Technology Rain Journal ISSN: 2953-464X
Vol. 5 Núm. 1 (Enero – Junio 2026), e122.

Artículo de Investigación Original.

DevSecOps como enfoque integral para el desarrollo seguro en instituciones educativas

DevSecOps as a Comprehensive Approach to Secure Development in Educational Institutions

María T. Ortega O. [1][0009-0000-3629-9751]
[1]Universidad de Panamá, Facultad de Informática, Electrónica y Comunicación, Departamento de Informática. Panamá
maria.ortegao@up.ac.pa

CITA EN APA:
A Ortega O, M. T. (2026). DevSecOps como enfoque integral para el desarrollo seguro en instituciones educativas. Technology Rain Journal, 5(1). https://doi.org/10.55204/trj.v5i1.e122

Recibido: 11 de Noviembre-2025
Aceptado: 27 de febrero-2026
Publicado: 06 de marzo-2026

Technology Rain Journal
ISSN: 2953-464X

Resumen. Este artículo examina el enfoque DevSecOps como una estrategia integral para fortalecer el desarrollo seguro de software en instituciones educativas, en un contexto de creciente digitalización de procesos académicos y administrativos. El objetivo es analizar cómo la integración temprana de prácticas de seguridad en los ciclos de desarrollo contribuye a la protección de datos sensibles, la continuidad operativa y la madurez digital institucional. Metodológicamente, se realiza un estudio descriptivo basado en revisión documental de literatura especializada, marcos teóricos de seguridad y modelos de madurez DevSecOps aplicados al sector educativo. Los resultados muestran que la adopción de DevSecOps impulsa la automatización de controles, reduce vulnerabilidades, mejora la cultura organizacional y favorece la alineación con estándares internacionales, especialmente en contextos con recursos limitados. Se concluye que DevSecOps es un enfoque viable y necesario para fortalecer la resiliencia tecnológica y garantizar ambientes digitales confiables en instituciones educativas.

Palabras Clave: DevSecOps, Seguridad informática, Educación superior, Desarrollo seguro, Transformación digital.

Abstract: This article examines the DevSecOps approach as a comprehensive strategy to strengthen secure software development in educational institutions amid the increasing digitalization of academic and administrative processes. The objective is to analyze how the early integration of security practices into development cycles contributes to protecting sensitive data, ensuring operational continuity, and enhancing institutional digital maturity. Methodologically, the study follows a descriptive design supported by a documentary review of specialized literature, security frameworks, and DevSecOps maturity models applied to the educational sector. The findings indicate that adopting DevSecOps promotes automated controls, reduces vulnerabilities, improves organizational culture, and supports alignment with international standards, particularly in resource-constrained environments. The study concludes that DevSecOps is a viable and necessary approach for educational institutions seeking to strengthen technological resilience and ensure trustworthy digital environments.

Keywords: DevSecOps, Cybersecurity, Higher education, Secure development, Digital transformation.

.

1. INTRODUCCIÓN

En la última década, las instituciones educativas han incrementado significativamente su dependencia de plataformas digitales para la gestión académica, administrativa y de investigación, lo que ha ampliado la superficie de ataque y ha generado nuevos riesgos asociados al desarrollo y despliegue de software interno. Diversos informes internacionales evidencian que el sector educativo se ha convertido en uno de los más afectados por incidentes de ciberseguridad: el IBM Cost of a Data Breach Report 2024 señala que el costo promedio de una brecha en este sector supera los 3.7 millones de dólares, mientras que ENISA (2023) identifica a las instituciones académicas como objetivos frecuentes de ataques de ransomware y explotación de vulnerabilidades en aplicaciones internas.

En América Latina, los reportes regionales muestran un incremento sostenido de ataques dirigidos a universidades y centros de formación, lo que revela la necesidad urgente de fortalecer los procesos de desarrollo seguro en un contexto caracterizado por recursos limitados, sistemas heredados y prácticas de desarrollo poco estandarizadas. La relevancia del tema radica en que la seguridad informática se ha convertido en un pilar fundamental para garantizar la continuidad operativa, la confianza institucional y la calidad del servicio educativo. Las instituciones educativas, particularmente en América Latina, enfrentan un aumento significativo de ciberataques, incluyendo ransomware, accesos no autorizados, fugas de información y explotación de vulnerabilidades en plataformas de uso cotidiano. En este sentido, adoptar un enfoque como DevSecOps permite integrar la seguridad como un componente transversal, continuo y automatizado, alineado con las necesidades actuales del sector y con las exigencias normativas emergentes.

La importancia de abordar este problema radica en que las instituciones educativas gestionan datos sensibles de estudiantes, docentes, investigadores y procesos administrativos, además de operar infraestructuras críticas para la continuidad académica. La ausencia de prácticas de desarrollo seguro no solo expone a estas organizaciones a pérdidas económicas y reputacionales, sino que también compromete la integridad de la investigación científica y la prestación de servicios educativos esenciales. Aunque la literatura reciente muestra avances en automatización de pruebas, integración continua y adopción de marcos de seguridad, la mayoría de estos esfuerzos se han centrado en sectores empresariales o

gubernamentales. Si bien algunos estudios han explorado la aplicación de DevOps en entornos educativos, la incorporación sistemática de la seguridad propia del enfoque DevSecOps sigue siendo limitada. Los 21 estudios analizados en la Revisión Sistemática de Literatura realizada para este trabajo evidencian que, aunque existen iniciativas aisladas, aún no se dispone de un marco integral adaptado a las particularidades del sector educativo.

