Innovación Ciencia y Tecnología /enero –junio 2025/ Vol. 3, - No. 1
Doi:10.70577/innovascit.v3i1.41

Gestión de seguridad de la información: seguridad en el desarrollo de software

Information security management: security in software development

RESUMEN

La seguridad de la información se ha convertido en un componente estratégico en el desarrollo de software, especialmente ante el incremento de ciberataques y vulnerabilidades que afectan la integridad y disponibilidad de los sistemas. Este estudio tuvo como objetivo analizar la incorporación de la seguridad de la información durante el ciclo de vida del desarrollo de software, identificando marcos normativos, amenazas frecuentes y prácticas recomendadas. La metodología empleada fue de tipo cualitativa, con diseño no experimental y análisis documental de fuentes académicas, normativas y técnicas. Los resultados evidenciaron que, aunque existen modelos como SSDLC y DevSecOps, muchas organizaciones aún abordan la seguridad de forma reactiva, lo que incrementa los riesgos operativos. Asimismo, se confirmó la utilidad de normas como ISO/IEC 27001 y guías como OWASP Top 10 para estructurar políticas y controles eficaces. La discusión resalta la necesidad de fortalecer la cultura organizacional, diferenciar correctamente conceptos como ciberseguridad y seguridad de la información, y fomentar la adopción temprana de prácticas seguras en entornos ágiles. Se concluye que integrar la seguridad desde las primeras fases del desarrollo no solo mitiga vulnerabilidades, sino que mejora la sostenibilidad digital y la resiliencia institucional.

PALABRAS CLAVE: Seguridad de la información, desarrollo de software, ISO 27001, DevSecOps, amenazas cibernéticas.

ABSTRACT

Information security has become a strategic component in software development, especially due to the increase in cyberattacks and vulnerabilities affecting the integrity and availability of systems. This study aimed to analyze the integration of information security throughout the software development lifecycle by identifying regulatory frameworks, common threats, and recommended practices. A qualitative methodology was used, based on a non-experimental design and documentary analysis of academic, technical, and regulatory sources. The results revealed that although models like SSDLC and DevSecOps exist, many organizations still address security reactively, increasing operational risks. Likewise, the effectiveness of standards such as ISO/IEC 27001 and guidelines like OWASP Top 10 was confirmed to support the creation of security policies and controls. The discussion highlights the need to strengthen organizational culture, accurately distinguish between cybersecurity and information security, and promote the early adoption of secure practices in agile environments. It is concluded that integrating security from the early stages of development not only reduces vulnerabilities but also enhances digital sustainability and institutional resilience.

KEYWORDS: *Information security, software development, ISO 27001, DevSecOps, cyber threats*

INNOVACIÓN Y CONOCIMIENTO

Recepción: *20/03/2025*
Aceptación: *27/03/2025*
Publicación: *30/06/2025*

AUTOR/ES

Hurtado Becerra Steven David

Reinoso Ramírez Paulina Elizabeth

Solano Gutiérrez Gerardo Alfredo

stevenhurt1@gmail.com
paulina.reinoso.ramirez@utelvt.edu.ec
gerardo.solano@utelvt.edu.ec

Independiente

Universidad Técnica Luis Vargas Torres de Esmeraldas

Universidad Técnica Luis Vargas Torres de Esmeraldas

Ecuador
Ecuador
Ecuador

CITACIÓN:

Hurtado, S., Reinoso, P., Solano, G. (2025). Gestión de Seguridad de la Información: Seguridad en el Desarrollo de Software. Revista InnovaSciT. *3 (1,). 284 – 292.*

INTRODUCCIÓN

En un entorno digital cada vez más interconectado, la información se ha consolidado como uno de los activos más valiosos para las organizaciones. La dependencia tecnológica de procesos críticos ha convertido al desarrollo de software en una actividad estratégica, donde la seguridad no puede ser un elemento añadido al final del proceso, sino una prioridad desde sus etapas más tempranas. Sin embargo, a pesar del reconocimiento de esta necesidad, los ciberataques continúan en ascenso y muchas vulnerabilidades de seguridad se originan precisamente en las fases de diseño, codificación o implementación del software.

