DOI: https://doi.org/10.56124/encriptar.v6i12.003

Propuesta de aplicación de la metodología DevOps con un enfoque de seguridad

Luis Antonio Iñiguez Vergara, Jorge Arun Zambrano Cedeño, José Manuel Morán Tubay
Universidad Técnica de Manabí

Resumen

DevOps incluye un procedimiento de trabajo cooperativo entre los grupos de giro de eventos y tareas para abordar el ciclo de mejora del producto de forma eficaz, garantizando ciclos coordinados y seguros, además de trabajar con una transmisión incesante y pensando en la naturaleza del resultado final.Esta investigación se realizó con el objetivo de desarrollar una propuesta de aplicación de la metodología DevOps con un enfoque de seguridad en la Universidad Técnica de Manabí, puesto que el departamento de TI no cuenta con las seguridades ni estrategias adecuadas para identificar, consolidar y manejar vulnerabilidades halladas en el ciclo de integración y despliegue continuo dentro de la Universidad. La metodología se centra en un diseño no experimental, mismo que se caracteriza porque no se manipulan directamente sus variables, además se trabajó bajo una investigación cuantitativa en la que se aplicó encuestas a los involucrados, la población fue el personal del área de TIC de la Universidad Técnica de Manabí. Entre los resultados obtenidos, destacó que el 86% tiene un nivel bajo en el manejo de herramientas de automatización para DevOps, así mismo se pudo constatar que el 42,86% tiene un conocimiento medio, y 28,57% un bajo conocimiento de DevOps, esto generó un interés significativo hacia la adopción de la metodología, concluyendo que la aplicación de una propuesta para utilizar DevOps con un enfoque de seguridad en la Universidad Técnica de Manabí, permitirá agilizar los ciclos de vida del desarrollo, posicionarse competitivamente y adaptarse al ritmo de las demandas de sus clientes.
Palabras claves: DevOps, Metodología, seguridad.

Proposal for the application of the DevOps methodology with a security approach

Abstract

DevOps includes a cooperative work procedure between the groups of turning events and tasks to address the product improvement cycle effectively, ensuring coordinated and secure cycles, in addition to working with a relentless transmission and thinking about the nature of the final result. This research was conducted with the aim of developing a proposal to apply the DevOps methodology with a security approach at the Technical University of Manabi, since the IT department does not have the security or adequate strategies to identify, consolidate and manage vulnerabilities found in the cycle of integration and continuous deployment within the University. The methodology focuses on a non-experimental design, which is characterized by the fact that its variables are not directly manipulated, also worked under a quantitative research in which surveys were applied to those involved, the population was the staff of the ICT area of the Technical University of Manabi. Among the results obtained, it was highlighted that 86% have a low level in the management of automation tools for DevOps, likewise it was found that 42.86% have a medium knowledge, and 28.57% have a low knowledge of DevOps, this generated a significant interest towards the adoption of the methodology, concluding that the implementation of a proposal to use DevOps with a security approach at the Technical University of Manabi, will allow speeding up the development life cycles, position itself competitively and adapt to the pace of the demands of its customers.

Keyworks: DevOps, methodology, security

Introducción

En el actual contexto, la seguridad informática ha adquirido un rol central en el ámbito de la computación, dado su impacto en el respaldo del abastecimiento computacional y en todo lo concerniente a la documentación relacionada con la Seguridad Informática (S.I. en adelante). Es por ello que las instituciones dependen en gran medida de la tecnología y los sistemas informáticos para llevar a cabo de manera eficiente sus actividades diarias (Guerrero, 2022).

A lo largo del tiempo, se han desarrollado protocolos, estándares, herramientas, metodologías, reglas y leyes que permitan a las empresas expandirse al ritmo del mercado mediante el uso de la tecnología, optimizando recursos y, con ello, minimizando los posibles problemas de seguridad de software o de documentación. Es importante destacar que, según Ramón (2018), la seguridad informática "abarca software, bases de datos, metadatos, archivos y cualquier elemento que la empresa valore y que represente un riesgo si cae en manos de terceros; este tipo de documentación se conoce como documentación privilegiada o confidencial" (p. 19).

La pandemia originada por el COVID-19 ha llevado a un gran número de negocios a adaptarse al comercio virtual o electrónico, lo que resultó en un aumento significativo de las ventas, como lo reporta el Diario Primicias (2021), que señala un incremento del 20% entre 2019 y 2020, pasando de USD 1.900 millones a USD 2.300 millones (p.1). Si bien esto fue beneficioso para los emprendedores y las pymes, también resultó en una lamentable reducción de personal y la necesidad de mejorar la publicidad de los productos o servicios para mantener las ventas. En este sentido, el cierre de las tiendas físicas es una realidad que se ha manifestado y continúa vigente en Ecuador, dependiendo de la coyuntura de los diferentes sectores comerciales (Sumba, Almendariz, Baque y Aliatis, 2020).

La migración de procesos manuales a automatizados resulta beneficiosa para las empresas dedicadas al desarrollo de software, ya que implica una mayor eficiencia operativa, digitalización en lugar de acumulación de documentos, reducción de errores, operaciones ininterrumpidas, seguridad mejorada, mayor confiabilidad, optimización de los procesos de negocios, capacidad de respuesta rápida y la posibilidad de realizar cambios en los planes en cualquier punto del proyecto. Esto asegura que las tareas se ejecuten de manera continua y evita que se ingresen datos incorrectos (Pumasunta, 2020).

El uso de plataformas de comercio electrónico o e-commerce se refiere a cualquier aplicación en línea que permite acceder a información integral de productos o servicios a nivel global, facilitando alianzas entre compradores, proveedores y otras partes involucradas en el ciclo comercial. Estas plataformas son útiles para todos los sectores, incluidos el financiero, industrial, transporte e incluso las instituciones gubernamentales, que buscan intercambiar datos. Algunos aspectos prácticos que ofrece esta alternativa de comercio a los clientes son la comodidad, ahorro de tiempo, diversos medios de pago y catálogos más amplios para conocer los productos, lo que permite realizar compras en línea independientemente de la ubicación geográfica de la empresa (Carrera, Rodríguez y Mancilla, 2019).

