Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

DEVSECOPS Y SU IMPACTO EN LA GOBERNANZA TI EN UNIVERSIDADES LATINOAMERICANAS

DEVSECOPS AND ITS IMPACT ON IT GOVERNANCE IN LATIN AMERICAN UNIVERSITIES

Maria Teodolinda Ortega Ovalle
Universidad de Panamá

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22753

DevSecOps y su impacto en la gobernanza TI en universidades latinoamericanas

Maria Teodolinda Ortega Ovalle[1]
maria.ortegao@up.ac.pa
https://orcid.org/0009-0000-3629-9751
Facultad de Informática, Electrónica y Comunicación.
Universidad de Panamá
Departamento de Informática.

RESUMEN

La gobernanza de Tecnologías de la Información (TI) en universidades latinoamericanas enfrenta desafíos crecientes asociados a la complejidad operativa, la dependencia de sistemas digitales y la necesidad de garantizar seguridad en entornos académicos cada vez más interconectados. En este contexto, el enfoque DevSecOps emerge como una alternativa estratégica para integrar prácticas de seguridad desde las primeras fases del desarrollo y operación tecnológica. El objetivo de este estudio es analizar el impacto de DevSecOps en la gobernanza TI universitaria, identificando beneficios, limitaciones y oportunidades de adopción en instituciones de educación superior de la región. La metodología se basó en una revisión documental sistemática y un análisis comparativo de modelos de gobernanza y prácticas DevSecOps aplicadas en entornos educativos. Los resultados muestran que la incorporación de DevSecOps fortalece la gestión de riesgos, mejora la trazabilidad de procesos, promueve la automatización de controles y facilita la alineación entre equipos técnicos y administrativos. Asimismo, se evidencia que su adopción contribuye a una gobernanza más ágil, transparente y orientada a la mejora continua. Se concluye que DevSecOps representa un marco viable para modernizar la gobernanza TI en universidades latinoamericanas, siempre que se acompañe de políticas institucionales claras, capacitación continua y una cultura organizacional orientada a la seguridad.

Palabras clave: DevSecOps, gobernanza TI, educación superior, gestión de riesgos, automatización, seguridad digital.

[1] Autor principal
Correspondencia: maria.ortegao@up.ac.pa

DevSecOps and Its Impact on IT Governance in Latin American Universities

ABSTRACT

Information Technology (IT) governance in Latin American universities faces increasing challenges related to operational complexity, reliance on digital systems, and the need to ensure security in highly interconnected academic environments. Within this context, the DevSecOps approach emerges as a strategic alternative to integrate security practices from the earliest stages of development and technological operations. This study aims to analyze the impact of DevSecOps on university IT governance, identifying benefits, limitations, and adoption opportunities within higher education institutions in the region. The methodology consisted of a systematic literature review and a comparative analysis of governance models and DevSecOps practices applied in educational settings. The findings indicate that incorporating DevSecOps strengthens risk management, enhances process traceability, promotes the automation of security controls, and improves alignment between technical and administrative teams. Additionally, results show that DevSecOps contributes to more agile, transparent, and continuously improving governance structures. The study concludes that DevSecOps represents a viable framework for modernizing IT governance in Latin American universities, provided it is supported by clear institutional policies, ongoing training, and a security-oriented organizational culture.

Keywords: DevSecOps, IT governance, higher education, risk management, automation, digital security.

Artículo recibido 18 diciembre 2025
Aceptado para publicación: 23 enero 2026

INTRODUCCIÓN

La gobernanza de Tecnologías de la Información (TI) en las universidades latinoamericanas atraviesa un proceso de transformación acelerada impulsado por la digitalización de los servicios académicos, administrativos y de investigación. La expansión de plataformas virtuales de aprendizaje, sistemas de gestión institucional, repositorios científicos, servicios en la nube y herramientas colaborativas ha incrementado la complejidad operativa y los riesgos asociados a la seguridad digital. En este contexto, las instituciones de educación superior enfrentan el desafío de garantizar la integridad, disponibilidad y confidencialidad de la información, al tiempo que deben responder a demandas crecientes de eficiencia, transparencia, continuidad académica y cumplimiento normativo.

