UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del artículo

Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales

Línea de Investigación:

Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable

Campo amplio de conocimiento:

Tecnologías de la Información y la Comunicación (TIC)

Autor:

Darwin Fernando Adriano Moromenacho

Tutores:

Mg. Renato Mauricio Toasa Guachi

PhD. Maryory Urdaneta Herrera

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Mg. **Toasa Guachi Renato Mauricio** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales.

Elaborado por: **Darwin Fernando Adriano Moromenacho**, de C.I: **1716233083,** estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Mg. Toasa Guachi Renato Mauricio

ORCID: 0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, PhD. **Urdaneta Herrera Marjory** con C.I**.: 1759316126** en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales.

Elaborado por**: Darwin Fernando Adriano Moromenacho**, de C.I: **1716233083**, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

PhD. Urdaneta Herrera Marjory

ORCID: 0000-0001-8773-5349

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Darwin Fernando Adriano Moromenacho con C.I: 1716233083, autor del proyecto de titulación denominado: Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.

3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
DARWIN FERNANDO
ADRIANO MOROMENACHO

Darwin Fernando Adriano Moromenacho

ORCID: 0009-0001-4197-5934

Tabla de contenidos

APROBACIÓN DEL TUTOR 2
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE 4
INFORMACIÓN GENERAL 8
Contextualización del tema 8
Problema de investigación 9
Objetivo general 11
Objetivos específicos 11
Vinculación con la sociedad y beneficiarios directos: 11
CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL 13
1.1. Contextualización general del estado del arte 13
1.2. Proceso investigativo metodológico 16
1.3. Análisis de resultados 18
CAPÍTULO II: ARTÍCULO PROFESIONAL 23
2.1. Resumen 23
2.2. Abstract 23
2.3. Introducción 24
2.4. Metodología 28
2.5. Resultados – Discusión 32
CONCLUSIONES 40
RECOMENDACIONES 41
BIBLIOGRAFÍA 42
ANEXOS 44

Índice de tablas

Tabla 1 Tabulación de listado de tipo de software y origen 9
Tabla 2 Revisión de publicaciones de otros autores 18
Tabla 3 Cadena de suministros de software 20

Índice de figuras

Figura 1 Integración Continua 14
Figura 2 Entrega Continua 15
Figura 3 Pilares para alcanzar un software resiliente 20
Figura 4 Fases del ciclo de vida de DevSecOps 21
Figura 5 Inversión en proyectos OpenSource a nivel global, 2023 25
Figura 6 Tecnologías Open Source para automatización y configuración 26
Figura 7 Tecnologías de software libre CI/CD 27
Figura 8 Principales desafíos de herramientas CI / CD 27
Figura 9 Herramientas de software libre para seguridad 28
Figura 10 Principales lineamientos de DevSecOps 30
Figura 11 Fases del ciclo de vida para DevSecOps 31
Figura 12 Pruebas de Seguridad 33
Figura 13 Compilación continua 34
Figura 14 Integración Continua 34
Figura 15 Entrega Continua 35
Figura 16 Despliegue Continuo 36
Figura 17 Operación Continua 36
Figura 18 Monitoreo Continuo 37
Figura 19 Modelo Conceptual de Plataformas DevSecOps 37

INFORMACIÓN GENERAL

Contextualización del tema

En el marco de los Objetivos de Desarrollo Sostenible (OSD) la Organización de Naciones Unidas ONU se planteó una agenda para el 2023 donde existen 17 objetivos para transformar nuestro mundo donde se busca alcanzar la erradicación de la pobreza juntamente con las estrategias que fomenten un crecimiento económico brindando respuestas a temas sociales como la educación, sanidad, protección social y empleo. De esta forma el presente trabajo busca ser un aporte delimitado geográficamente como principal zona de aplicación, el territorio ecuatoriano enfocándose al Objetivo 9: Industria, innovación e Infraestructura (Naciones Unidas, 2023).