En el ámbito de la innovación de datos, se espera una reacción rápida a las necesidades de los clientes, junto con una ayuda constante, segura y sin contratiempos. Esto implica un compromiso entre la confiabilidad y el cambio. A menudo, una respuesta que permite cambios continuos (como las metodologías ágiles) sin tener en cuenta la confiabilidad en la gestión operativa o la comunicación entre desarrollo y operaciones puede no ser suficiente. En este sentido, el desarrollo DevOps, según Wiley y Sons (2019), "propone

DOI: https://doi.org/10.56124/encriptar.v6i12.003

una visión integrada en el desarrollo del software que permite implementar cambios de manera rápida y segura, garantizando la confiabilidad en las operaciones (lanzamiento del software, monitoreo y análisis de incidentes)" (p.34).

DevOps implica una cooperación entre los equipos de Desarrollo y Operaciones para supervisar el progreso de la programación de manera coordinada, abarcando todo el ciclo de vida del producto y centrándose en la suavización y obtención de procesos, así como en el avance en el transporte constante y una mejor calidad. Es importante tener en cuenta que DevOps no se refiere a una herramienta, lenguaje o tecnología en particular, sino a un esfuerzo coordinado entre los equipos de desarrollo (Desarrollo) y operaciones (Operaciones) en función de las normas de habilidad. Cada organización adapta las prácticas de DevOps según su estructura y necesidades, utilizando diferentes herramientas para automatizar los procesos y ciclos de desarrollo, lo que permite optimizar los procesos (UNIR, 2023).

Esta metodología ha demostrado ser exitosa para empresas como Amazon, Facebook, Netflix, empresas de servicios financieros como Barclays Bank y empresas de medios de comunicación como Sony Pictures (Orozco, Pardo y Zúñiga, 2022). La metodología consta de fases: planificación, codificación, construcción y pruebas, formando el proceso de integración continua, responsable de planificar y construir el código, y las fases del proceso de despliegue o entrega continua: lanzamiento, despliegue, operación y monitoreo, responsables de la implementación del software en producción (Jaramillo, 2022).

La integración de DevOps en el entorno académico aún es poco común, y hasta el momento de esta investigación no se han identificado estudios o artículos similares en el contexto de instituciones educativas de educación superior en Ecuador. Este fenómeno sugiere una brecha en la adopción de DevOps en el ámbito académico y plantea la pregunta sobre las posibles razones detrás de esta falta de implementación, especialmente en el contexto específico de entidades educativas en el país (Prosper Heredia & Vargas Lombardo, 2020).

Es importante destacar que el estudio se lleva a cabo en la Universidad Técnica de Manabí (UTM) debido a la presencia de una problemática que es la falta de una metodología ágil que permita integrar el desarrollo de software en el departamento de TI. Existen demoras en el desarrollo de artefactos que se implementan continuamente, lo que se debe a dos factores: una iniciativa interna por mejorar los servicios digitales para los usuarios y la regulación por parte del CES (Consejo de Educación Superior), que envía implementaciones de forma esporádica, políticas a las universidades, y esto tiene afectación directa en los servicios digitales que están en producción. La UTM realiza las actualizaciones a sus productos de software sin un control automático de versiones y sin tomar en cuenta los riesgos de seguridad que implica actualizar los artefactos o arquitectura sin el apoyo de herramientas de análisis de código.

2. Materiales y Métodos

2.1. Diseño de investigación

El diseño del estudio fue no experimental el cual, como lo indican Agudelo, Aigneren y Ruiz (2010), se caracteriza porque las variables no son manipuladas. Además, es cuantitativo porque busca evaluar las variables de estudio con la información que se recolecte por medio de las encuestas aplicadas a los involucrados, la tabulación, análisis estadístico e interpretación de las mismas ; al respecto Angulo (2018) expresa que “es cuantitativa, ya que realiza la recogida y análisis de la información para responder a las

preguntas de investigación mediante la estimación matemática, el recuento y, con frecuencia, la utilización de mediciones para establecer con precisión ejemplos de conducta en una población.” (p. 14).

2.2. Tipo de investigación

El tipo de estudio seleccionado es descriptivo y de campo, el primero porque dio a conocer las características que se observaron en la situación de la problemática, con la finalidad de delimitar los hechos que se han suscitado en la problemática.

Investigación de campo porque mediante este tipo de investigación se pudo obtener información por parte de los encuestados, con este tipo de investigación se obtiene información relevante. Así mismo, implica una simultaneidad entre la narración de los datos narrativos y el análisis de los mismos.

2.3. Materiales

Los materiales, equipos e instrumentos empleados en la investigación consistieron en recursos materiales como papel, bolígrafos, acceso a internet, publicaciones periódicas y una computadora portátil. Por otro lado, los recursos humanos comprendieron los miembros de la población investigada, quienes participaron activamente durante el estudio mediante la aceptación y aplicación de los instrumentos de recolección de datos, específicamente siete encuestas administradas al equipo de la Dirección de Tecnologías de la Información y Comunicación (TIC) de la Universidad Técnica de Manabí (UTM), las cuales fueron evaluadas utilizando la escala de Likert.

El método utilizado fue el inductivo-deductivo, que se caracteriza por integrar lo particular hasta alcanzar lo general y viceversa, con el propósito de relacionar eventos específicos. Este enfoque, que incluye la observación, permitió el análisis de los resultados de las investigaciones empíricas, facilitando la formulación de generalizaciones, la construcción de alternativas de solución para la problemática identificada, y, por ende, la elaboración de conclusiones y recomendaciones.

2.4. Métodos y procedimientos

Esta etapa se inicia con la búsqueda exhaustiva de estudios previos aplicados en entornos educativos similares. Con los elementos obtenidos, se procede a la construcción de un modelo de métrica de seguridad destinado al proceso de desarrollo de software. Posteriormente, se llevará a cabo una discusión detallada y un análisis profundo de los indicadores adquiridos mediante la métrica propuesta.

El desarrollo del trabajo implica diversas etapas, que se centrarán en el análisis y la evaluación de las metodologías aplicadas en las aplicaciones. A continuación, se detallan los pasos a seguir:

Investigación bibliográfica de trabajos relacionados con estudios similares.

Recopilación y procesamiento de datos obtenidos de las diferentes normas, estándares y métodos identificados.

Establecimiento de un análisis comparativo de las diversas métricas utilizadas en el desarrollo de aplicaciones.

Análisis y verificación de los datos obtenidos.

Elaboración de los resultados, discusión y conclusiones.