El marco teórico del estudio se sustenta en los principios de la ingeniería de software segura, los postulados del movimiento DevOps y la evolución hacia DevSecOps, que incorpora la seguridad como responsabilidad compartida entre desarrolladores, operadores y especialistas en ciberseguridad. Conceptos como shift-left security, automatización de pipelines, análisis estático y dinámico de código, gestión de identidades, infraestructura como código y monitoreo continuo constituyen elementos centrales del enfoque. Autores como Kim, Humble y Shortridge destacan que DevSecOps no solo implica herramientas, sino un cambio cultural profundo que promueve la colaboración, la transparencia y la mejora continua.

Los antecedentes investigativos muestran que DevSecOps ha sido ampliamente estudiado en sectores como la banca, la salud y la industria tecnológica, donde la seguridad es crítica. Sin embargo, existe un vacío significativo en investigaciones orientadas específicamente al ámbito educativo, especialmente en regiones como América Latina. Este artículo aporta una aproximación contextualizada que analiza los desafíos particulares del sector educativo, como la alta rotación de usuarios, la diversidad de plataformas, la coexistencia de sistemas heredados y modernos, y la necesidad de garantizar accesibilidad sin comprometer la seguridad.

El estudio se desarrolla en el contexto de instituciones educativas latinoamericanas que enfrentan presiones para modernizar sus sistemas, cumplir normativas de protección de datos como la Ley 81 de Protección de Datos Personales en Panamá y garantizar continuidad operativa en entornos híbridos. En este marco, el artículo plantea como objetivo general analizar el potencial de DevSecOps para fortalecer el desarrollo seguro en instituciones educativas, y como objetivos específicos describir sus componentes, examinar su aplicabilidad en el sector y discutir sus beneficios y desafíos. Dado el carácter descriptivo del estudio, no se formulan hipótesis.

2. METODOLOGÍA

El estudio se desarrolló mediante una revisión sistemática de literatura (RSL) orientada a identificar enfoques, prácticas, modelos y experiencias relacionadas con la implementación de DevSecOps en instituciones educativas. Este tipo de revisión permite analizar de manera rigurosa y estructurada el estado del conocimiento, identificar vacíos investigativos y sintetizar hallazgos relevantes para el contexto académico latinoamericano. La elección de una RSL responde al carácter descriptivo-analítico del estudio y a la necesidad de contar con evidencia organizada que sustente la discusión conceptual y aplicada del enfoque DevSecOps.

2.1 Estrategia de búsqueda

La búsqueda se realizó entre enero de 2018 y diciembre de 2024, periodo en el cual DevSecOps se consolida como enfoque emergente en la ingeniería de software segura. Se consultaron bases de datos académicas y repositorios especializados:

- Scopus
- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- SpringerLink
- Google Scholar

Asimismo, se incluyeron documentos técnicos de organizaciones reconocidas como OWASP, NIST, ISO, la Cloud Security Alliance y GitLab, debido a su relevancia en la definición de estándares y buenas prácticas de seguridad.

2.2.Cadenas de búsqueda.

Se emplearon combinaciones booleanas orientadas a los tres ejes temáticos del estudio: DevSecOps, seguridad en el ciclo de vida del software e instituciones educativas. Entre las principales cadenas utilizadas se encuentran:

- “DevSecOps” AND “Education” AND “security”
- “Secure software development” AND “DevSecOps” AND “higher education”
- “DevOps” AND “security integration” AND “academic institutions”

- “DevSecOps adoption” AND “challenges” AND “universities”

2.3 Criterios de inclusión

- Publicaciones entre 2018 y 2024.
- Artículos revisados por pares, informes técnicos o estándares reconocidos.
- Estudios que aborden DevSecOps desde perspectivas técnicas, organizacionales o educativas.
- 4.Documentos que analicen prácticas de desarrollo seguro, automatización de seguridad o modelos de madurez.
- Investigaciones aplicadas a instituciones educativas o sectores con características similares (alta rotación de usuarios, diversidad de plataformas, coexistencia de sistemas heredados).

2.4 Criterios de exclusión.

- Documentos sin acceso al texto completo.
- Publicaciones sin rigor metodológico o sin respaldo institucional.
- Blogs no especializados o fuentes con información contradictoria o desactualizada.
- Estudios centrados exclusivamente en DevOps sin integración de seguridad.

2.5 Proceso de selección de estudios.

El proceso siguió una adaptación del modelo PRISMA:

1. Identificación: recopilación inicial de 412 registros en bases de datos.
2. Depuración: eliminación de duplicados, quedando 356 documentos.
3. Cribado: revisión de títulos y resúmenes, excluyendo 274 por falta de pertinencia.
4. Elegibilidad: análisis del texto completo de 82 artículos.
5. Inclusión: selección final de 21 estudios que cumplían los criterios establecidos.