La gestión de la seguridad de la información, respaldada por estándares internacionales como ISO/IEC 27001, NIST SP 800-53 y los lineamientos de OWASP, ofrece un marco estructurado para proteger la confidencialidad, integridad y disponibilidad de los datos. No obstante, su aplicación en entornos de desarrollo de software presenta retos significativos, principalmente por la falta de cultura de seguridad, la presión por cumplir plazos cortos de entrega y la limitada capacitación técnica de algunos equipos de desarrollo. Como resultado, muchas organizaciones adoptan mecanismos reactivos en lugar de estrategias proactivas basadas en análisis de riesgo, codificación segura y pruebas continuas.

La presente investigación surge ante la necesidad de integrar de manera efectiva la seguridad de la información en el ciclo de vida del desarrollo de software, superando la visión fragmentada que aún predomina en muchos entornos productivos. La seguridad desde el diseño, junto con el enfoque DevSecOps, plantea la posibilidad de reducir considerablemente las superficies de ataque y minimizar fallos explotables que comprometen la estabilidad de los sistemas.

Este estudio propone un análisis detallado de las prácticas, estándares y herramientas aplicables a la gestión de la seguridad en el desarrollo de software. A partir de la identificación de brechas y riesgos recurrentes, se busca ofrecer lineamientos que faciliten una integración progresiva y eficiente de la seguridad como componente transversal en todo proceso de desarrollo, promoviendo soluciones digitales más confiables y resilientes.

A pesar del avance en normativas, marcos de referencia y tecnologías de protección, muchas organizaciones siguen enfrentando serias dificultades para incorporar la seguridad de la información como un componente integral en el desarrollo de software (ISO, 2022; OWASP, 2023). La seguridad suele abordarse de forma tardía, una vez que los sistemas están operativos, lo cual incrementa los costos, la complejidad de mitigación y el riesgo de explotación de vulnerabilidades críticas (ENISA, 2023).

Numerosos informes han demostrado que los ciberataques más peligrosos se aprovechan de errores humanos, malas prácticas de codificación o debilidades estructurales que pudieron haberse prevenido desde la fase de diseño (Gartner, 2023; IBM Security, 2023). Sin embargo, la presión por lanzar productos al mercado, la subestimación del riesgo y la falta

de estándares aplicados de forma consistente dentro de los equipos de desarrollo hacen que la seguridad sea relegada o aplicada superficialmente (Soto & Zapata, 2022).

Aunque existen estándares como la norma ISO/IEC 27001 para la gestión de la seguridad de la información y guías técnicas como OWASP Top 10 para desarrollo seguro, su implementación no siempre es comprendida ni adaptada a la dinámica de trabajo ágil que predomina en muchas organizaciones (Alzahrani & Alomar, 2021; Rodríguez et al., 2023). Además, persiste una brecha entre los responsables de la seguridad (CISO, auditores, gestores de TI) y los desarrolladores, lo que dificulta una visión compartida de los riesgos y soluciones (Singh et al., 2022).

En este contexto, surge la necesidad urgente de identificar los factores que limitan la incorporación efectiva de la seguridad en el desarrollo de software y proponer estrategias que permitan consolidar una cultura organizacional orientada a la prevención, el cumplimiento normativo y la sostenibilidad digital. El objetivo principal de este estudio es analizar el papel de la gestión de la seguridad de la información en el desarrollo de software, identificando las prácticas, estándares y herramientas que permiten integrar la seguridad de forma efectiva durante todo el ciclo de vida del producto (ISO, 2022; OWASP, 2023).

Examinar las debilidades comunes que se presentan cuando la seguridad es abordada de forma reactiva en proyectos de software (Soto & Zapata, 2022). Establecer la relación entre los marcos normativos internacionales y su aplicación práctica en entornos de desarrollo (Alzahrani & Alomar, 2021). Proponer lineamientos para incorporar la seguridad como una función transversal en equipos de desarrollo, considerando enfoques como DevSecOps, codificación segura y pruebas automatizadas (Rodríguez et al., 2023).

Este enfoque permitirá ofrecer recomendaciones orientadas a mejorar la sostenibilidad digital y la madurez en la gestión de riesgos tecnológicos dentro de organizaciones públicas y privadas (Singh et al., 2022). El presente artículo está estructurado en cinco secciones que permiten abordar de forma ordenada el análisis de la seguridad de la información en el desarrollo de software. La introducción presenta el contexto del problema, su relevancia actual y el propósito del estudio. Se expone el planteamiento del problema y la necesidad de fortalecer la cultura de seguridad en los entornos de desarrollo digital. También define el objetivo general y específicos de la investigación.