Para cumplir con el acometido de ser un aporte sustancial al Objetivo 9, del ODS se busca apuntalar los pilares como son la inversión en investigación y desarrollo (I+D) y la búsqueda del crecimiento de las industrias de la tecnología media-alta. También se busca cumplir con uno los objetivos que se menciona en el artículo 3 numeral 1 de la Ley de Orgánica de Telecomunicaciones “Promover el desarrollo y fortalecimiento del sector de las telecomunicaciones” y el artículo 88 “1. Garantizar el derecho a la comunicación y acceso a la Información. (…) 5. Promover el desarrollo y masificación del uso de las tecnologías de información y comunicación en todo el territorio nacional (...)”

La situación actual del desarrollo de aplicaciones de software a nivel gubernamental se apoya sobre plataformas colaborativas para dar impulso a varios aplicativos de uso tanto a nivel ejecutivo como legislativo, podemos tomar como ejemplo el sistema Quipux, Firma EC, Portal de gobierno electrónico, GPR (Gestión por Resultados) y otros aplicativos de uso específico para cada entidad de acuerdo con sus necesidades. De esta forma el gobierno pone a disposición de un listado de software Publico Nacional, así como el repositorio de Software libre MINKA, disponible para su uso y distribución, todo el desarrollo de las aplicaciones, tienen distintas metodologías en su proceso de construcción, pero no se detecta que alguna tenga incorporado una metodología que tenga intrínsecamente el tema de seguridad informática. (Gobierno Ecuador, 2024)

Actualmente se tiene la necesidad de poder realizar la integración de metodologías ágiles de desarrollo de aplicaciones informáticas que permitan realizar de forma óptima una validación de seguridad informática, es así como nace el requerimiento de poder contar con un marco de referencia en el que la seguridad no sea un paso a seguir una vez finalizado el desarrollo en sus distintas fases, pasando a formar parte del proceso de desarrollo mediante los pasos adecuados se garantice que se incorpora la seguridad informática y garantizar el desarrollo de aplicaciones informáticas resilientes.

Para poder alcanzar la propuesta inicial del presente trabajo se realizará sobre el apoyo de tecnologías libres y disponibles actualmente, donde se integre los conceptos de DevSecOps propuestos como es la Integración continua (CI) y el Despliegue continuo (CD) haciendo llegar un producto de prueba o producto final con las últimas pruebas y características realizadas en la medida de lo posible securizado.

Para la presente investigación se ha realizado una búsqueda de autores y trabajos que se encuentren en la misma línea que se pretende desarrollar, dando un enfoque muy específico al desarrollo seguro que cuente con integración y despliegue continuo que pueda contribuir a obtener productos o aplicaciones desarrolladas de forma ágil sin perder o comprometer la seguridad con las que se encuentra desarrollado, cerrando cualquier brecha que pueda ser explotada al no tener en cuenta la seguridad al momento realizar el ciclo de desarrollo dentro de una institución gubernamental.

Problema de investigación

La investigación realizada se apoya en el catálogo de software disponible para la contratación y se encuentra a disposición del sector público para su uso y de esta forma poder aplicar un análisis que se plantea para realizar un desarrollo de aplicaciones informáticas, de esta forma se queda planteado el tipo de licenciamiento que se usa en las distintas ofertas realizadas, así como la ubicación geográfica del proveedor, información que se encuentra tabulada en la **Tabla *1***.

Tabla 1

Tabulación de listado de tipo de software y origen

Ciudad	Propietario	Software Libre
Quito	17	4
Guayaquil	10	1
Cuenca	7	1
Ambato	1	0
Esmeraldas	1	0
Ibarra	1	0
Machala	1	0
Portoviejo	1	0

Ciudad	Propietario	Software Libre
Riobamba	0	1
Sangolquí	0	1

Nota. Elaborado con información del portal: (Gobierno Ecuador, 2024)

Se realiza un análisis de los casos de estudio en los que se emplea el enfoque utilizando una aproximación al desarrollo de aplicaciones seguras mediante la metodología de *DevSecOps* para abordar una solución que integre las características necesarias para realizar un desarrollo ágil y seguro en todas sus etapas que comprende hasta lograr un producto final que cumpla con parámetros de calidad y seguridad.