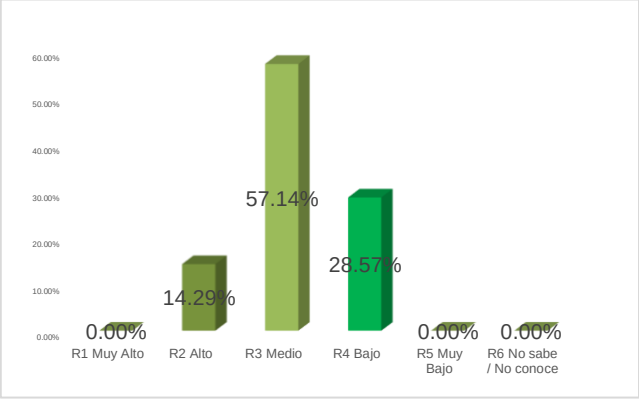
La población de estudio estuvo compuesta por siete miembros del equipo del área de Tecnologías de la Información y Comunicación (TIC) de la Universidad Técnica de Manabí.

DOI: https://doi.org/10.56124/encriptar.v6i12.003

3. Resultados

Una vez aplicados los instrumentos (Anexo 1) de investigación al personal del área de TIC de la UTM, se pudo obtener información de relevancia relacionada con el nivel de conocimiento, aplicación y aprobación de las metodologías agiles, y si sería oportuna la creación de una propuesta para implementar la metodología DevOps, los resultados obtenidos son:

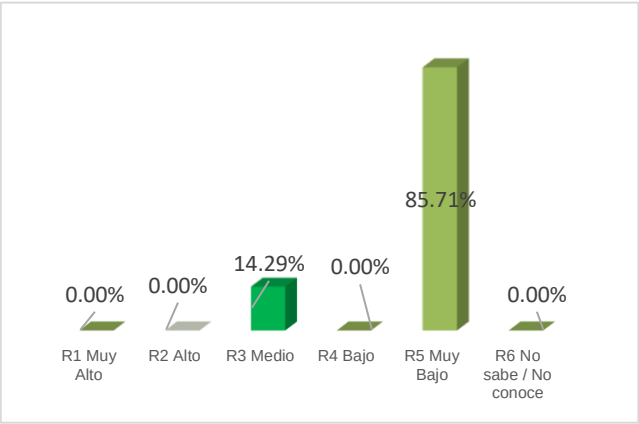
Figura 1. Conocimiento de metodologías ágiles



Fuente: Encuestas realizadas al personal del equipo de TIC de UTM (2023)

Respecto al conocimiento de metodologías ágiles, el 57,14% de los encuestados tiene un conocimiento medio, el 28,57% tiene un conocimiento bajo, y el 14,29% tiene un conocimiento alto. Estos resultados sugieren que la mayoría de los encuestados tienen un conocimiento promedio de metodologías ágiles, mientras que una proporción significativa tiene un conocimiento bajo. Es posible que se necesite más capacitación o educación para mejorar el nivel de conocimiento en este campo.

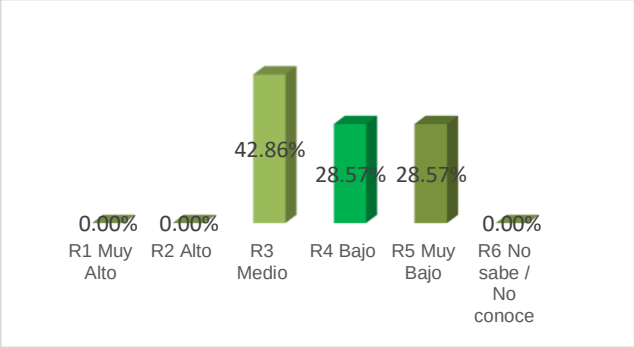
Figura 2. Nivel de experiencia de metodologías ágiles



Fuente: Encuestas realizadas al personal del equipo de TIC, UTM (2023)

En cuanto a la experiencia con metodologías ágiles en el lugar de trabajo, el 87,71% indicó que tienen una experiencia muy baja, mientras que el 14,29% indicó que tiene una experiencia media. Estos resultados sugieren que la mayoría de los encuestados tienen una experiencia limitada o nula en el uso de metodologías ágiles en su entorno laboral. Podría ser necesario implementar programas de formación o prácticas para mejorar la experiencia en este ámbito.

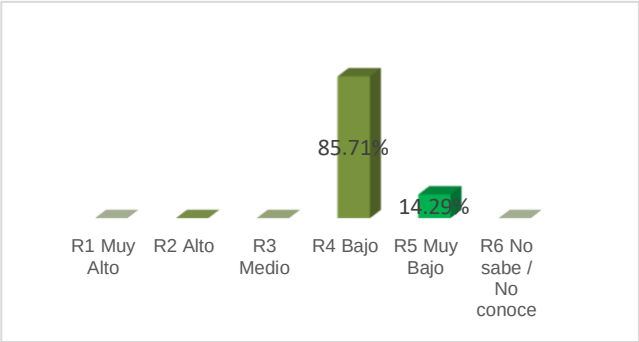
Figura 3. Conocimiento de metodología DevOps



Fuente: Encuestas realizadas al personal del equipo de TIC, UTM (2023)

En relación con el conocimiento de DevOps, el 42,86% tiene un conocimiento medio, el 28,57% tiene un conocimiento bajo, y otro 28,57% indicó tener un conocimiento muy bajo. Estos resultados muestran que hay una variedad de niveles de conocimiento en DevOps, pero la mayoría de los encuestados tienen un conocimiento medio o bajo. Es posible que se requieran más recursos de formación o capacitación en DevOps para mejorar la competencia en este campo.

Figura 4. Manejo de herramientas DevOps

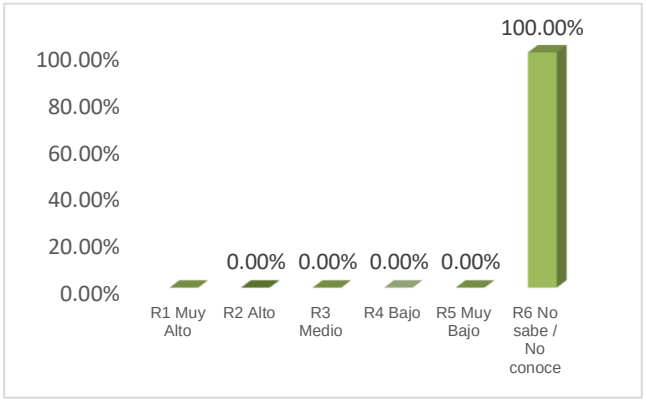


Fuente: Encuestas realizadas al personal del equipo de TIC, UTM (2023)

Respecto al manejo de herramientas de automatización DevOps, el 85,71% indicó un nivel bajo y el 14,29% indicó un nivel muy bajo. Estos resultados sugieren que la mayoría de los encuestados tienen una capacidad limitada para manejar herramientas de automatización en el contexto de DevOps. Se podría necesitar una formación específica en herramientas de automatización para mejorar las habilidades en este aspecto.