A pesar de estos avances, la gobernanza TI en la región continúa marcada por estructuras jerárquicas tradicionales, procesos manuales, baja automatización y enfoques reactivos frente a incidentes de seguridad. Estas limitaciones se hacen más evidentes ante el aumento de ciberataques dirigidos a universidades, la proliferación de vulnerabilidades en sistemas heredados y la necesidad de integrar múltiples servicios digitales en ecosistemas cada vez más interconectados. La falta de alineación entre equipos de desarrollo, operaciones y seguridad genera brechas que afectan la capacidad institucional para responder oportunamente a amenazas emergentes.

En este escenario, el enfoque DevSecOps surge como una alternativa estratégica que integra desarrollo, operaciones y seguridad en un ciclo continuo, automatizado y colaborativo. Su adopción implica no solo la incorporación de herramientas y prácticas técnicas, sino también transformaciones culturales orientadas a la responsabilidad compartida, la mejora continua y la gestión proactiva del riesgo. Para las universidades latinoamericanas, DevSecOps representa una oportunidad para fortalecer la gobernanza TI mediante procesos más ágiles, trazables y seguros, alineados con las necesidades institucionales contemporáneas.

Este artículo analiza el impacto de DevSecOps en la gobernanza TI universitaria, identificando beneficios, desafíos y oportunidades de adopción en instituciones de educación superior de la región. Asimismo, se examina cómo este enfoque puede contribuir a la modernización de los modelos de gestión tecnológica, promoviendo una cultura organizacional orientada a la seguridad y la innovación.

MARCO TEÓRICO

Gobernanza de Tecnologías de la Información en universidades latinoamericanas.

La gobernanza de Tecnologías de la Información (TI) se define como el conjunto de estructuras, procesos y mecanismos que aseguran que las inversiones tecnológicas estén alineadas con los objetivos institucionales, generen valor y gestionen adecuadamente los riesgos asociados. En el contexto universitario latinoamericano, la gobernanza TI adquiere una relevancia particular debido a la diversidad de servicios digitales que soportan la docencia, la investigación, la administración y la vinculación con la sociedad. Sin embargo, múltiples estudios señalan que las universidades de la región presentan modelos de gobernanza fragmentados, con baja estandarización, limitada automatización y escasa integración entre áreas técnicas y administrativas.

Factores como la dependencia de sistemas heredados, la falta de políticas institucionales actualizadas, la insuficiente inversión en ciberseguridad y la carencia de personal especializado dificultan la consolidación de una gobernanza TI robusta. A ello se suma la creciente sofisticación de las amenazas cibernéticas, que afectan directamente la continuidad académica y la protección de datos sensibles. En este escenario, se requieren enfoques modernos que permitan fortalecer la gestión tecnológica mediante prácticas colaborativas, automatizadas y orientadas a la seguridad.

Evolución de los modelos DevOps y su transición hacia DevSecOps.

DevOps surgió como una respuesta a la necesidad de integrar los equipos de desarrollo (Dev) y operaciones (Ops) para acelerar la entrega de software, mejorar la calidad y reducir los tiempos de despliegue. Su filosofía se basa en la colaboración continua, la automatización de procesos y la retroalimentación constante. Sin embargo, la creciente exposición a riesgos digitales evidenció que la seguridad no podía mantenerse como un proceso aislado o posterior al desarrollo.

En este contexto, DevSecOps emerge como una evolución natural de DevOps, incorporando la seguridad (Sec) como un componente transversal desde las primeras etapas del ciclo de vida del software. DevSecOps promueve la automatización de controles, la integración de pruebas de seguridad en pipelines, la gestión proactiva de vulnerabilidades y la responsabilidad compartida entre todos los actores involucrados. Este enfoque permite reducir riesgos, mejorar la trazabilidad y garantizar que las aplicaciones cumplan con estándares de seguridad desde su concepción.

Principios fundamentales de DevSecOps.

DevSecOps se sustenta en una serie de principios que orientan su implementación:

1. Seguridad integrada desde el diseño (Security by Design): La seguridad se incorpora desde la planificación y no como una etapa final.
2. Automatización de controles: Uso de herramientas para análisis estático, dinámico, escaneo de dependencias y verificación continua.
3. Responsabilidad compartida: Todos los equipos, desarrollo, operaciones y seguridad participan activamente en la protección del sistema.
4. Cultura colaborativa: Comunicación abierta, retroalimentación continua y eliminación de silos organizacionales.
5. Mejora continua: Evaluación constante de procesos, herramientas y prácticas para adaptarse a nuevas amenazas.
6. Trazabilidad y auditoría: Registro detallado de cambios, despliegues y eventos de seguridad.