Se ha demostrado mediante varios estudios e implementaciones que utilizar una metodología o enfoque orientado a *DevSecOps* desde el mismo inicio del proyecto se provee de herramientas que puedan contribuir a un desarrollo sostenible en el tiempo que brinde seguridad y calidad de los productos finales que ofrecen los equipos de desarrollo informático.

Ramos y Reclade (2022), indican por su parte que el desarrollo del despliegue de las buenas prácticas de DevSecOps, para mantener de una forma óptima y segura el desarrollo de aplicativos webs, minimizando los posibles errores en las distintas fases del desarrollo. La pertinencia del tema nos guía en una forma clara para poder entender el framework utilizado en este caso particular permitiendo ser un primer acercamiento a las herramientas y marco de referencia utilizado para las mejores prácticas.

Detallar la conceptualización de una implementación de DevSecOps utilizando herramientas de software libre verificando el estado del arte actual respecto a la adopción, así como el análisis del ciclo de vida. El tema lo desarrolla con herramientas disponibles mediante software libre para una implementación de DevSecOps, (Elez y López, 2023).

Se realiza el análisis de la perspectiva desde DevSecOps aplicado a un Centro de datos, permitiendo desarrollar estrategias que permitan una correcta implementación con la infraestructura disponible. Se presenta como un enfoque orientado a un centro de datos que pone énfasis en la disponibilidad de la infraestructura necesaria para poder realizar una implementación del enfoque DevSecOps, (Díaz y Muñoz, 2018).

Objetivo general

Elaborar una propuesta para desarrollar aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales aplicando una metodología DevSecOps que permita integrar en el proceso de desarrollo de aplicaciones.

Objetivos específicos

1. Analizar las prácticas de seguridad implementadas en el proceso de desarrollo de aplicaciones en los distintos grupos de trabajo que ofrecen sus productos para el Estado, así como desarrollos propios de instituciones gubernamentales para una aplicación de la metodología DevSecOps.

2. Evaluar los beneficios y desafíos específicos que surgen al aplicar el enfoque DevSecOps en una organización gubernamental encargada de la recopilación y gestión de datos.

3. Elaborar un conjunto de directrices y recomendaciones específicas basadas en los hallazgos de la investigación, con el propósito de servir como guía para futuras implementaciones de DevSecOps para proyectos de desarrollo.

4. Validar el impacto que puede tener la implementación en los procesos de desarrollo de aplicaciones al realizarlo con una metodología que considere la Seguridad Informática como parte de este proceso como lo realiza DevSecOps.

Vinculación con la sociedad y beneficiarios directos:

Al realizar la presente investigación basado en una entidad gubernamental se pretende optimizar los recursos asignados, mediante la mejora de procesos en el desarrollo de aplicaciones de software que permitan realizar la entrega de productos de forma ágil y segura permitiendo integrar las últimas características desarrolladas en las primeras versiones sin llegar a replantear y reformular el proceso de desarrollo brindando en todo los pasos y fases conceptos de seguridad informática integrado a las actividades realizadas.

Se pretende levantar un marco referencial general que pueda ser aplicado a los casos particulares dentro de las organizaciones e instituciones que tengan dentro de su plantilla un equipo de desarrollo principalmente y también puede ser aplicable y trabajar de forma conjunta con un equipo de seguridad informática, así como el equipo de control de calidad QA.

Al integrar los procesos metodológicos que consideren a la seguridad informática como parte del desarrollo de aplicaciones de software y al aplicarlo se considera que se está realizando un aporte sustancial para cumplir con los Objetivos de Desarrollo Sostenible al estar acorde al objetivo 9 y de

esta forma se logra una optimización de los recursos que se realizan en la innovación así como en investigación y desarrollo (I+D), al optimizar los recursos evitando los reprocesos en el desarrollo de aplicaciones informáticas por parte del estado y acortando los tiempos de entrega de productos y servicios informáticos que involucre el desarrollo de aplicaciones brindando una respuesta oportuna a los ciudadanos haciendo un buen uso de los recursos asignados.