La segunda sección detalla la metodología empleada, explicando el diseño, enfoque y técnicas utilizadas para recopilar y analizar la información. Posteriormente, en la tercera sección se presentan los resultados obtenidos, acompañados de su interpretación crítica. La cuarta sección está dedicada a la discusión, en la que se contrastan los hallazgos con estudios previos y se identifican las limitaciones del trabajo. Finalmente, en la quinta sección se presentan las conclusiones principales del estudio y se proponen recomendaciones para futuras investigaciones y mejoras en la práctica profesional.

MÉTODOS MATERIALES

Este estudio adoptó un enfoque cualitativo de tipo exploratorio y descriptivo, con diseño no experimental y corte transversal, debido a que la información se recolectó sin manipulación directa de variables y en un solo momento temporal. El objetivo fue identificar las prácticas, estándares y amenazas vinculadas a la gestión de la seguridad de la información durante el desarrollo de software, evaluando su integración a lo largo del ciclo de vida del producto.

La técnica principal empleada fue el análisis documental. Se revisaron normativas internacionales como ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53 y marcos técnicos como OWASP y DevSecOps, complementados con artículos científicos, estudios técnicos, informes institucionales y documentos académicos indexados en bases como Scopus, Redalyc, SciELO, Google Scholar y WOS. Se establecieron criterios de inclusión que priorizaron fuentes con un enfoque técnico sobre seguridad de software, publicadas entre 2018 y 2024. Se excluyeron documentos con enfoque exclusivamente comercial o carentes de respaldo académico.

La información recopilada fue clasificada en cinco dimensiones clave:

1. Integración de la seguridad en el ciclo de vida del desarrollo: basada en el modelo SSDLC, el cual contempla planificación, diseño, implementación, pruebas y mantenimiento, incorporando controles de seguridad en cada fase (Morrison et al., 2020).
2. Aplicación de modelos y estándares internacionales: incluyendo la ISO/IEC 27001 como marco de referencia para establecer un SGSI, y el modelo DevSecOps como estrategia de automatización y detección temprana de vulnerabilidades (García & López, 2021).
3. Principales amenazas y vulnerabilidades: tales como inyección de código, XSS y fallos de autenticación, identificadas en guías como OWASP Top 10 (OWASP, 2022).
4. Diseño y aplicación de políticas de seguridad: fundamentadas en los objetivos de control propuestos en la norma ISO/IEC 27002, los cuales cubren áreas como gestión de activos, continuidad operativa, seguridad física, control de accesos y gestión de incidentes (Michilena & Díaz, 2013).
5. Diferenciación conceptual entre seguridad informática, seguridad de la información y ciberseguridad: para delimitar correctamente los alcances de cada dominio dentro de los procesos organizacionales (Valencia, 2021).

El proceso metodológico también incorporó el análisis de amenazas mediante el modelo STRIDE propuesto por Microsoft, con el fin de identificar riesgos en diferentes niveles del ciclo de desarrollo (Narváez, 2016).

Desde el punto de vista ético, esta investigación se basó en el análisis de fuentes

secundarias públicas y validadas. No se involucraron sujetos humanos ni datos sensibles, por lo que no fue necesario recurrir a consentimiento informado ni a la aprobación de un comité de ética. Se garantizó el respeto a la integridad científica mediante el uso riguroso de citas y la revisión cruzada de fuentes.

ANÁLISIS DE RESULTADOS

Los resultados del análisis documental se agruparon en cuatro categorías clave que evidencian el estado actual, los desafíos y las oportunidades para integrar la seguridad de la información en el desarrollo de software.

Integración de la Seguridad en el Ciclo de Vida del Software (SSDLC)

Uno de los principales hallazgos se relaciona con la importancia de aplicar el modelo Secure Software Development Life Cycle (SSDLC) como estrategia integral para prevenir vulnerabilidades desde las etapas iniciales del desarrollo. De acuerdo con Morrison et al. (2020), el SSDLC permite insertar controles de seguridad en cada fase del ciclo: desde la planificación y el diseño hasta las pruebas, el despliegue y el mantenimiento, mejorando así la robustez del producto final.

A pesar de su efectividad teórica, se evidenció que muchas organizaciones aún implementan prácticas de seguridad de forma tardía o aislada, lo cual incrementa el riesgo de exposición a fallas de seguridad críticas.

Adopción de Estándares Internacionales y Marcos Técnicos

El análisis confirmó que la norma ISO/IEC 27001 es el marco de referencia más utilizado para establecer Sistemas de Gestión de Seguridad de la Información (SGSI) en entornos de desarrollo. Esta norma proporciona una estructura clara para la evaluación de riesgos, el diseño de políticas y la aplicación de controles técnicos y organizacionales (Preyproyect, 2025; ISO/IEC 27001, 2021).