DOI: https://doi.org/10.56124/encriptar.v6i12.003

Figura 5. Conocimiento en desarrollo de software



Fuente: Encuestas realizadas al personal del equipo de TIC, UTM (2023)

En cuanto al nivel de conocimiento en el desarrollo de software con metodologías de desarrollo seguro, el 100,00% indicó que no sabe o no conoce. Este resultado sugiere que ninguno de los encuestados tiene conocimiento sobre el desarrollo de software con metodologías de desarrollo seguro. Podría ser esencial proporcionar formación y recursos educativos sobre este tema para mejorar la comprensión y la aplicación de prácticas de desarrollo seguro.

4. Discusión

Según los resultados obtenidos de las encuestas, se puede conocer que la mayoría de los involucrados en el estudio no tiene conocimiento en metodologías agiles, ni en el manejo de herramientas automatizadas DevOps, tal como lo afirmaron Wiley y Sons (2019) en su investigación realizada acerca de la importancia de DevOps; así mismo expresaron que tienen cero conocimientos en el desarrollo de software con metodologías de desarrollo seguro. Estos resultados dejan clara la necesidad de realizar una propuesta de solución al problema dirigidos a los miembros del equipo del área de TIC de La Universidad Técnica de Manabí, para que puedan adoptar una metodología que le permita integrar el desarrollo de software y las operaciones con un enfoque de seguridad en cada una de las etapas del ciclo de vida del desarrollo del software.

A través de los resultados obtenidos, se propone una alternativa de solución a la problemática presente con lo cual se espera cubrir las brechas de seguridad que pueden ser utilizadas para comprometer el correcto funcionamiento de una aplicación. Partiendo de esto, se construyó este documento, el cual cuenta con la propuesta de implementar DevOps, es decir, una estrategia de seguridad integral, flexible y adaptable al tamaño de la empresa que permita integrar el desarrollo de software y las operaciones con un enfoque de seguridad en cada una de las etapas del ciclo de vida del desarrollo del software, así como lo indica Jaramillo (2022) en su trabajo denominado “Estrategia de seguridad para el manejo de vulnerabilidades en el ciclo de integración y despliegue continúo en aplicaciones web desarrolladas bajo la metodología DevOps”. De igual forma se podrá alcanzar el nivel de madurez del equipo de seguridad que la desee implementar. Se espera que a través de la propuesta de metodologías DevOps con enfoque de seguridad se logre la entrega continua con un enfoque a la seguridad en el proceso de desarrollo de software y puesta en producción en la Universidad Técnica de Manabí.

5. Propuesta

Enfoque de la propuesta

Cabe recalcar que la propuesta de implementación de metodologías DevOps con un enfoque integral en seguridad no sólo busca cerrar las brechas de seguridad existentes, sino también establecer una nueva norma de desarrollo de software que asegure no solo la continuidad del proceso, sino una entrega continua de aplicaciones con estándares de seguridad robustos.

El enfoque de seguridad en la propuesta de DevOps para el área de TIC de la Universidad Técnica de Manabí implica varios aspectos cruciales que deben ser considerados y abordados de manera integral. Entre ellos se encuentran:

Integración temprana de la seguridad: La seguridad debe ser parte integral de todo el proceso de desarrollo y despliegue de software desde el inicio, incorporándola en cada etapa del ciclo de vida de desarrollo de software, desde la planificación hasta la operación.

Pruebas de seguridad automatizadas: Se deben implementar herramientas y técnicas para la detección temprana de vulnerabilidades en el código y configuraciones de sistemas, realizando pruebas automatizadas de seguridad de manera continua durante el desarrollo y despliegue.

Gestión de identidades y accesos: Es fundamental implementar controles de acceso adecuados para proteger los recursos de información, asegurando que solo los usuarios autorizados tengan acceso a los sistemas y datos pertinentes.

Monitorización continua de la seguridad: Se debe establecer un sistema de monitorización y detección de amenazas en tiempo real para identificar y responder a posibles incidentes de seguridad de manera proactiva.

Políticas de seguridad coherentes: Se deben establecer y hacer cumplir políticas de seguridad claras y coherentes en toda la organización, abordando aspectos como la gestión de parches, la configuración segura de sistemas y la gestión de incidentes.

Cultura de seguridad: Se debe promover una cultura de seguridad dentro del equipo de desarrollo y toda la organización, fomentando la conciencia sobre las amenazas y buenas prácticas de seguridad, así como la responsabilidad compartida en la protección de los activos de información.

Auditoría y cumplimiento: Es necesario establecer mecanismos de auditoría interna y externa para evaluar el cumplimiento de las políticas de seguridad y normativas relevantes, así como realizar evaluaciones periódicas de la postura de seguridad de los sistemas de información.

En resumen, el enfoque de seguridad debe ser integral, abordando aspectos técnicos, procesuales y culturales para garantizar la protección adecuada de los activos de información y mantener la confianza de los usuarios y partes interesadas.

6. Metodología propuesta a aplicarse

La adaptabilidad inherente a DevOps permitirá a la Universidad Técnica de Manabí ajustar esta metodología según sus necesidades específicas, independientemente del tamaño de la institución o el nivel de experiencia del equipo de seguridad. Se aspira a que mediante esta propuesta no sólo se fortalezca la seguridad del entorno digital de la institución, sino que también impulse una eficiencia en la producción de software,

DOI: https://doi.org/10.56124/encriptar.v6i12.003

transformando positivamente las operaciones y el manejo de vulnerabilidades a lo largo del ciclo de vida del desarrollo.