Los estamentos que hacen uso de los recursos del estado en lo referente al uso y desarrollo de software están en la obligación de dar cumplimiento al Código Orgánico de la Economía Social de los Conocimientos Creatividad e innovación, Artículo 148 donde establece 5 prelaciones detalladas en la figura 1 donde se prioriza el uso de Software Libre y también el componente de valor agregado ecuatoriano

Como se observó en la **Tabla *1*** los proveedores del listado de software que facilitan sus servicios y productos al estado ecuatoriano en su gran mayoría ofrecen como software propietario, esto quiere decir que la propiedad intelectual la reservan para ser los únicos autorizados a realizar modificaciones y actualizaciones al software. Al no tener acceso las entidades gubernamentales al código fuente ni al proceso de desarrollo de sus aplicaciones informáticas no se puede realizar un estudio y evaluación de la propuesta que realiza el presente trabajo para la adopción de una metodología de DevSecOps de tal forma que no serán parte del estudio realizado.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1. Contextualización general del estado del arte

Un primer acercamiento que permita brindar una contextualización del estado del desarrollo de las herramientas para una implementación basada en un enfoque de DevSecOps remarcando el significado en desarrollo, seguridad y operaciones. Muestra la utilidad para tener un enfoque referencial del estado del arte mediante un actor principal en la metodología DevSecOps, (RedHat, 2023)

Se pretende realizar una contextualización más amplia del flujo de trabajo de DevSecOps realizando el análisis de una implementación evaluando los riesgos y beneficios que puede aportar esta metodología, delimitando el estudio a un país en particular, (Pachacuti, 2021).

Presentar una evaluación de los riesgos y beneficios de realizar una implementación, tomando en cuenta que existe un cambio en el enfoque del desarrollo al realizarlo como un servicio (SaaS, *Software as a Service*), en el que el desarrollo se realiza sobre una infraestructura que no lo controla la entidad que requiere el producto, haciendo que los productos entregados y desplegados se realice de forma continua tradicionalmente conocido como DevOps, (Fontela y Paez, 2022).

Para el presente estudio se pretende ampliar el concepto manejado como DevOps integrando los conceptos de seguridad informática al proceso de desarrollo ágil. Actualmente no es una metodología muy ampliamente aceptada pues agrega varios pasos de validación que se requiere para garantizar un desarrollo seguro, cambiando varios pasos o aumentando algunas validaciones previas a la entrega o despliegue del software.

En el presente trabajo se está utilizando la terminología DevSecOps (*Development Secutiry Operations*) un concepto derivado de DevOps (*Development Operations*) o desarrollo agile que se encuentran muy estrechamente ligados ya que los dos conceptos o metodologías hacen referencia al desarrollo de aplicaciones informáticas que comprende trabajar con las definiciones de los procesos de integración y entrega continua (CI / CD), en el ciclo de desarrollo haciendo que DevSecOps vaya un paso más allá en el proceso de desarrollo al incorporar medidas de seguridad en todo el ciclo de vida del desarrollo y en los datos que maneja, al integrar esta validación se procura no extender los tiempos de desarrollo y en la medida de que el proyecto lo permita automatizar la mayor parte de las validaciones que son necesarias.

Para poder cumplir con esta funcionalidad la metodología DevSecOps se apoya en varias soluciones de software ya presentes como son maquina virtuales, hipervisores o contenedores de esta forma se

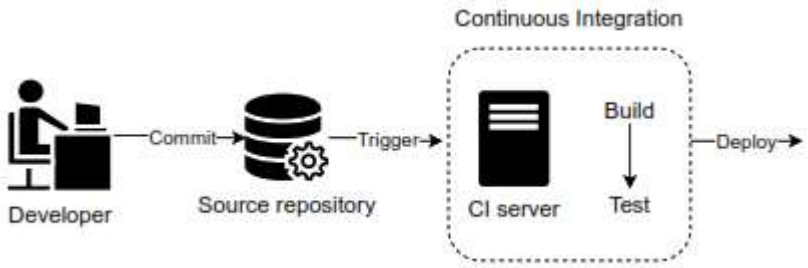
puede recrear el ambiente de desarrollo sin mayor esfuerzo o instalación de toda la paquetería de software necesario para el funcionamiento o la configuración y parametrización de las variables necesarias para poner en marcha una estación que cuente con un entorno adecuado y aislado al tener las herramientas esenciales para poder realizar las tareas de desarrollo.