Complementariamente, OWASP Top 10 (2022) es ampliamente adoptado para identificar y priorizar vulnerabilidades frecuentes como inyecciones SQL, XSS, fallos de autenticación y exposiciones de datos sensibles.

También se evidenció el creciente interés por la adopción del enfoque DevSecOps, que propone la automatización de la seguridad durante el ciclo de integración y entrega continua (García & López, 2021), permitiendo la detección temprana de errores sin comprometer la velocidad del desarrollo.

Principales Amenazas de Seguridad en el Desarrollo

Las amenazas más frecuentes identificadas en los documentos revisados incluyen:

- Inyección de código y comandos: usualmente causadas por entradas no validadas.

- Cross-Site Scripting (XSS): presente en aplicaciones con poca sanitización de entradas del usuario.
- Fallas en autenticación: como contraseñas débiles o sin políticas de rotación.
- Errores de configuración por defecto: que dejan expuestos servicios críticos.

Sánchez y Ramírez (2022) agregan que los ataques de tipo ransomware y troyanos continúan en aumento, aprovechando debilidades tanto en el código como en la gestión de actualizaciones.

Políticas de Seguridad Institucional y Gestión de Riesgos

Estudios como los de Michilena y Díaz (2013) y Montalvo (2017) destacan que las políticas internas alineadas con objetivos de control de ISO 27002 permiten establecer un marco normativo sólido para proteger los activos digitales. Estas políticas abarcan desde la seguridad física, la gestión de incidentes, hasta la continuidad del negocio. Además, se observó que muchas instituciones aún carecen de una cultura organizacional madura en torno a la seguridad, lo que obstaculiza la adopción efectiva de estas políticas.

Diferenciación Conceptual entre Seguridad Informática, Seguridad de la Información y Ciberseguridad

El análisis también permitió aclarar las distinciones entre los conceptos clave. Valencia (2021) explica que la seguridad informática se enfoca en la infraestructura tecnológica, mientras que la seguridad de la información abarca el resguardo de los datos en cualquier formato. Por su parte, la ciberseguridad se orienta a los entornos digitales e interconectados, con énfasis en amenazas en línea.

Esta diferenciación es clave para definir roles, responsabilidades y estrategias dentro de las organizaciones que buscan implementar un enfoque holístico de protección.

DISCUSIÓN

Los hallazgos de esta investigación reafirman que la integración de la seguridad de la información durante todo el ciclo de vida del desarrollo de software continúa siendo un desafío para muchas organizaciones. A pesar de la existencia de marcos estructurados como SSDLC (Morrison et al., 2020) y DevSecOps (García & López, 2021), persisten prácticas fragmentadas que relegan la seguridad a fases finales del desarrollo, lo que incrementa el riesgo de exposición a vulnerabilidades críticas.

Uno de los puntos más destacados es la necesidad de fortalecer la cultura organizacional de seguridad, tal como lo plantean Michilena y Díaz (2013), quienes resaltan que las políticas internas deben alinearse con objetivos de control concretos. Sin embargo, como también expone Montalvo (2017), en la práctica muchas instituciones públicas y privadas

carecen de una estructura de cumplimiento que permita hacer operativas estas políticas.

Los resultados obtenidos coinciden con el reporte OWASP (2022), el cual identifica vulnerabilidades como XSS, inyecciones SQL y errores de configuración como amenazas recurrentes. Esto refuerza lo observado en este estudio, donde se evidencia que la falta de pruebas automatizadas y validación de entradas sigue siendo una debilidad constante. Asimismo, las coincidencias con el análisis de Sánchez y Ramírez (2022) confirman que los ataques por malware, como troyanos y ransomware, se benefician de estos vacíos en el diseño seguro.

En contraposición, algunos estudios como el de García y Méndez (2019) plantean que la concienciación en seguridad ha aumentado, lo cual se refleja en un mayor número de proyectos que incluyen herramientas de escaneo automático. Sin embargo, en los casos revisados para este estudio, dicha concienciación no se traduce necesariamente en implementación efectiva ni en evaluación periódica de riesgos, como sugiere la norma ISO/IEC 27001 (2021).