A continuación, se detallan las fases del diseño de la propuesta DevOps

1. Establecer una cultura dentro de la compañía
2. Implementación de DevOps
3. Prácticas DevOps
4. Técnicas y Herramientas DevOps
5. Beneficios de DevOps
6. Gestión del Cambio
7. Barreras DevOps
8. Post-Implementación de DevOps

Establecer una cultura dentro de la compañía

La cultura DevOps se ha convertido en una de las tendencias más populares en el desarrollo de software, por ello se ha propuesto que se cree una cultura en el departamento de TIC de la Universidad Técnica de Manabí con el fin de combinar la colaboración, la integración continua, la entrega continua y la automatización para mejorar la calidad y la eficiencia del software.

Implementación de DevOps

La implementación de DevOps en la UTM implica la adopción de un conjunto de procesos consolidados y automatizados diseñados para promover el Feedback rápido y ágil entre los equipos de desarrollo y operaciones. Esto conlleva a la reducción de los plazos de entrega de software, facilitando un ciclo de mejoras continuas. Además, para garantizar la eficiencia en la reducción de los tiempos de entrega, es necesario llevar a cabo una revisión continua para asegurar que ninguna funcionalidad o característica importante sea pasada por alto. Es importante destacar que la seguridad también juega un papel fundamental en este proceso, lo que da paso al concepto de DevSecOps, integrando la seguridad en todas las etapas del ciclo de vida del desarrollo de software.

La necesidad de seguridad en el desarrollo

La necesidad de seguridad en el desarrollo dentro del contexto de la metodología DevOps en una universidad es fundamental para garantizar la integridad y confiabilidad del software entregado a los usuarios. A menudo, los equipos de desarrollo pueden tener una visión errónea de que priorizar la seguridad conlleva más desventajas que beneficios, ya que su enfoque principal puede estar en cumplir con los plazos y ofrecer nuevas funcionalidades. Sin embargo, la seguridad no puede subestimarse, ya que una vulnerabilidad podría tener repercusiones graves para el proyecto y la organización, incluyendo la filtración de datos confidenciales como información de identificación personal (PII), contraseñas y números de cuentas, lo que podría resultar en sanciones por incumplimiento de la legislación de protección de datos personales.

Estas vulnerabilidades suelen surgir debido a errores en el código o en su diseño. Algunas de estas situaciones pueden ser conocidas y haber ocurrido previamente, mientras que otras pueden ser nuevas y plantear desafíos adicionales. Además, la complejidad aumenta cuando hay dependencias de software de terceros, ya que a menudo no se pueden garantizar que no existan vulnerabilidades. Por lo tanto, es crucial que los equipos de desarrollo de la UTM adopten prácticas de seguridad proactivas y realicen pruebas exhaustivas para identificar y mitigar posibles riesgos de seguridad en todas las etapas del ciclo de vida del desarrollo de software.

Desplazar la seguridad al inicio del proyecto

En el contexto de la aplicación de metodología DevOps en una universidad, específicamente en la UTM, la velocidad para entregar partes del software para pruebas de usuario se ha vuelto fundamental, priorizando la satisfacción de las necesidades del cliente. Aunque DevOps no tenía la intención de descuidar la seguridad, el entorno existente contribuyó al distanciamiento entre los equipos de desarrollo y operaciones, creando un silo de seguridad separado.

La introducción de DevSecOps busca abordar esta situación, promoviendo la integración de la seguridad desde el inicio del proyecto y a lo largo de todas sus etapas, fomentando una cultura de responsabilidad compartida en todas las áreas de desarrollo. Este enfoque implica desplazar hacia el inicio del proyecto la implementación de medidas de seguridad, alineándose así con las nuevas metodologías y facilitando la incorporación natural de buenas prácticas de seguridad en el proceso de desarrollo.

Anadir la capa de seguridad a DevOps

Compartir la responsabilidad de las tareas relacionadas con la seguridad es primordial, pero en la mayoría de las ocasiones, los miembros del equipo de desarrollo de la Universidad Técnica de Manabí no pueden estar formándose de manera continua, ya que esto conlleva una dedicación plena. Incluir a un experto en seguridad que esté actualizado en los vectores de ataque y las últimas técnicas de desarrollo para paliarlos es vital, para que pueda trasladar estos conocimientos al resto del equipo y promover una cultura de colaboración con el equipo de seguridad.

Contar con las herramientas apropiadas

En el contexto de la metodología DevOps en la UTM, contar con las herramientas adecuadas es crucial para garantizar la calidad y seguridad del código desarrollado. Además de los conocimientos internos del equipo, las herramientas de terceros son aliados importantes que evolucionan constantemente para ofrecer servicios más avanzados y automatizados. Estas herramientas proporcionan resultados a través de interfaces intuitivas o notificaciones directas de incidencias, permitiendo obtener Feedback en tiempo real.

Entre las herramientas disponibles, se encuentran las SAST (Static Application Security Testing), que analizan el código estático en busca de vulnerabilidades como sobrecarga de buffer o inyecciones SQL. Estas herramientas pueden integrarse con el entorno de desarrollo integrado (IDE) para ofrecer Feedback instantáneo mientras se escribe el código, lo que ayuda a prevenir errores desde el inicio del proceso de desarrollo. Es importante tener en cuenta que las SAST pueden generar falsos positivos, por lo que es necesario contar con la capacidad de descartarlos para evitar distracciones innecesarias.

Por otro lado, las herramientas DAST (Dynamic Application Security Testing) adoptan un enfoque de "caja negra" y realizan pruebas durante la ejecución de la aplicación para identificar posibles vulnerabilidades conocidas, como malware, configuraciones inseguras o inyecciones SQL. Estas herramientas suelen utilizarse en etapas más avanzadas del proyecto, ya que operan durante el tiempo de ejecución de la aplicación, brindando una evaluación más completa de su seguridad.

Verificar las dependencias del software

En el marco de la metodología DevOps en una universidad, es esencial verificar las dependencias del software, ya que las bibliotecas de código abierto y otros componentes pueden representar una fuente potencial de vulnerabilidades. En las etapas iniciales del desarrollo, es recomendable emplear herramientas de Análisis de Componentes de

DOI: https://doi.org/10.56124/encriptar.v6i12.003

Software (SCA, por sus siglas en inglés), las cuales examinan los componentes en busca de posibles vulnerabilidades.

Esta tarea debe ser responsabilidad de los desarrolladores, quienes deben asegurarse de mantener actualizadas estas herramientas para detectar las últimas vulnerabilidades conocidas. Mantener un proceso regular de verificación de dependencias del software contribuye significativamente a fortalecer la seguridad del proyecto y reducir el riesgo de explotación de vulnerabilidades en el software desarrollado.