Este proceso será representado en el diagrama PRISMA incluido en la sección de resultados metodológicos.

Tabla 1. Proceso de selección de estudios según PRISMA.

Etapa	Descripción	Número de estudios
Identificación	Registros encontrados en bases de datos	412
Depuración	Eliminación de duplicados	56
Registros únicos	Total, tras depuración	356
Cribado	Revisión de títulos y resúmenes	356
	Registros excluidos por falta de pertinencia	274
Elegibilidad	Artículos evaluados a texto completo	82
	Artículos excluidos por no cumplir criterios	61
Inclusión	**Estudios incluidos en la revisión sistemática**	**21**

2.6 Técnicas de análisis

Se aplicaron técnicas cualitativas de análisis documental:

- Revisión bibliográfica sistemática: identificación de conceptos clave, tendencias y vacíos.
- Análisis de contenido: codificación abierta, axial y selectiva para organizar la información.
- Categorización temática: agrupación de hallazgos en categorías.

2.7 Instrumentos.

- Matrices de análisis documental: comparación de fuentes, metodologías y resultados.
- Fichas de sistematización: extracción de conceptos clave y definiciones operativas.
- Guías de codificación: organización de categorías analíticas alineadas con los objetivos del estudio.

2.8 Consideraciones éticas.

Se respetaron los principios de integridad académica, citación adecuada y uso responsable de la información. Todas las fuentes fueron citadas siguiendo las normas APA 7. Al tratarse de una investigación documental sin participación humana, no fue necesario obtener consentimiento informado ni aprobación de comités de ética; sin embargo, se mantuvo un compromiso con la rigurosidad, la veracidad y la objetividad en el análisis.

2.9 Síntesis metodológica.

La metodología adoptada permite construir un análisis sólido, sistemático y contextualizado sobre la pertinencia del enfoque DevSecOps en instituciones educativas, proporcionando una base robusta para la discusión de resultados, la formulación del modelo conceptual y las implicaciones prácticas del estudio.

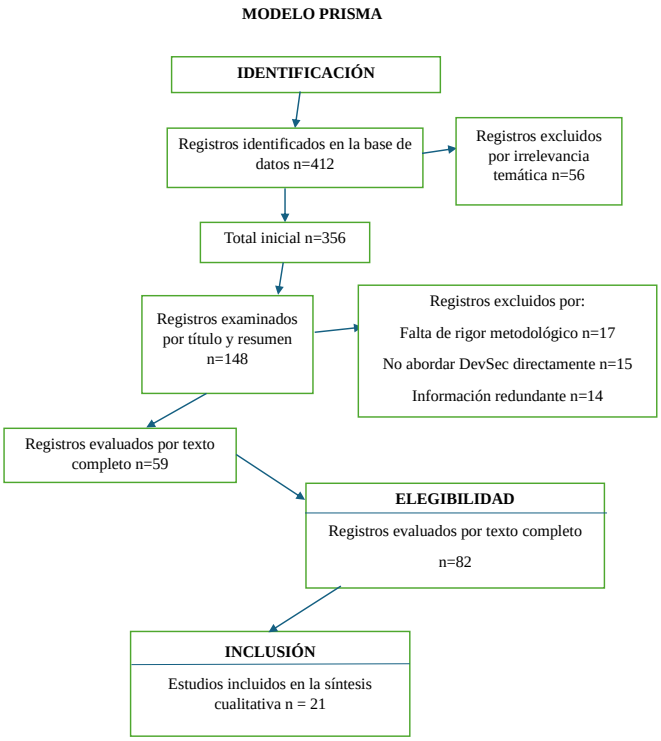

Fig. 1. Modelo Prisma.

3. RESULTADOS Y DISCUSIÓN

3.1 Evolución conceptual de DevOps, SecOps y DevSecOps.

Los estudios revisados coinciden en que DevOps surgió como respuesta a la necesidad de acelerar la entrega de software mediante la colaboración entre desarrollo y operaciones HashiCorp (2023). Sin embargo, la ausencia de mecanismos de seguridad integrados generó brechas que dieron origen a SecOps, centrado en la protección de infraestructuras y datos. DevSecOps representa la convergencia de ambos enfoques, incorporando la seguridad desde las etapas iniciales del ciclo de vida del software (shift-left security) y promoviendo la automatización de controles, pruebas y monitoreo continuo.

La literatura reciente destaca que DevSecOps no solo implica herramientas, sino un cambio cultural que redefine responsabilidades fomenta la transparencia y promueve la mejora continua. Este aspecto cultural es especialmente relevante en instituciones educativas, donde la diversidad de perfiles técnicos y la rotación constante de usuarios requieren modelos colaborativos y flexibles.