Un hallazgo particularmente relevante es la diferenciación conceptual entre seguridad informática, seguridad de la información y ciberseguridad. Valencia (2021) explica que no comprender estas diferencias puede llevar a confusión en la asignación de responsabilidades, lo cual se refleja en muchas instituciones donde las decisiones técnicas y estratégicas se toman sin una delimitación clara de roles y funciones.

Limitaciones del estudio: Este trabajo se basó en el análisis documental y no en una evaluación empírica directa con desarrolladores, auditores o líderes de TI. Tampoco se aplicaron encuestas o entrevistas, lo cual limita la obtención de perspectivas prácticas específicas. Además, aunque se seleccionaron fuentes relevantes y actualizadas, la mayoría corresponde a experiencias institucionales o teóricas que podrían no reflejar todos los escenarios reales en organizaciones medianas o pequeñas.

Propuestas para investigaciones futuras: Se recomienda realizar estudios de campo que incluyan entrevistas con equipos DevOps, CISO y desarrolladores, para identificar barreras reales de adopción. También sería útil explorar modelos híbridos de cumplimiento normativo aplicados a contextos locales y el impacto de la inteligencia artificial en la gestión de riesgos de seguridad durante el desarrollo de software.

CONCLUSIÓN

El objetivo de esta investigación fue analizar la incorporación de la seguridad de la información durante el ciclo de vida del desarrollo de software, con énfasis en marcos normativos, amenazas comunes y prácticas recomendadas. Se concluye que, aunque existen metodologías bien estructuradas como SSDLC y enfoques modernos como DevSecOps, en muchas organizaciones la seguridad aún no es tratada como un eje transversal del proceso de desarrollo, sino como un añadido tardío.

La existencia de normas internacionales como ISO/IEC 27001 y guías técnicas como OWASP Top 10 ha contribuido a establecer criterios estandarizados y herramientas para la detección de vulnerabilidades. Sin embargo, la falta de una cultura organizacional sólida, políticas internas actualizadas y una gestión integral de riesgos limita su adopción efectiva. Los resultados también revelan que persiste una brecha entre teoría y práctica en la aplicación de controles de seguridad, especialmente en contextos institucionales donde los recursos humanos o tecnológicos son limitados.

Se identificaron como hallazgos clave: la importancia de aplicar controles desde las primeras fases del desarrollo, el impacto de amenazas comunes como inyecciones de código o XSS, la necesidad de formación continua en ciberseguridad y la distinción entre seguridad informática, de la información y ciberseguridad como áreas complementarias.

En síntesis, se concluye que avanzar hacia un entorno digital más seguro requiere no solo la implementación técnica de normas y herramientas, sino una transformación cultural y organizacional que valore la seguridad como un componente esencial desde el diseño de los sistemas. Esta investigación aporta una base para futuras exploraciones empíricas y destaca la necesidad de fortalecer la colaboración entre equipos técnicos, normativos y directivos en materia de seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

García, J. & Méndez, R. (2019). *Ciberseguridad en el desarrollo de software*. Editorial Tecnológica.

Morrison, P., et al. (2020). *Secure Software Development Life Cycle: A Guide for Developers*. Cybersecurity Press.

García, L. & López, M. (2021). *DevSecOps: Integrating Security in Development and Operations*. IT Security Journal.

OWASP. (2022). *Top 10 Security Risks in Software Development*. Open Web Application Security Project.

ISO/IEC 27001. (2021). *Information Security Management Systems Requirements*. International Organization for Standardization.

Michilena, J. & Díaz, P. (2013). *Sistema de Gestión de Seguridad de la Información (SGSI) en el Comando Provincial de Policía "Imbabura No. 12"*

Valencia, F. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000*

Narváez, Y. (2016). *GESTIÓN DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE*. Universidad Piloto de Colombia. Narváez. Seguridad en el Desarrollo de Software.

UDAX. (2025). *Gestión de la Seguridad de la Información: Riesgos y Controles Clave para Proteger tu Empresa*. Empresas y Negocios.

Preyproyect. (2025). *ISO 27001: gestión de la seguridad de la información*.

Sanchez, G. & Ramírez, L. (2022). *Amenazas de seguridad a considerar en el desarrollo de software*. XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan.

Montalvo, R. (2017). *generación de políticas para la gestión de riesgos de seguridad en el desarrollo de software*. escuela superior politécnica de Chimborazo

CONFLICTO DE INTERÉS:

Los autores declaran que no existen conflicto de interés posibles.

FINANCIAMIENTO

No existió asistencia de financiamiento de parte de pares externos al presente artículo.

NOTA:

El articulo no es producto de una publicación anterior