a partir del proceso de desarrollo de software AGILISO y el estándar OWASP. *Tecnología en Marcha, 36*(8), 5–22. https://doi.org/10.18845/tm.v36i8.6923

Calero, C., & Piattini, M. (2021). Introduction to green and sustainable software. *Journal of Systems and Software*, *174*, 110892. https://doi.org/10.1016/j.jss.2020.110892

Cao, Y., & Alyousuf, F. Q. A. (2025). A framework to assess the impact of emerging IT technologies on quality management systems. *Journal of Big Data, 12*, Article 8. https://doi.org/10.1186/s40537-025-01061-5

Condori-Fernandez, N., Lago, P., & Razavian, M. (2021). A systematic mapping study on sustainability in software engineering. *Journal of Systems and Software, 179*, 111003. https://doi.org/10.1016/j.jss.2021.111003

Gómez, P., Juiz, C., & Freire, P. (2025). Green IT and green software engineering: A systematic literature review. *Journal of Information Systems Engineering and Management, 10*(42s), 811–833. https://doi.org/10.52783/jisem.v10i42s.8195

International Organization for Standardization. (2022). *ISO/IEC 27001:2022—Information security management systems—Requirements*. https://www.iso.org/standard/27001.html

International Organization for Standardization. (2023). *ISO/IEC 25010:2023—Systems and software quality models*. https://www.iso.org/standard/35733.html

Kamboj, A. (2025). Sustainable software development practices: A conceptual and empirical review. *Journal of Software Engineering Research and Development, 13*(1), 1–18. https://doi.org/10.1186/s40411-025-00145-9

Lago, P., Koçak, S. A., Crnkovic, I., & Penzenstadler, B. (2021). Framing sustainability as a property of software quality. *Communications of the ACM, 64*(10), 56–65. https://doi.org/10.1145/3460938

Martínez-Fernández, S., Chatzipetrou, P., Becker, C., & Franch, X. (2021). Sustainability-aware software engineering. *Journal of Systems and Software, 177*, 110955. https://doi.org/10.1016/j.jss.2021.110955

Noman, H., Mahoto, N. A., Bhatti, S., & Rajab, A. (2024). Towards sustainable software systems: A software sustainability analysis framework. *Information and Software Technology, 169*, 107411. https://doi.org/10.1016/j.infsof.2024.107411

Nurbojatmiko, N., Karimiyah, M. S. K., Asnadi, N. M., & Anisyah, R. (2025). ISO 27001 as an information security solution: A systematic literature review. *Sinkron: Jurnal dan Penelitian Teknik Informatika, 9*(1), 484–492. https://doi.org/10.33395/sinkron.v9i1.14448

Penzenstadler, B., Becker, C., Chitchyan, R., Duboc, L., & Mahaux, M. (2020). Software engineering for sustainability: Findings and research directions. *Journal of Systems and Software, 162*, 110517. https://doi.org/10.1016/j.jss.2019.110517

Qiang, Y., Che Pa, N., & Ismail, R. (2024). Sustainable software solutions integrating life cycle analysis and ISO quality models. *International Journal on Advanced Science, Engineering and Information Technology, 14*(5), 1728–1737. https://doi.org/10.18517/ijaseit.14.5.11268

Rashid, A., Chitchyan, R., & Riaz, M. (2022). Managing software security risks throughout the software lifecycle. *IEEE Security & Privacy, 20*(3), 45–53. https://doi.org/10.1109/MSEC.2022.3158054

Sarker, S., & Nihat, M. B. M. (2025). AI-powered quality assurance and risk management in sustainable software ecosystems. *Journal of Software: Evolution and Process, 37*(2), e2541. https://doi.org/10.1002/smr.2541

Seacord, R. C., Plakosh, D., & Lewis, G. A. (2020). Modernizing software security practices. *IEEE Software, 37*(5), 80–87. https://doi.org/10.1109/MS.2020.3003868

Shams, Z., & Petersen, K. (2021). A systematic review of system availability metrics in software-intensive systems. *Empirical Software Engineering, 26*, 1–39. https://doi.org/10.1007/s10664-020-09898-5

Sriraman, G., & Raghunathan, S. (2023). A systems thinking approach to sustainability in software engineering. *Sustainability, 15*(11), 8766. https://doi.org/10.3390/su15118766

Tøndel, I. A., Jaatun, M. G., & Line, M. B. (2021). Information security challenges and practices in agile software development. *Computers & Security, 102*, 102150. https://doi.org/10.1016/j.cose.2020.102150

Venters, C. C., Jay, C., Lau, L., Griffiths, M. K., Ward, R., Xu, J., & Holmes, V. (2020). Software sustainability: Research and practice from a software architecture viewpoint. *Journal of Systems and Software, 167*, 110543. https://doi.org/10.1016/j.jss.2020.110543

Wiesner, S., Nilsson, J., & Thoben, K. D. (2022). Integrating quality management and information security in digital systems. *Computers in Industry, 140*, 103676. https://doi.org/10.1016/j.compind.2022.103676

Yılmaz, H., & Şenvar, Ö. (2025). Quality management systems and secure software infrastructures. *Journal of Information Systems and Management Research*, *7*(1), 14–28. https://doi.org/10.59940/jismar.1563163