Estos principios permiten que DevSecOps no sea únicamente un conjunto de herramientas, sino un marco cultural y organizacional que transforma la forma en que se construyen y operan los sistemas.

DevSecOps en entornos educativos: oportunidades y desafíos.

La adopción de DevSecOps en universidades presenta oportunidades significativas. Entre ellas destacan la mejora en la gestión de riesgos, la reducción de vulnerabilidades en sistemas académicos, la automatización de procesos críticos y la alineación entre equipos técnicos y administrativos. Además, DevSecOps facilita la modernización de plataformas educativas, la protección de datos estudiantiles y el cumplimiento de normativas de privacidad.

No obstante, su implementación enfrenta desafíos particulares en la región: limitaciones presupuestarias, resistencia al cambio cultural, falta de capacitación especializada, infraestructura tecnológica heterogénea y ausencia de políticas institucionales claras. Superar estas barreras requiere estrategias de gobernanza que integren DevSecOps como parte de un modelo de gestión más amplio, orientado a la seguridad, la eficiencia y la innovación.

Relación entre DevSecOps y la gobernanza TI

DevSecOps contribuye directamente al fortalecimiento de la gobernanza TI mediante:

Mejor gestión del riesgo tecnológico

Mayor transparencia y trazabilidad de procesos

Automatización de controles y auditorías

Alineación entre objetivos institucionales y prácticas técnicas

Reducción de incidentes y tiempos de respuesta

Promoción de una cultura organizacional orientada a la seguridad

En universidades latinoamericanas, donde la gobernanza TI suele ser reactiva y fragmentada, DevSecOps ofrece un marco para avanzar hacia modelos más ágiles, integrados y sostenibles.

METODOLOGÍA

Enfoque de investigación

Este estudio se desarrolló bajo un enfoque cualitativo de carácter descriptivo–analítico, orientado a comprender el impacto del enfoque DevSecOps en la gobernanza de Tecnologías de la Información (TI) en universidades latinoamericanas. El propósito metodológico fue identificar patrones, tendencias, beneficios y desafíos asociados a la adopción de prácticas DevSecOps en contextos educativos, así como analizar su contribución a la modernización de los modelos de gestión tecnológica.

Diseño de investigación

Se empleó un diseño de revisión documental sistemática, complementado con un análisis comparativo de modelos de gobernanza TI y prácticas DevSecOps aplicadas en instituciones de educación superior. Este diseño permitió integrar evidencia reciente, contrastar enfoques y generar una visión amplia y fundamentada del fenómeno estudiado.

Procedimiento de búsqueda y selección de información.

La revisión documental se realizó siguiendo los lineamientos del modelo PRISMA, adaptado al contexto del estudio. El proceso incluyó:

1. Identificación de fuentes: bases de datos académicas como Scopus, IEEE Xplore, ScienceDirect, RedALyC y Google Scholar.
2. Palabras clave utilizadas: “DevSecOps”, “IT governance”, “higher education”, “cybersecurity”, “Latin America”, “educational technology governance”.
3. Rango temporal: publicaciones entre 2018 y 2025 para asegurar actualidad.

4. Tipos de documentos: artículos científicos, informes técnicos, libros especializados y documentos institucionales.

Criterios de inclusión y exclusión

Criterios de inclusión

Estudios que abordaran DevSecOps en contextos educativos o institucionales.

Investigaciones sobre gobernanza TI en universidades.

Documentos que analizaran prácticas de seguridad integradas al ciclo de vida del software.

Publicaciones en español o inglés.

Criterios de exclusión

Estudios sin rigor metodológico verificable.

Documentos que no abordaran DevSecOps de manera directa.

Información redundante o duplicada.

Publicaciones anteriores a 2018.

Análisis de la información

La información seleccionada fue analizada mediante:

Codificación temática: identificación de categorías como gobernanza TI, automatización, seguridad integrada, cultura organizacional y riesgos.

Comparación transversal: contraste entre prácticas DevSecOps y modelos tradicionales de gobernanza TI.

Síntesis narrativa: integración de hallazgos para construir una visión coherente del impacto de DevSecOps en universidades latinoamericanas.