Integración Continua

También conocido en su forma abreviada CI (*Continuous Integration*) la integración continua indica y motiva que el desarrollador del proyecto realice la integración con su plataforma de desarrollo de los últimos cambios realizados de manera frecuente asegurando que siempre estén disponibles las nuevas características en momento de realizar la entrega continua del código (Rajapakse et al., 2022) se puede tener un esquema básico como muestra la **Figura *1***.

Figura 1

Integración Continua



Nota. Tomado de (Rajapakse et al., 2022)

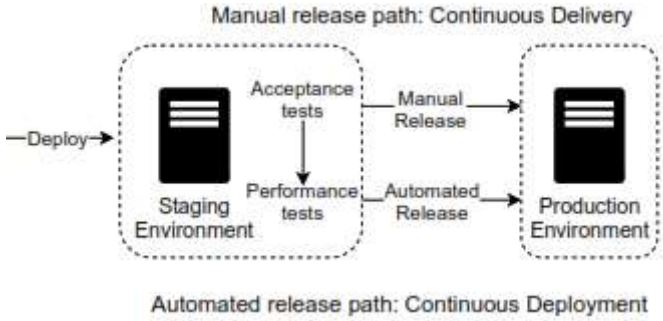
Una herramienta útil para poner en práctica la Integración continua se puede encontrar en git en el que el desarrollo de aplicaciones se realiza en forma de ramificaciones para cada participante del proyecto, es necesario impulsar el código a la rama máster para que todos los involucrados puedan tener acceso a las últimas modificaciones.

Entrega Continua

Conocido de su forma abreviada como CD (*Continuous Delivery*) Hace referencia a un enfoque para conformar los equipos de trabajo que son los encargados de realizar las publicaciones de los productos desarrollados con una frecuencia continua y estable conforme se va realizando el desarrollo de los aplicativos tomando desde los repositorios el código fuente y realizar la producción de forma lo más automatizado posible (Rajapakse et al., 2022) mostrado en la **Figura *2***.

Figura 2

Entrega Continua



Nota. Tomado de *(Rajapakse et al., 2022)*

Para que realice una buena labor se puede pensar que trabaja como una canalización (*pipeline*) direccionando los flujos de trabajo que en su mayoría deben estar automatizados, esto no quiere decir que se deba excluir la intervención manual, pero si tratar de minimizar para reducir la superficie de posibles riesgos de incluir fallas humanas.

La arquitectura del proyecto influye finalmente en los flujos de trabajo, direccionamiento de las pruebas automatizadas y los artefactos que se producen en esta fase.

Artefactos Agile SCRUM

Según De Dios (2024), menciona: "*Toda empresa debe asegurar que el equipo implicado conoce sus tareas y plazos de tiempo de entrega. SCRUM es un marco de trabajo que nos ayuda a conseguirlo y que, además, permite agilizar la entrega de valor al cliente en iteraciones cortas de tiempo*", de esta forma con SCRUM podemos conformar los equipos de desarrollo para lograr los objetivos trazados en el proyecto con iteraciones en el menor tiempo posible.

Seguridad Informática

La seguridad informática también referenciado como ciberseguridad *"se refiere al uso de modelos, marcos de trabajo, estándares, metodologías, normas, técnicas, herramientas y estructuras organizacionales encaminadas a proteger la información en sus diferentes formas y estados"* tomando como fundamento la triada Confidencialidad, Integridad y Disponibilidad, (Muñoz y Rivas, 2015).