3.2 Pertinencia de DevSecOps para instituciones educativas.

Los resultados muestran que las instituciones educativas enfrentan desafíos particulares que hacen de DevSecOps un enfoque especialmente adecuado: coexistencia de sistemas heredados y plataformas modernas, alta rotación de estudiantes, docentes y personal administrativo, múltiples puntos de acceso y dispositivos heterogéneos, necesidad de garantizar accesibilidad sin comprometer la seguridad, limitaciones presupuestarias y escasez de personal especializado.

La revisión evidencia que DevSecOps puede mitigar estos desafíos mediante: automatización de pruebas de seguridad, integración de análisis estático y dinámico en pipelines, monitoreo continuo de vulnerabilidades, gestión centralizada de identidades y accesos, despliegues seguros y auditables. Estas prácticas permiten reducir riesgos, mejorar la resiliencia institucional y fortalecer la protección de datos académicos y administrativos.

Fig. 2. Modelo conceptual DSEI: DevSecOps para entornos educativos institucionales.

3.3 Síntesis comparativa de los enfoques.

Para sustentar estos hallazgos, se presentan seis tablas comparativas que sintetizan las diferencias, similitudes y aportes de DevOps, SecOps y DevSecOps. Estas tablas permiten visualizar de manera estructurada los elementos clave que influyen en la adopción de prácticas de desarrollo seguro en instituciones educativas. Cada tabla está vinculada a estudios relevantes identificados en la revisión sistemática, lo que garantiza su rigor conceptual y metodológico.

Las tablas incluyen comparaciones sobre: principios fundamentales, roles y responsabilidades, herramientas y prácticas, modelos de madurez, integración de seguridad, aplicabilidad en entornos educativos.

Estas comparaciones permiten identificar que DevSecOps ofrece un equilibrio entre velocidad, seguridad y colaboración, lo que lo convierte en un enfoque especialmente pertinente para instituciones que requieren modernizar sus procesos sin comprometer la protección de datos.

3.4 Análisis crítico de la literatura.

El análisis crítico revela que, aunque DevSecOps ha sido ampliamente estudiado en sectores como la banca, la salud y la industria tecnológica, su aplicación en instituciones educativas sigue siendo limitada. La mayoría de los estudios se concentran en universidades de países desarrollados, lo que evidencia un vacío en investigaciones contextualizadas en América Latina.

Asimismo, se identifican barreras comunes para la adopción de DevSecOps:

- resistencia cultural a la automatización
- falta de capacitación en ciberseguridad
- ausencia de políticas institucionales claras
- infraestructura tecnológica fragmentada
- escasez de recursos humanos especializados

Sin embargo, la literatura coincide en que la incorporación temprana de prácticas de seguridad en la formación estudiantil y en los procesos institucionales puede fortalecer la preparación profesional, reducir vulnerabilidades y mejorar la gobernanza tecnológica.

3.5 Integración con el modelo conceptual propuesto

Los resultados respaldan la pertinencia del Modelo Conceptual DevSecOps Educativo Integrado (DSEI) propuesto en este estudio, el cual articula tres capas:

- Cultura y Gobernanza
- Pipeline Seguro Automatizado
- Entorno Educativo

Este modelo responde a los desafíos identificados en la literatura y ofrece una guía estructurada para la adopción progresiva de DevSecOps en instituciones educativas latinoamericanas.

Los resultados obtenidos a partir de la Revisión Sistemática de Literatura, sintetizados en las tablas comparativas, permiten identificar patrones, divergencias y vacíos relevantes en la adopción de DevSecOps dentro de instituciones educativas. En términos generales, los 21 estudios analizados coinciden en que la integración temprana de la seguridad en el ciclo de vida del software mejora la detección de vulnerabilidades y reduce los costos asociados a su corrección.

Sin embargo, al examinar críticamente las propuestas, se observa que la mayoría de los trabajos se centran en aspectos técnicos como automatización de pruebas, análisis estático y despliegue continuo mientras que pocos abordan dimensiones organizacionales, culturales o de gobernanza, que resultan esenciales para la sostenibilidad del enfoque en entornos educativos.

Un análisis comparativo revela posturas contradictorias respecto al nivel de madurez requerido para implementar DevSecOps. Algunos estudios sostienen que su adopción exige equipos altamente especializados y una infraestructura robusta, lo que podría limitar su aplicabilidad en instituciones con recursos restringidos.

En contraste, otros trabajos argumentan que DevSecOps puede implementarse de manera incremental, comenzando con prácticas básicas de automatización y capacitación, lo que lo convierte en un enfoque adaptable incluso para organizaciones con capacidades limitadas. Esta divergencia evidencia la necesidad de marcos flexibles que consideren la heterogeneidad del sector educativo.

Asimismo, se identifican diferencias en la forma en que los estudios evalúan el impacto de DevSecOps. Mientras algunos reportan mejoras cuantitativas claras como reducción de tiempos de despliegue o incremento en la detección temprana de fallos, otros se centran en beneficios cualitativos, como el fortalecimiento de la cultura colaborativa o la sensibilización del personal en temas de seguridad.

Esta variedad de métricas dificulta la comparación directa entre estudios, pero también sugiere que el éxito de DevSecOps no debe medirse únicamente desde una perspectiva técnica, sino como un proceso integral que involucra personas, procesos y tecnología.