Consideraciones éticas

El estudio se basó exclusivamente en fuentes secundarias de acceso público y académico, por lo que no involucró datos personales ni procedimientos que requirieran aprobación ética. Se respetaron los principios de integridad académica, citación adecuada y uso responsable de la información.

RESULTADOS

Panorama actual de la gobernanza TI en universidades latinoamericanas.

El análisis documental evidencia que la gobernanza TI en universidades de América Latina se caracteriza por estructuras organizacionales tradicionales, baja estandarización de procesos y una limitada integración entre áreas técnicas, administrativas y académicas. La mayoría de las instituciones operan con sistemas heredados, infraestructura híbrida y procesos manuales que dificultan la trazabilidad y la gestión eficiente del riesgo tecnológico. Asimismo, se identifican brechas significativas en políticas de seguridad, actualización de normativas internas y mecanismos de auditoría continua. Estas condiciones generan vulnerabilidades que afectan la continuidad académica, la protección de datos estudiantiles y la capacidad institucional para responder a incidentes de seguridad.

Necesidad de enfoques modernos para la gestión tecnológica.

Los resultados muestran que las universidades enfrentan un incremento sostenido en ciberataques, especialmente ransomware, phishing dirigido y explotación de vulnerabilidades en plataformas educativas. La dependencia de servicios digitales —como aulas virtuales, sistemas de matrícula, repositorios científicos y plataformas administrativas— exige modelos de gobernanza más ágiles, automatizados y orientados a la seguridad. En este contexto, los enfoques tradicionales resultan insuficientes para gestionar la complejidad actual, lo que abre paso a metodologías como DevSecOps.

Impacto de DevSecOps en la gestión del riesgo institucional.

La revisión comparativa revela que la adopción de DevSecOps contribuye significativamente a fortalecer la gestión del riesgo en universidades. Entre los principales impactos identificados se encuentran:

Reducción de vulnerabilidades mediante análisis estático y dinámico integrados en pipelines.

Mayor trazabilidad de cambios, despliegues y eventos de seguridad.

Automatización de controles críticos, como escaneo de dependencias, pruebas de seguridad y validación de configuraciones.

Respuesta más rápida a incidentes, gracias a la integración continua y la retroalimentación inmediata.

Mejor alineación entre equipos, lo que reduce errores humanos y brechas de comunicación.

Estos resultados indican que DevSecOps no solo mejora la seguridad técnica, sino que también fortalece la gobernanza institucional al proporcionar procesos más transparentes y auditables.

Transformación cultural y organizacional.

Uno de los hallazgos más relevantes es que la implementación de DevSecOps requiere una transformación cultural profunda. Las universidades que han avanzado en este enfoque muestran:

Mayor colaboración entre áreas antes aisladas.

Adopción de prácticas de responsabilidad compartida.

Capacitación continua en seguridad y automatización.

Integración de métricas de desempeño orientadas a la seguridad.

Este cambio cultural es clave para que DevSecOps se consolide como un componente de la gobernanza TI y no solo como una práctica técnica.

Beneficios institucionales observados.

El análisis de casos documentados y experiencias institucionales muestra beneficios concretos:

Mejora en la continuidad académica al reducir fallos en sistemas críticos.

Optimización de recursos mediante automatización y reducción de retrabajos.

Cumplimiento normativo más eficiente gracias a auditorías automatizadas.

Mayor confianza institucional en los procesos tecnológicos.

Incremento en la calidad del software académico y de los servicios digitales.

Estos beneficios posicionan a DevSecOps como un catalizador para modernizar la gobernanza TI en la región.

Limitaciones y desafíos identificados.

A pesar de sus ventajas, la adopción de DevSecOps enfrenta desafíos importantes:

Limitaciones presupuestarias para adquirir herramientas especializadas.

Falta de personal capacitado en automatización y seguridad.

Resistencia al cambio por parte de equipos tradicionales.

Infraestructura tecnológica heterogénea y sistemas heredados.

Ausencia de políticas institucionales que respalden la integración de seguridad desde el diseño.

Estos desafíos requieren estrategias institucionales claras y un compromiso sostenido para lograr una implementación efectiva.

APLICACIÓN PRÁCTICA

Implementación de DevSecOps en plataformas académicas institucionales.