Integración y entrega continua (CI/CD)

La demanda de los servicios digitales se ha disparado desde el 2020 y se espera que solo sea el comienzo de un prometedor periodo. Las organizaciones se encuentran en una competencia constante, donde diferenciarse de la competencia es indispensable, y la velocidad de lanzamientos para adelantarse a otros se ha convertido en habitual.

Para ello, se ha propuesto adoptar prácticas DevOps, como la integración y entrega continua, "CI/CD" (Continuous Integration and Continuous Delivery) en la UTM. Se trata de una serie de procesos relacionados que permite crear software de calidad a través de un conjunto de técnicas alineadas y automatizadas. El conjunto de estas prácticas, garantizan una colaboración más eficaz junto a una mayor eficacia de todo del ciclo de vida de desarrollo del software. Esto se traduce en una capacidad mejorada para entregar nuevas funcionalidades y actualizaciones de manera rápida, segura y consistente, lo que a su vez mejora la satisfacción del cliente y la competitividad de la organización en el mercado digital.

Agilidad en el desarrollo

Dentro del contexto de la metodología DevOps en la UTM, la práctica de Integración Continua (CI) juega un papel fundamental en agilizar el proceso de desarrollo de software. Esta práctica permite a múltiples desarrolladores trabajar en diferentes módulos de una misma aplicación de forma concurrente y enviar sus contribuciones a un repositorio compartido al finalizar su trabajo. Posteriormente, se realiza una verificación de la compilación del código, y en caso de que esta falle, se notifica al equipo correspondiente para corregir los errores de manera rápida y eficiente.

La Integración Continua ayuda a prevenir el fenómeno conocido como “merge hell”, que ocurre cuando diferentes desarrolladores realizan cambios que afectan la compilación de la línea principal de desarrollo. Al realizar fusiones de manera regular, los equipos pueden completar el software de manera más rápida y eficiente, garantizando siempre una compilación actualizada y correcta. Esto ahorra tiempo y recursos, al tiempo que mejora la calidad y la consistencia del código entregado.

Tipo de actores/ usuarios

En el contexto de la propuesta de DevOps para el área de TIC de la Universidad Técnica de Manabí, se pueden identificar varios tipos de actores o usuarios con responsabilidades específicas en relación con la seguridad:

Equipo de desarrollo: Este grupo está compuesto por desarrolladores de software y otros profesionales involucrados en la creación y mantenimiento de aplicaciones. Sus responsabilidades incluyen escribir código seguro, realizar pruebas de seguridad, corregir vulnerabilidades y seguir prácticas de desarrollo seguro durante todo el ciclo de vida del software.

Equipo de operaciones: Este equipo se encarga de implementar y mantener los sistemas y aplicaciones en producción. Sus responsabilidades incluyen configurar y administrar de manera segura los entornos de producción, aplicar parches de seguridad,

monitorear la infraestructura en busca de posibles amenazas y responder a incidentes de seguridad.

Equipo de seguridad: Este grupo se dedica específicamente a la seguridad de la información y desempeña un papel crucial en la protección de los activos de información de la universidad. Sus responsabilidades incluyen establecer políticas y procedimientos de seguridad, realizar evaluaciones de riesgos y vulnerabilidades, implementar controles de seguridad, y proporcionar formación y concienciación sobre seguridad a otros equipos.

Usuarios finales: Estos son los miembros de la comunidad universitaria que utilizan los sistemas y servicios de TIC en su trabajo diario. Su responsabilidad principal es seguir las políticas de seguridad establecidas, proteger sus credenciales de acceso y reportar cualquier incidente de seguridad que puedan encontrar.

Directivos y responsables de toma de decisiones: Este grupo tiene la responsabilidad de establecer la visión y las prioridades en materia de seguridad de la información en la universidad. Deben asegurarse de asignar recursos adecuados para la implementación de medidas de seguridad, tomar decisiones estratégicas relacionadas con la gestión de riesgos y apoyar las iniciativas de seguridad en toda la organización.

Cada uno de estos actores tiene un papel fundamental en la protección de la seguridad de la información en la Universidad Técnica de Manabí, y es importante que trabajen de manera colaborativa y coordinada para garantizar un enfoque integral de seguridad en la propuesta de DevOps.

Beneficios de CI/CD

Los beneficios de la integración y entrega continuas (CI/CD) en el marco de la metodología DevOps en la Universidad Técnica de Manabí, son significativos y contribuyen al éxito de los proyectos de desarrollo de software. Algunos de estos beneficios incluyen:

1. Reducción del tiempo de desarrollo: CI/CD permite acortar considerablemente el tiempo necesario para desarrollar aplicaciones, lo que otorga a la UTM es una ventaja competitiva sobre sus competidores al poder lanzar productos al mercado de manera más rápida.
2. Iteración continua y lanzamiento de nuevas funciones: La implementación de CI/CD facilita la iteración y el lanzamiento continuo de nuevas funciones. Esto significa que los equipos pueden agregar y mejorar funciones de manera regular y rápida, manteniendo a todos trabajando con la misma versión del código.
3. Aumento de la eficiencia del equipo: Con la implementación continua, los equipos pueden dedicar menos tiempo a esperar los resultados de las pruebas y más tiempo al desarrollo real. Esto acelera el Feedback de los usuarios y ayuda a mejorar los resultados comerciales.
4. Mejora de la calidad del software: La automatización de pruebas y la entrega continua garantizan un alto nivel de calidad en el software entregado, ya que los errores se detectan y corrigen rápidamente durante el proceso de desarrollo.

*Nota. El pase emergente a producción que puede tener el escenario que el CES solicite un cambio con tiempos muy cortos para el desarrollo.

7. Propuesta de mejora en el departamento de TIC de la UTM

En la actualidad el equipo de Ti está conformado por 1 administrador de bases de datos, un Project manager, 2 personas para la Infraestructura tecnológica, un director de TI, y 2 desarrolladores, sin embargo, para obtener más eficiencia y por lo tanto mejores

DOI: https://doi.org/10.56124/encriptar.v6i12.003

resultados, se propone que el personal debe ser el siguiente para el correcto desarrollo de las actividades.

Gerente de Proyecto / Líder de Equipo: Este individuo es responsable de liderar el proyecto de implementación de DevOps en la universidad. Coordina las actividades del equipo, establece objetivos y plazos, y se comunica con las partes interesadas.