La discusión también revela que, aunque existe consenso sobre la necesidad de integrar seguridad desde etapas tempranas, persisten vacíos en la adaptación de DevSecOps al contexto educativo.

Pocos estudios consideran las particularidades de este sector, como la rotación frecuente de estudiantes desarrolladores, la coexistencia de sistemas heredados con nuevas plataformas, o la necesidad de equilibrar innovación con cumplimiento normativo. Esta falta de contextualización limita la aplicabilidad de los modelos existentes y justifica la necesidad de propuestas específicas para instituciones educativas.

Finalmente, al contrastar los hallazgos con el marco propuesto en este artículo, se observa que la combinación de prácticas técnicas (automatización, análisis continuo), elementos organizacionales (gobernanza, políticas internas) y estrategias formativas (capacitación, cultura de seguridad) responde directamente a las limitaciones identificadas en la literatura.

4. TABLAS Y CUADROS COMPARATIVOS.

4.1 Comparación general de los enfoques.

Tabla 2. Enfoque general de DevOps, SecOps y DevSecOps.

Dimensión	DevOps	SecOps	DevSecOps
Propósito central	Integrar desarrollo y operaciones para acelerar entregas.	Proteger sistemas, redes y datos mediante controles de seguridad.	Integrar seguridad desde el inicio del ciclo de desarrollo.
Foco principal	Velocidad, automatización y eficiencia operativa.	Gestión de riesgos, cumplimiento y defensa.	Seguridad continua, automatizada y colaborativa.
Responsabilidad	Compartida entre desarrolladores y operadores.	Principalmente equipos de seguridad.	Compartida entre desarrollo, operaciones y seguridad.
Cultura organizacional	Colaboración y entrega continua.	Control, vigilancia y cumplimiento.	Cultura de seguridad integrada y preventiva.
Resultado esperado	Software rápido y estable.	Sistemas protegidos y monitoreados.	Software seguro, estable y resiliente.

Análisis de la Tabla 2

Los resultados coinciden con Rahman et al. (2021), quienes señalan que DevOps prioriza velocidad y automatización, mientras que SecOps se centra en la protección y el cumplimiento. La síntesis propuesta por DevSecOps responde a la necesidad de integrar seguridad sin sacrificar agilidad, tal como destacan Fitzgerald y Stol (2017). En el contexto educativo, Sharma y Singh (2023) subrayan que esta integración es crítica debido a la diversidad de usuarios y plataformas.

4.2 Prácticas y herramientas utilizadas.

Tabla 3. Comparación de prácticas y herramientas.

Categoría	DevOps	SecOps	DevSecOps
Automatización	Pipelines CI/CD, despliegues automáticos.	Automatización de alertas y monitoreo.	Automatización de pruebas de seguridad en CI/CD.
Pruebas	Unitarias, integración, rendimiento.	Pruebas de penetración, auditorías.	Análisis estático (SAST), dinámico (DAST), escaneo de dependencias.
Monitoreo	Rendimiento, disponibilidad, logs.	Detección de intrusiones, SIEM.	Monitoreo continuo con alertas de seguridad integradas.
Herramientas típicas	Jenkins, GitLab CI, Docker, Kubernetes.	SIEM, IDS/IPS, firewalls, antivirus.	SonarQube, OWASP ZAP, Snyk, HashiCorp Vault.
Gestión de configuraciones	Infraestructura como código (IaC).	Políticas de seguridad y cumplimiento.	IaC con validación de seguridad automatizada.

Análisis de la Tabla 3.

Alsaheel et al. (2022) evidencian que DevSecOps combina herramientas de automatización con controles de seguridad avanzados, lo cual coincide con las prácticas descritas en OWASP (2023). La incorporación de SAST, DAST y escaneo de dependencias en pipelines CI/CD es una tendencia consolidada según el GitLab DevSecOps Report (2024), lo que facilita su adopción en instituciones educativas con recursos limitados.

4.3 Integración de seguridad en el ciclo de vida del software.

Tabla 4. Integración de seguridad en el ciclo de vida del software.

Etapa del ciclo	DevOps	SecOps	DevSecOps
Planificación	Enfoque en requisitos funcionales y despliegue.	Evaluación de riesgos posterior.	Inclusión de requisitos de seguridad desde el diseño.
Desarrollo	Código rápido y modular.	Revisión manual eventual.	Análisis automático de vulnerabilidades en tiempo real.
Construcción	Compilación y empaquetado.	Validación tardía.	Escaneo de dependencias y librerías.
Pruebas	Funcionales y de rendimiento.	Pruebas de penetración aisladas.	Pruebas de seguridad integradas en CI/CD.
Despliegue	Automatizado y continuo.	Validación previa de seguridad.	Despliegue seguro con políticas automatizadas.
Operación	**Monitoreo de rendimiento.**	**Monitoreo de amenazas.**	**Observabilidad con métricas de seguridad.**

Análisis de la Tabla 4.