Una de las aplicaciones más relevantes de DevSecOps en universidades latinoamericanas es la integración de prácticas de seguridad en el desarrollo y mantenimiento de plataformas académicas, como sistemas de matrícula, aulas virtuales, repositorios institucionales y portales administrativos. La incorporación de análisis estático (SAST) y dinámico (DAST) en los pipelines de integración continua permite identificar vulnerabilidades antes del despliegue, reduciendo fallos en periodos críticos como inscripciones o evaluaciones finales. Asimismo, la automatización de pruebas de seguridad garantiza que cada actualización cumpla con estándares mínimos sin depender exclusivamente de revisiones manuales.

Automatización de controles en infraestructura híbrida universitaria.

Muchas universidades de la región operan con infraestructuras híbridas que combinan servidores locales con servicios en la nube. DevSecOps facilita la automatización de controles de configuración, escaneo de contenedores, verificación de permisos y monitoreo continuo de logs. Herramientas como IaC (Infrastructure as Code) permiten gestionar entornos de laboratorio, aulas virtuales y servicios administrativos con mayor consistencia y trazabilidad. Esto reduce errores humanos, acelera despliegues y fortalece la gobernanza TI mediante auditorías automatizadas.

Integración de DevSecOps en proyectos estudiantiles y de investigación

Otra aplicación práctica consiste en incorporar DevSecOps en proyectos de investigación y desarrollo estudiantil. Los laboratorios de ingeniería, informática y ciencias aplicadas pueden adoptar pipelines seguros para garantizar que los prototipos, aplicaciones y experimentos cumplan con buenas prácticas de seguridad desde su diseño. Esto no solo mejora la calidad de los proyectos, sino que también forma a los estudiantes en competencias altamente demandadas en el mercado laboral.

Fortalecimiento de la gobernanza TI mediante métricas y tableros de control

DevSecOps permite generar métricas clave para la gobernanza TI, como tiempo promedio de detección de vulnerabilidades, frecuencia de despliegues seguros, cumplimiento de políticas internas y niveles de

exposición a riesgos. La creación de tableros de control facilita la toma de decisiones informadas por parte de autoridades universitarias, promoviendo una gestión más transparente y basada en evidencia. Estas métricas fortalecen la rendición de cuentas y permiten evaluar el impacto real de las prácticas DevSecOps en la institución.

Caso práctico: adopción gradual en una universidad latinoamericana

El análisis de experiencias documentadas muestra que la adopción de DevSecOps suele iniciarse con proyectos piloto en áreas críticas, como plataformas de matrícula o sistemas de gestión académica. Posteriormente, se amplía hacia otros servicios institucionales mediante:

1. Capacitación del personal técnico en automatización y seguridad.
2. Definición de políticas institucionales que integren seguridad desde el diseño.
3. Implementación de pipelines seguros en proyectos prioritarios.
4. Monitoreo continuo mediante herramientas de observabilidad.
5. Evaluación periódica de resultados y ajustes iterativos.

Este enfoque gradual permite superar resistencias, optimizar recursos y demostrar beneficios tangibles en corto plazo.

DISCUSIÓN

Los resultados obtenidos permiten comprender que la adopción de DevSecOps en universidades latinoamericanas representa una oportunidad significativa para fortalecer la gobernanza TI, aunque su implementación requiere superar barreras estructurales, culturales y tecnológicas. En primer lugar, se observa que DevSecOps aporta mecanismos concretos para mejorar la gestión del riesgo institucional mediante la automatización de controles, la trazabilidad de procesos y la integración de la seguridad desde las primeras fases del ciclo de vida del software. Este enfoque contrasta con los modelos tradicionales de gobernanza TI, caracterizados por procesos manuales, baja estandarización y respuestas reactivas frente a incidentes.

Asimismo, la evidencia analizada sugiere que DevSecOps contribuye a reducir la brecha entre equipos técnicos y administrativos, promoviendo una cultura de responsabilidad compartida y colaboración continua. Este cambio cultural es especialmente relevante en universidades donde la fragmentación organizacional ha limitado históricamente la eficiencia de los procesos tecnológicos. La integración de

métricas, tableros de control y auditorías automatizadas fortalece la transparencia institucional y facilita la toma de decisiones basada en evidencia, aspectos esenciales para una gobernanza TI moderna.

Sin embargo, la discusión también revela desafíos importantes. La falta de personal especializado, las restricciones presupuestarias y la presencia de infraestructuras híbridas con sistemas heredados dificultan la adopción plena de DevSecOps. Además, la resistencia al cambio cultural y la ausencia de políticas institucionales claras pueden limitar su impacto. A pesar de ello, los casos analizados muestran que una implementación gradual, acompañada de capacitación continua y apoyo directivo, permite obtener beneficios tangibles en plazos razonables.