Uno de los principales objetivos de la metodología DevSecOps se encuentra orientado a mejorar el robustecimiento de la protección de la información de acuerdo con la experiencia y giro del negocio

intentando que los ciclos de desarrollo sean cortos o de inmediata puesta a producción sin que realizarlo de esta forma implique una baja calidad en el software entregable

Importancia de la Seguridad Informática en el proceso de desarrollo de aplicaciones según (Google Gemini, 2024).

La Seguridad Informática cumple con la función vital de proteger a las personas, organizaciones de toda naturaleza de los riegos existentes considerando el mundo físico como el digital donde los principales beneficios que se puede identificar son:

Protección de la Información confidencial como lo son datos personales, bancarios, médicos, comerciales y otros.

Prevenir daños económicos con la perdida de datos, suplantaciones de identidad, robo de información, interrupciones del servicios o daño de la reputación.

Mejorar la confianza de clientes, asociados Stakeholders mediante el fortalecimiento de la imagen y reputación de las organizaciones.

Realizar las actividades bajo un marco legal regulatorio y tener la certeza de cumplir con las obligaciones y normas legales como COIP, Protección de datos personales, otros.

Tipos de Seguridad Informática

Seguridad de red, protege la infraestructura de red contra accesos no autorizados, intrusiones y ataques.

Seguridad de datos, para realizar la protección de la confidencialidad de la información contra el hurto, corrupción y daño accidental

Seguridad de aplicaciones, protege los entornos de aplicaciones contra vulnerabilidades y ataques.

Seguridad de nube, principalmente utilizado para entornos de IaaS, SaaS, donde la principal protección se encuentra en los sistemas y datos alojados en la nube.

Seguridad de identidad, orientado a proteger las credenciales de acceso a los sistemas y datos que contiene esta información, aplicando políticas y reglas de complejidad.

1.2. Proceso investigativo metodológico

Para el proceso investigativo metodológico se realizó con un enfoque cualitativo descriptivo mediante la exploración de material bibliográfico comparativo, donde se procedió a la lectura de

fuentes de información fiables como artículos de investigación, tesis, entre otros para obtener una comparativa que permita tener un aporte significativo en la implementación y estudio de la metodología DevSecOps y levantar la propuesta formulada en el objetivo.

Investigación Descriptiva

Para poder llevar a delante el presente proceso investigativo Ñaupas et al.(2018), indica que en la Investigación Descriptiva el "Objeto principal es recopilar datos e informaciones sobre las características, propiedades, aspectos o dimensiones, clasificación de los objetos, agentes e instituciones ". Realizar bajo estos condicionamientos nos va a permitir realizar una investigación explicativa para tomar decisiones que afecten a la infraestructura disponible en las instituciones ajustándose a cada una de las realidades que afrontan.

El uso dado al proceso de investigación descriptiva resulta útil para el desarrollo del presente trabajo al recopilar y analizar la información disponible que tenga un aporte significativo y sustancial.

Investigación Bibliográfica

Dentro de la investigación bibliográfica, Salas Ocampo (2024), menciona que actualmente se tiene a disposición varios recursos para tener acceso inmediato a una amplia cantidad de información, el reto como investigador se encuentra en realizar una validación de la información a ser utilizada en el proceso investigativo, para esto nos basamos en medios tradicionales, así como información disponible electrónicamente y poder filtrar de una forma adecuada.

Sobre las bases que apoya el trabajo desarrollado en el presente documento investigativo se aplica un análisis para lograr una identificación de los elementos a utilizar en los diferentes componentes que conforman la investigación del tema propuesto. Haciendo uso como fuente principal de información los recursos como artículos científicos, informes comparativos del objeto de investigación, consultas de información de actores relevantes al desarrollo de DevSecOps y sus herramientas de implementación.