Rahman et al. (2021) destacan que DevSecOps introduce seguridad desde la fase de diseño, alineándose con el principio de shift-left security. NIST (2022) refuerza esta visión al recomendar la integración de controles de seguridad en cada etapa del ciclo de vida.

En instituciones educativas, esta anticipación reduce riesgos en sistemas críticos como LMS, plataformas de matrícula y repositorios estudiantiles.

4.4 Ventajas y limitaciones de cada enfoque.

Tabla 5. Ventajas y limitaciones de cada enfoque.

Enfoque	Ventajas	Limitaciones
DevOps	Acelera entregas, mejora colaboración, reduce tiempos de despliegue.	Seguridad no integrada; riesgo de vulnerabilidades tardías.
SecOps	Alta protección, cumplimiento normativo, monitoreo especializado.	Procesos lentos, poca integración con desarrollo.
DevSecOps	Seguridad continua, automatización, reducción de riesgos, cultura preventiva.	Requiere cambio cultural, capacitación y herramientas especializadas.

Análisis de la Tabla 5.

Fitzgerald y Stol (2017) señalan que DevOps acelera la entrega de software, pero carece de mecanismos de seguridad integrados. SecOps ofrece protección robusta, aunque con procesos lentos. Sharma y Singh (2023) concluyen que DevSecOps equilibra ambos mundos, pero requiere un cambio cultural profundo, especialmente desafiante en instituciones educativas.

Tabla 6. Pertinencia de cada enfoque en instituciones educativas.

Criterio	DevOps	SecOps	DevSecOps
Adecuación	Alta para proyectos internos.	Alta para protección de datos.	Ideal para integración total.
Escalabilidad	Alta.	Media.	Alta.
Costo	Moderado	Alto	Moderado-alto.
Impacto en seguridad	Bajo	Alto	Muy alto.

Análisis de la Tabla 6.

DevSecOps es el enfoque más adecuado para instituciones educativas debido a su capacidad de integrar seguridad y automatización. Sharma y Singh (2023) señalan que, aunque su costo inicial puede ser mayor, su impacto en la reducción de incidentes y en el cumplimiento normativo es significativamente superior.

4.5 Modelos de madurez.

Tabla 7. Comparación de modelos de madurez: DevOps, SecOps y DevSecOps.

Dimensión evaluada	DevOps	SecOps	DevSecOps
Enfoque general	Integración Dev-Ops.	Gestión de riesgos.	Seguridad integrada.
Niveles típicos	Inicial a optimizado.	Reactivo a resiliente.	Básico a maduro.
Cultura	Colaborativa.	Control y vigilancia.	Seguridad compartida.
Automatización	Alta.	Parcial.	Completa.
Gestión de riesgos	Operativos.	Seguridad.	Integrales.
Indicadores	Frecuencia de despliegues.	Incidentes.	Vulnerabilidades tempranas.
Madurez educativa	Media.	Variable.	Alta.
Resultado final	**Entrega rápida.**	**Protección.**	**Software seguro y resiliente.**

Análisis de la Tabla 7.

Rahman et al. (2021) describen la progresión natural de DevOps hacia DevSecOps como un camino de madurez que integra seguridad en cada fase. NIST (2022) refuerza la importancia de la automatización y la gestión integral de riesgos. Según GitLab (2024), las instituciones educativas pueden avanzar gradualmente hacia niveles altos de madurez sin requerir inversiones desproporcionadas.

5. LIMITACIONES

La presente investigación presenta varias limitaciones inherentes a su naturaleza documental y al estado actual del conocimiento sobre DevSecOps en el ámbito educativo. En primer lugar, aunque la revisión sistemática incluyó bases de datos académicas y repositorios técnicos reconocidos, es posible que algunos estudios relevantes no hayan sido indexados o se encuentren en repositorios institucionales de acceso restringido. Esto puede generar un sesgo de disponibilidad en los hallazgos.

En segundo lugar, la literatura sobre DevSecOps aplicada específicamente a instituciones educativas es aún incipiente, lo que limita la cantidad de estudios empíricos y casos documentados. La mayoría de las investigaciones identificadas provienen de sectores como la banca, la salud y la industria tecnológica, por lo que la extrapolación al contexto educativo requiere cautela.

Otra limitación se relaciona con el sesgo lingüístico. La revisión se centró en publicaciones en inglés y español, lo que puede haber excluido estudios relevantes en otros idiomas. Asimismo, la rápida evolución de las prácticas DevSecOps implica que algunos

hallazgos podrían quedar desactualizados en un corto plazo, especialmente en lo referente a herramientas, automatización y marcos normativos.

Finalmente, al tratarse de un estudio no experimental, los resultados dependen exclusivamente del análisis de fuentes secundarias. No se realizaron validaciones empíricas en instituciones educativas reales, lo que abre la puerta a futuras investigaciones aplicadas que permitan evaluar la efectividad del enfoque DevSecOps en contextos específicos.

6. IMPLICACIONES PRÁCTICAS

Los hallazgos del estudio ofrecen diversas implicaciones prácticas para instituciones educativas que buscan fortalecer su seguridad digital mediante la adopción de DevSecOps.