En síntesis, DevSecOps no solo mejora la seguridad técnica, sino que transforma la gobernanza TI al introducir prácticas más ágiles, auditables y orientadas a la mejora continua. Su adopción en universidades latinoamericanas es viable y estratégica, siempre que se aborde desde una perspectiva integral que combine tecnología, cultura organizacional y políticas institucionales.

CONCLUSIONES

El análisis realizado demuestra que la adopción de DevSecOps constituye una estrategia viable y altamente beneficiosa para fortalecer la gobernanza de Tecnologías de la Información en universidades latinoamericanas. La integración de prácticas de seguridad desde las primeras etapas del ciclo de vida del software, junto con la automatización de controles y la colaboración entre equipos, permite superar las limitaciones de los modelos tradicionales caracterizados por procesos manuales, baja estandarización y respuestas reactivas frente a incidentes. Los resultados evidencian que DevSecOps contribuye a mejorar la gestión del riesgo institucional, incrementar la trazabilidad de procesos, optimizar recursos y garantizar mayor continuidad en los servicios académicos y administrativos.

Asimismo, se concluye que la implementación de DevSecOps no es únicamente un cambio técnico, sino una transformación cultural que requiere compromiso institucional, capacitación continua y políticas claras que respalden la seguridad como responsabilidad compartida. Aunque persisten desafíos relacionados con infraestructura heredada, limitaciones presupuestarias y resistencia al cambio, las experiencias documentadas muestran que una adopción gradual y estratégica permite obtener beneficios tangibles en plazos razonables.

En síntesis, DevSecOps representa un marco integral para modernizar la gobernanza TI en universidades latinoamericanas, promoviendo modelos de gestión más ágiles, transparentes y orientados a la mejora continua. Su incorporación fortalece la resiliencia institucional y posiciona a las universidades para enfrentar con mayor solidez los retos tecnológicos y de seguridad del entorno digital contemporáneo.

REFERENCIAS BIBLIOGRAFICAS

Al-Breiki, H., Al-Qayoudhi, W., & Al-Khanjari, Z. (2022). Integrating DevSecOps practices into higher education software development projects. *International Journal of Advanced Computer Science and Applications,* 13, 45–53. https://doi.org/10.14569/IJACSA.2022.0130406

Almorsy, M., Grundy, J., & Müller, I. (2018). An analysis of the cloud computing security problem. *Journal of Cloud Computing*, 7, 1–16. https://doi.org/10.1186/s13677-018-0123-1

Bass, L., Weber, I., & Zhu, L. (2019). *DevOps: A software architect's perspective* (2nd ed.). Addison-Wesley.

Bhandari, S., & Gupta, S. (2021). DevSecOps: A systematic literature review. *Journal of Systems and Software,* 180, 111028. https://doi.org/10.1016/j.jss.2021.111028

Cruz, J., & García, M. (2023). Gobernanza de TI en universidades latinoamericanas: Retos y oportunidades en la era digital. *Revista Iberoamericana de Tecnología Educativa,* 19, 55–72. https://doi.org/10.1344/rite2023.19.2.55

Fitzgerald, B., & Stol, K. (2020*). Continuous software engineering: A roadmap and agenda.* Springer. https://doi.org/10.1007/978-3-030-39306-9

Kim, G., Humble, J., Debois, P., & Willis, J. (2021). *The DevOps handbook: How to create world-class agility, reliability, and security in technology organizations* (2nd ed.). IT Revolution Press.

Mohan, A., & Othmane, L. B. (2020). Security automation in DevSecOps pipelines: A systematic review. *Computers & Security, 96*, 101935. https://doi.org/10.106/j.cose.2020.101935

NIST. (2022). *Secure software development framework (SSDF): Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-218

Santos, R., & Pereira, L. (2024). Digital transformation and IT governance in Latin American higher education institutions. *Journal of Higher Education Policy and Management,* 46, 78–95. https://doi.org/10.1080/1360080X.2023.2256789

Sharma, P., & Gupta, R. (2022). DevSecOps adoption challenges in developing countries: A multi-case analysis. *Information and Computer Security*, 30, 763–781. https://doi.org/10.1108/ICS-02-2022-0021