Es relevante realizar una investigación bibliográfica ya que se puede apoyar de los enfoques de investigación cuantitativos y cualitativos al realizar un análisis desde distintos ángulos (Salas Ocampo, 2024)

La investigación mediante métodos y técnicas de recolección de la información se realiza mediante un análisis de documentación de artículos, libros, publicaciones relacionadas en repositorios, revistas y catálogos de información con el rigor de una investigación científica adecuada y relacionados con la

temática del estudio en curso como los es el desarrollo de aplicaciones seguras mediante la metodología DevSecOps

1.3. Análisis de resultados

Para poder analizar los resultados del proceso investigativo llevado a cabo se realizó una comparativa de las publicaciones realizadas previamente que sirve de aporte fundamental para realizar el presente trabajo aplicando la metodología de la investigación bibliográfica y descriptiva. De esta forma se pone a consideración los siguientes artículos investigados y que están condensados en la **Tabla *2***.

Tabla 2

Revisión de publicaciones de otros autores

Autor	Tema	Año	Artículo	Libro	Portal Web
Fontela, Carlos Páez Nicolas	Hacia otro modelo de proceso de desarrollo de software.	2022	SI		
Juan Pardón Miguel Flores Víctor García	DevSecOps: Integración de la Seguridad en Entornos CI/CD	2021	SI		
Oswaldo Díaz Mirna Muñoz	Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización mexicana	2018	SI		
Andres Ramos Pablo Recalde	Balanceo y despliegue de carga en aplicaciones web mediante kubernetes	2022	SI		
Maribel Pachacuti	DevSecOps, Estado del Arte en el Contexto Boliviano	2021	SI		
Roshan N. Rajapakse Mansooreh Zahedi M. Ali Babar Haifeng Shen	*Challenges and solutions when adopting DevSecOps: A systematic review*	2021	SI		
Department of Defense USA	*Enterprise DevSecOps Fundamentals*	2021		SI	

Autor	Tema	Año	Artículo	Libro	Portal Web
Department of Defense USA	*Enterprise DevSecOps Strategy Guide*	2021		SI	
Tony Hsu	*Hand-on Security in DevOps*	2018			SI

Cadena de Suministro de Software

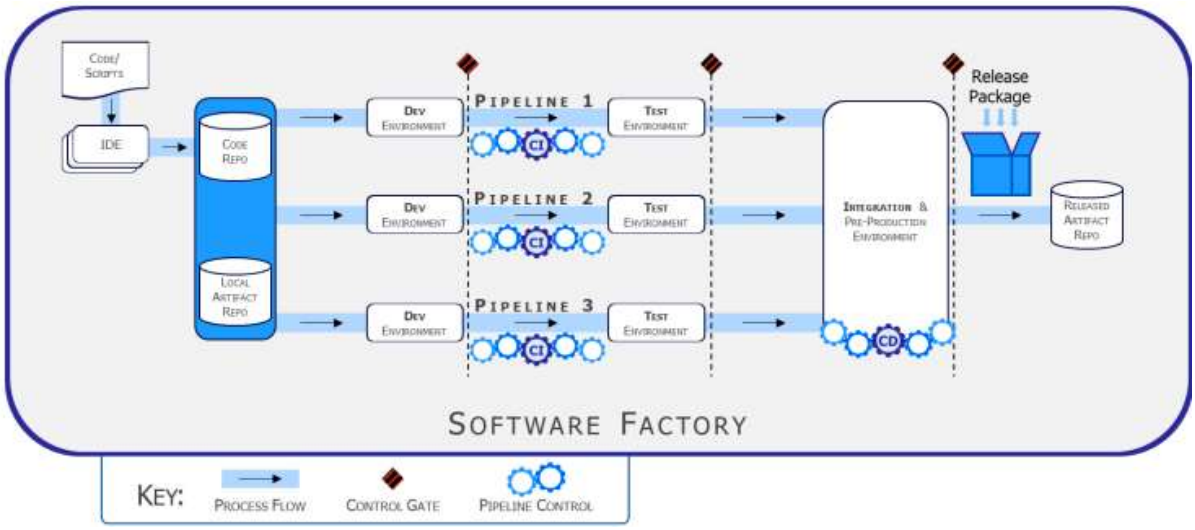
La cadena de suministro del software es la ruta logística que cubre de forma completa, todo el hardware, Infraestructura como servicio (IaaS), plataforma como servicio (PaaS), software como servicio (SaaS), multiplicadores de fuerza tecnológica, herramientas y prácticas que se combinan para ofrecer las capacidades específicas del software, como lo muestra la **Figura *3***.