Desarrolladores de Software: Son responsables de escribir y mantener el código de las aplicaciones y sistemas utilizados en la universidad. En el contexto de DevOps, los desarrolladores deben colaborar estrechamente con los equipos de operaciones para garantizar una entrega continua y una integración sin problemas de código.

Ingenieros de Operaciones (Ops): Estos profesionales se encargan de la gestión y operación de los sistemas de TI en la universidad. Trabajan en la automatización de infraestructuras, monitoreo y escalado automático, y despliegue de aplicaciones en los entornos de producción.

Administradores de Sistemas: Son responsables de la configuración, mantenimiento y administración de los servidores, redes y otros recursos de infraestructura utilizados por la universidad. Trabajan en estrecha colaboración con los ingenieros de operaciones para garantizar la disponibilidad y el rendimiento de los sistemas.

QA / Control de Calidad: Este equipo se encarga de garantizar la calidad del software desarrollado y desplegado en la universidad. Realizan pruebas de software, automatizan pruebas, y supervisan la calidad del código y la funcionalidad de las aplicaciones.

Seguridad de la Información: Estos profesionales se centran en garantizar la seguridad de los sistemas de TI de la universidad. Trabajan en la implementación de medidas de seguridad, monitoreo de amenazas, y cumplimiento de normativas y políticas de seguridad.

Analistas de Datos / Analistas de Negocio: Este equipo proporciona insights basados en datos para optimizar el rendimiento de las aplicaciones y sistemas de la universidad. Ayudan a identificar áreas de mejora y oportunidades para la optimización del proceso de desarrollo y despliegue.

Equipo de Soporte / Atención al Usuario: Este equipo proporciona soporte técnico a los usuarios finales de las aplicaciones y sistemas de la universidad. Ayudan a solucionar problemas técnicos, responden preguntas y proporcionan formación cuando sea necesario.

Cada uno de estos miembros del equipo desempeña un papel importante en la implementación exitosa de DevOps en la Universidad Técnica de Manabí, trabajando juntos para lograr una entrega de software rápida, segura y de alta calidad.

Impacto de la propuesta

La implementación de la propuesta de DevOps en la Universidad Técnica de Manabí (UTM) tendría un impacto significativo y positivo en varias áreas clave de la institución. En primer lugar, la adopción de prácticas DevOps permitiría mejorar la eficiencia y la velocidad en el desarrollo, despliegue y operación de sistemas y aplicaciones de TIC. Esto significa que la UTM podría ofrecer servicios digitales más innovadores y actualizados de manera más rápida y ágil, lo que mejoraría la experiencia de los usuarios y promovería la transformación digital en toda la institución.

Además, la integración de la seguridad en todas las etapas del proceso DevOps fortalecería la postura de seguridad de la UTM, protegiendo los activos de información y mitigando los riesgos de ciberseguridad. Al fomentar una cultura de seguridad y colaboración entre los diferentes equipos de la universidad, la propuesta de DevOps contribuiría a aumentar la conciencia y la responsabilidad en materia de seguridad de la

información. En resumen, la implementación de DevOps en la UTM no solo impulsaría la eficiencia operativa y la innovación tecnológica, sino que también reforzaría la seguridad de los sistemas de información, fortaleciendo así la posición de la universidad como una institución líder en el ámbito de las tecnologías de la información y la comunicación.

5. Conclusiones

Tras llevar a cabo el análisis de la Propuesta de aplicación de la metodología DevOps con un enfoque de seguridad en la Universidad Técnica de Manabí, se puede establecer las siguientes conclusiones:

La adopción de la metodología DevOps en instituciones académicas ha sido limitada hasta el momento. Durante el curso de esta investigación, no se han hallado estudios similares realizados en organizaciones ecuatorianas. Por otro lado, la Universidad Técnica de Manabí carece de una estrategia definida que permita la integración fluida entre el desarrollo de software y las operaciones, con un enfoque centrado en la seguridad en todas las fases del ciclo de vida del desarrollo de software. Este documento identifica algunas de las repercusiones derivadas de la ausencia de implementación de dicha metodología.

Se logró fundamentar manera clara y argumentada la metodología DevOps, cuáles son sus aportes a las metodologías ágiles y la importancia de adoptarlo, proponiendo estrategias, así como algunas sugerencias para su implementación.

Los resultados revelan que la mayoría de los integrantes del equipo de Tecnologías de la Información (TI) de la Universidad no estaban familiarizados con metodologías ágiles para el desarrollo de software. Esto generó un interés significativo hacia la adopción de DevOps.

A pesar de haber transcurrido más de una década desde su surgimiento, varias empresas han optado por reconfigurar sus procedimientos de desarrollo de aplicaciones empresariales y la infraestructura correspondiente, y DevOps continúa expandiéndose. Esta metodología ha proporcionado a las empresas de desarrollo una opción concreta para agilizar los ciclos de vida del desarrollo, lo que les permite posicionarse competitivamente y adaptarse al ritmo de las demandas de sus clientes y del mercado.

Promover la conciencia de seguridad en TI por medio de la aplicación de la metodología propuesta, con el fin de entre los empleados del Departamento de TI que utilizan activos de información, lo cual resulta esencial para fomentar una cultura de seguridad en la Universidad Técnica de Manabí. Este enfoque contribuirá a la protección de la información y la prevención de riesgos cibernéticos.

Agradecimientos

Agradezco al personal que conforma el departamento de TIC de la Universidad Técnica de Manabí, a mi docente tutor y a todos quienes colaboraron con este trabajo.

DOI: https://doi.org/10.56124/encriptar.v6i12.003

Apéndice o Anexo

Tabla 1. Cuestionario

N°	**Pregunta**	**1**	**2**	3	**4**	**5**	NS/NC
1	¿Cuál es su nivel de conocimiento en metodologías ágiles para el desarrollo de software?						
2	¿Cuál es su nivel de experiencia con metodologías ágiles en su lugar de trabajo?						
3	¿Cuál es su nivel de conocimiento en la metodología de trabajo DevOps?						
4	¿Cuál es su nivel en el manejo de herramientas de automatización para DevOps?						
5	¿Cuál es su nivel de conocimiento en el desarrollo de software con metodologías de desarrollo seguro ?						
Descripción: 01 Muy Alto 02Alto 03 Medio 04 Bajo 05 Muy Bajo							

Fuente: Iñiguez Luis (2023)

Referencias

Agenda digital para América Latina y el Caribe. (2022). *CEPAL.* Obtenido de https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content