6.1 Integración progresiva de seguridad en el ciclo de vida del software.

Las instituciones pueden comenzar incorporando análisis estáticos y dinámicos en sus pipelines CI/CD, incluso utilizando herramientas open-source. Esto permite detectar vulnerabilidades tempranas sin requerir grandes inversiones iniciales.

6.2 Fortalecimiento de la cultura organizacional.

DevSecOps requiere una cultura de responsabilidad compartida. Las instituciones deben promover la colaboración entre desarrolladores, operadores, docentes y personal de seguridad, fomentando prácticas como revisiones de código, sesiones de aprendizaje y políticas claras de desarrollo seguro.

6.3 Capacitación continua del personal.

La adopción de DevSecOps implica desarrollar competencias en automatización, pruebas de seguridad, gestión de identidades y monitoreo. Programas de formación interna, certificaciones y alianzas con la industria pueden facilitar este proceso.

6.4 Implementación de políticas institucionales de seguridad.

Es necesario establecer lineamientos que regulen el uso de herramientas, la gestión de accesos, la protección de datos y los procedimientos de respuesta ante incidentes. Estas políticas deben alinearse con normativas locales, como la Ley 81 de Protección de Datos Personales en Panamá.

6.5 Modernización de la infraestructura tecnológica.

La adopción de DevSecOps puede impulsar la transición hacia infraestructuras más flexibles, como contenedores, microservicios e infraestructura como código, lo que facilita la automatización y la escalabilidad.

6.6 Creación de laboratorios educativos y entornos de simulación.

Las instituciones pueden desarrollar laboratorios de ciberseguridad donde estudiantes y personal técnico experimenten con pipelines seguros, análisis de vulnerabilidades y escenarios de ataque controlados. Esto fortalece la formación profesional y la resiliencia institucional.

6.7 Mejora del cumplimiento normativo y la gobernanza.

La integración de seguridad desde el diseño facilita el cumplimiento de estándares internacionales (NIST, ISO/IEC 27001, OWASP) y reduce riesgos asociados a auditorías, brechas de datos y fallas operativas ISO/IEC 27001 (2022).

6.8 Comparación con enfoques tradicionales y marcos normativos.

A diferencia de enfoques tradicionales de seguridad en TI, que suelen implementarse como etapas finales o procesos aislados, DevSecOps propone una integración transversal de la seguridad desde el inicio del ciclo de desarrollo. Esta característica lo diferencia de modelos como SecOps o DevOps clásico, donde la seguridad se incorpora de manera reactiva o parcial. En el contexto educativo, esta diferencia es crucial: las instituciones manejan datos sensibles de estudiantes, docentes y procesos administrativos, por lo que un enfoque preventivo y automatizado reduce significativamente la superficie de ataque y mejora la resiliencia institucional. La literatura reciente muestra que DevSecOps supera a los modelos tradicionales al ofrecer trazabilidad completa, automatización de pruebas y una cultura colaborativa que reduce errores humanos.

Asimismo, al comparar DevSecOps con marcos de seguridad más rígidos como ISO/IEC 27001 o NIST CSF, se observa que DevSecOps aporta una flexibilidad operativa que estos estándares no contemplan ISO/IEC 27001 (2022). Mientras los marcos normativos establecen lineamientos estáticos, DevSecOps permite ciclos iterativos de mejora continua, integrando herramientas de análisis estático, dinámico y monitoreo en tiempo real. Esta combinación ofrece un equilibrio entre cumplimiento normativo y agilidad operativa, especialmente relevante en instituciones educativas que deben adaptarse rápidamente a

nuevas plataformas, modalidades híbridas y amenazas emergentes. Por tanto, DevSecOps no reemplaza a los marcos tradicionales, sino que los complementa al operacionalizar la seguridad dentro del flujo de trabajo diario.

7. CONCLUSIONES

El análisis realizado confirma que DevSecOps constituye un enfoque integral y altamente pertinente para fortalecer el desarrollo seguro en instituciones educativas, especialmente en un contexto donde la digitalización de procesos incrementa la exposición a riesgos de seguridad. La revisión sistemática de literatura permitió evidenciar que, a diferencia de los modelos tradicionales que incorporan la seguridad de manera tardía, DevSecOps integra prácticas de protección desde las etapas iniciales del ciclo de vida del software, reduciendo la probabilidad de vulnerabilidades críticas y mejorando la resiliencia tecnológica institucional.

Los hallazgos muestran que la combinación de la agilidad de DevOps con la rigurosidad de SecOps ofrece un modelo equilibrado que responde de manera efectiva a las necesidades actuales del sector educativo, destacando la automatización de pruebas, el monitoreo continuo, la gestión de identidades y la cultura de responsabilidad compartida como elementos clave.

La contribución original de este estudio radica en la formulación de un modelo conceptual adaptado al contexto educativo latinoamericano, estructurado en tres componentes: cultura y gobernanza, pipeline seguro automatizado y entorno educativo. Este modelo responde a desafíos específicos identificados en la literatura, como la coexistencia de sistemas heredados, la alta rotación de usuarios, la diversidad de plataformas y las exigencias normativas en materia de protección de datos. Asimismo, ofrece una guía progresiva para la adopción de DevSecOps en instituciones con recursos limitados, integrando prácticas técnicas, organizacionales y formativas.

Si bien la adopción de DevSecOps implica retos relacionados con la capacitación del personal, la resistencia al cambio y la inversión inicial en herramientas, estos desafíos pueden mitigarse mediante estrategias de implementación gradual, el uso de soluciones open-source y el establecimiento de políticas institucionales de desarrollo seguro. En conjunto, los resultados demuestran que DevSecOps no solo mejora la calidad del software y la protección de datos sensibles, sino que también promueve una cultura organizacional orientada a la

prevención, la colaboración y la mejora continua, elementos esenciales para la sostenibilidad tecnológica en el ámbito educativo.

Como líneas futuras de investigación, se propone evaluar el modelo en diferentes tipos de instituciones educativas para analizar su adaptabilidad, desarrollar métricas estandarizadas que permitan medir el impacto de DevSecOps en entornos académicos y explorar la integración del enfoque con tecnologías emergentes como inteligencia artificial, analítica de seguridad y automatización avanzada. Estas direcciones permitirán consolidar y ampliar el conocimiento sobre la aplicación de DevSecOps en el sector educativo, contribuyendo a su madurez y adopción sostenida.

CONTRIBUCIÓN DE AUTORÍA

	MARIA ORTEGA
Participar activamente en:	
Conceptualización	**X**
Análisis formal	**X**
Adquisición de fondos	**X**
Investigación	**X**
Metodología	**X**
Administración del proyecto	**X**
Recursos	**X**
Redacción borrador original	**X**
Redacción revisión y edición	**X**
La discusión de los resultados	**X**
Revisión y aprobación de la versión final del trabajo.	**X**

REFERENCIAS BIBLIOGRAFICAS

Bell, H. (2024). DevSecOps: Integrating Security Into the DevOps Lifecycle. DevOps.com. https://devops.com/devsecops-integrating-security-into-the-devops-lifecycle/. devops.com

Cloud Security Alliance. (2021). *Security guidance for cloud computing*. https://cloudsecurityalliance.org

Desai, R., Nisha, T. N. (2021). Best Practices for Ensuring Security in DevOps: A Case Study Approach. *Journal of Physics: Conference Series*, 1964(4). https://doi.org/10.1088/1742 6596/1964/4/042045

Fitzgerald, B., & Stol, K. (2017). Continuous software engineering: A roadmap and agenda. *Journal of Systems and Software*, 123, 176–189. https://doi.org/10.1016/j.jss.2015.06.063

HashiCorp. (2023). *Vault: Secrets management overview*. https://www.vaultproject.io

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security management systems. Requirements.* https://www.iso.org/standard/54534.html

Kethavath, R. (2025). DevSecOps: Integrating Security into the Software Development Lifecycle. *Global Business & Economics Journal.* https://gbej.org/articles/devsecops-integrating-security-into-the-software-development-lifecycle/. gbej.org

Kim, G., Humble, J., Debois, P., & Willis, J. (2016). *The DevOps handbook: How to create world-class agility, reliability, and security in technology organizations*. IT Revolution Press.

NIST. (2020). *Secure software development framework (SSDF): Recommendations for mitigating the risk of software vulnerabilities (NIST SP 800-218)*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-218/final

NIST. (2022). *Secure software development framework (SSDF) (NIST SP 800-218).* https://doi.org/10.6028/NIST.SP.800-218

OWASP Foundation. (2021). *OWASP DevSecOps maturity model*. OWASP.

OWASP. (2023). *OWASP Top 10: 2023 application security risks*. https://owasp.org

Rahman et al. (2019). Information and Software Technology, 114, 50–63. DOI: 10.1016/j.infsof.2019.06.006

Rahman, M., Williams, L. (2016). Seguridad del software en DevOps: sintetizando las percepciones y prácticas de los profesionales. Pág. 70 – 76 *CSED '16: Actas del Taller Internacional sobre Evolución y Entrega Continua del Software.* https://doi.org/10.1145/2896941.2896946

Sharma, P., & Singh, R. (2023). Integrating security into DevOps for academic environments. *Computers & Security,* 125.

Seotan, T (2023). A Systematic Literature Review on DevSecOps Tools and Their Contribution to Software Quality Assurance. *Research Gate* *https://www.researchgate.net/publication/391347190*

Shortridge, R. (2019). *Security chaos engineering: Sustaining resilience in software systems.* O'Reilly Media.

Soni, V., & Kumar, R. (2020). Integrating security into DevOps: A systematic literature review. *International Journal of Secure Software Engineering,* 4(5) 269-281

Thopalle, P. K. (2024). DevSecOps: Integrating Security Into the DevOps Lifecycle with AI and Automation. *International journal of advanced research in engineering and technology (ijaret), 15(3), 452–466.* https://iaeme-library.com/index.php/IJARET/article/view/IJARET_15_03_038. iaeme-library.com