Alvarado, J. (2018). *Análisis de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la Municipilidad Distrital de independencia, mediante el uso de Phising 2017. [Tesis de Grado, USS]* . Obtenido de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8170/Alvarado%20Tolentino%20Joseph%20Darwin.pdf?sequence=1&isAllowed=y

Angulo, E. (15 de Julio de 2018). *Metodología cuantitativa*. Obtenido de https://www.eumed.net/tesis-doctorales/2012/eal/metodologia_cuantitativa.html

Apiumhub. (20 de Octubre de 2019). *Estudio sobre la situación actual del software.* Obtenido de https://apiumhub.com/es/tech-blog-barcelona/situacion-actual-del-software/

Basilio, D. (2020). El paradigma DevOps y su implementación en el desarrollo de software. *Universidad y Ciencia, 9*(3), 134-142. Obtenido de https://revistas.unica.cu/index.php/uciencia/article/view/1604/pdf

Carrera Mora, O. Y., Rodruíguez, A., Rodríguez, G., & Mancilla, M. (2019). Tecnología Blockchain en la Administración Pública como Plataforma para la Construcción de Confianza del Internet y de la Integridad de la Información. *SISTEMAS, CIBERNÉTICA E INFORMÁTICA, XVI*(1).

CITEC. (26 de Abril de 2022). *Datos oficiales del comercio electrónico.* Obtenido de https://citec.com.ec/

Diario Primicias. (12 de Marzo de 2021). *Nueve de cada 10 pymes en Ecuador invierte en tecnología.* Obtenido de https://www.primicias.ec/noticias/economia/pymes-ecuador-inversion-tecnologia-pandemia/

Felipe , A., & Núñez, F. (2022). DevOps: un vistazo rápido. *Ciencia Huasteca, 10*(19), 35-40.

Franco, A. (2016). *Comercio electrónico y desarrollo de la tecnología.* Quito: BID.

García, R., & Ríos, E. (2019). *Canal Cifrado para comunicación Cliente/Servidor. [Tesis de Maestría, UNAM].* Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/.../Tesis.pdf?

Guerrero, J. (2022). Modelo DevOps en la práctica: Aplicación de un modelo de referencia novedoso para respaldar y fomentar la adopción de DevOps en una

DOI: https://doi.org/10.56124/encriptar.v6i12.003

empresa de desarrollo de software como estudio de caso. *Revista Ibérica, 5*(1), 67-89.

González, D. (7 de Julio de 2022). *Comercio Electrónico de Ecuador impulsa la economía local*. Obtenido de https://www.america-retail.com/ecommerce/comercio-electronico-de-ecuador/

Jaramillo, C. (2022). *Estrategia de seguridad para el manejo de vulnerabilidades en el ciclo de integración y despliegue continúo en aplicaciones web esarrolladas bajo la metodología DevOps. [Tesis de Grado, ITM]*. Obtenido de https://Downloads/Sebastia%CC%81n_Corte%CC%81sMarulanda_2023%20(1).pdf

Ñacato , C. (2023). *Despliegue de VRF mediante Devops. [Tesis de Maestría, EPN]*. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/23841/1/CD%2013096.pdf

Orozco, C., Pardo, C., & Salazar , Y. (2022). ¿Qué hay acerca de la evaluación de DevOps? Un mapeo sistemático. *Rev. Fac. ing, 59*(23), 1121-1129. doi:https://doi.org/10.19053/01211129.v31.n59.2022.13896.

Orozco, C., Pardo, C., & Zúñiga , K. (2022). Proceso para fomentar y apoyar la adopción de DevOps en PyMEs de software. *Revista Científica CIDC, 45*(3), 422-437. Obtenido de http://revistas.udistrital.edu.co:8080/index.php/revcie/article/view/19644/18548

Pazmiño, E. (2018). *Bussines to Consumer en la era digital.* Panamá: Booking.

Prosper Heredia, R., & Vargas Lombardo, M. (2020). DevOps en el desarrollo SaaS desde el punto de vista de los experto. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Información, 6*(3), 252-263. Obtenido de https://www.researchgate.net/publication/354065539_DevOps_en_el_desarrollo_SaaS_desde_el_punto_de_vista_de_los_expertos

Pumasunta, E. (2020). *Migración de sistema "control de bienes" de Oracle Forms a una a una Arquitectura (JSF) Java para la empresa Municipal de movilidad y obras públicas (EMMOP-Q). [Tesis de Grado, UTI].* Obtenido de https://repositorio.uisrael.edu.ec/bitstream/47000/2490/1/UISRAEL-EC-SIS-378.242-2020-008.pdf

Ramírez, & Suárez. (2018). Tecnologías Información, «Introducción a Agile y Scrum: Principios y enfoques,». *TIC, 18*(2), 118-145. Obtenido de https://www.tecnologiasinformacion.com/agile-scrum.html

Rodriguez, K., Ortiz, O., & Quiroz, A. (2020). *El e-commerce y las Mipymes en tiempos de Covid-19. Revista espacios, 41(42). 100-118.* Obtenido de https://revistaespacios.com/a20v41n42/a20v41n42p09.pdf

Sumba Bustamante , R., Almendariz Gonzalez, S., Baque Chancay, C., & Aliatis Bravo, V. (Octubre-Diciembre de 2020). Emprendimientos en tiempo de covid-19: De lo tradicional al comercio electrónico. *FIPCAEC, V*(4), 137-164. doi:doi.org/ 10.23857/fipcaec.v5i4.300

Thorpe, E. (2019). Guía Completa para Principiantes Aprende DevOps paso a paso. *Independently Published,, 14*(3), 45-66.

UNIR. (10 de Noviembre de 2023). *¿Qué es DevOps y qué herramientas utiliza?* Obtenido de https://unirfp.unir.net/revista/ingenieria-y-tecnologia/devops/#:~:text=DevOps%20es%20una%20metodolog%C3%ADa%20de,entregas%20continuas%20y%20mejor%20calidad.

Varón, A. (2021). *Técnicas para formular proyectos de software e ingeniería web. [Fundación universitaria Area Andina]*. Obtenido de https://digitk.areandina.edu.co/bitstream/handle/areandina/3915/Tecnicas%20para%20formular%20proyectos%20de%20software%20e%20ingenieria%20web.pdf?sequence=5

Wiley, & Sons. (2019). *DevOps For Dummies.* Guadalajara: MaxiBook.