Existen cadenas de suministro de software para sistemas comerciales, sistema de despliegue y en todo lugar que se realiza el desarrollo e implementación de software. Es fácil pensar que el software desarrollado dentro de un proyecto se encuentra aislado y desconectado, pero sería incorrecto pensar de esta forma, ya que el proyecto incluye software embebido que fue compilado incluyendo librerías de terceras partes y enlaces a *frameworks* o kits de desarrollo.

La metodología DevSecOps contempla varios enlaces a la cadena de suministros de software. DevSecOps no puede existir sin esta cadena de suministro logístico como Ambientes de Desarrollo integrado (IDE), herramientas de compilado, repositorio de código, repositorio de artefactos, software de pruebas, y otras piezas de software que deben trabajar conjuntamente para asegurar la efectividad de la metodología DevSecOps, la totalidad de estos entornos deben considerarse al evaluar la cadena de suministro de software.

Figura 3

Pilares para alcanzar un software resiliente



Nota. Permite visualizar la cadena de suministros de software, tomado de (Department of Defense USA, 2021)

Adoptando DevSecOps

La adopción de DevSecOps conduce al concepto de fábricas de software al ser todo un ecosistema combinado que conduce a un cambio estratégico de entrega y ofrecimiento de software resiliente a la brevedad posible con los pasos que muestra **Tabla *3***. Esta estrategia de DevSecOps se guía por los principios que son abstracciones que se pueden considerar de forma aislada creando controles de seguridad para el equipo de trabajo.

Tabla 3

Cadena de suministros de software

Metodología DevSecOps
Búsqueda de desarrollo Ágil
Fábricas de desarrollo con seguridad integrada
Integración, automatización y pruebas / monitoreo continuo
Infraestructura Inmutable
Adopción de la nube inteligente

Búsqueda de desarrollo Ágil

El manifiesto de desarrollo Ágil busca descubrir mejores formas de realizar el desarrollo de software mediante la experiencia propia, así como de terceros valorando los siguientes aspectos:

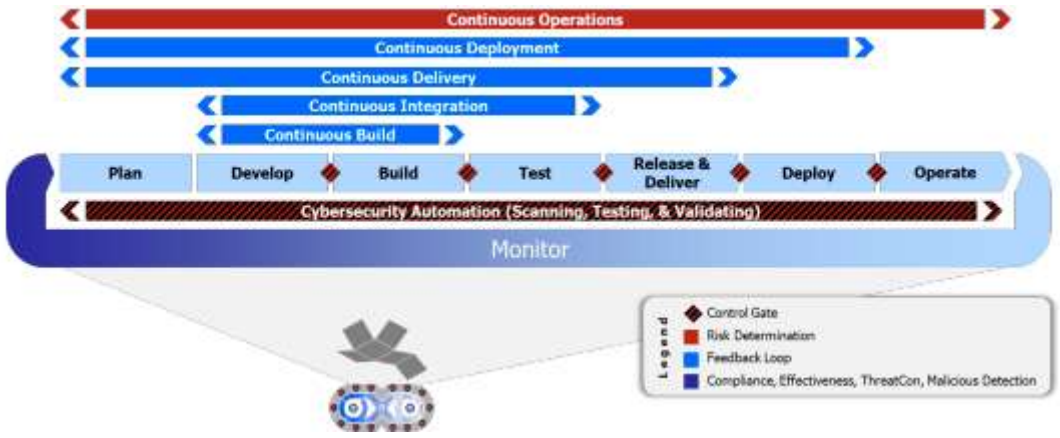
- Individuos e interacciones sobre los procesos y herramientas
- Software funcionando sobre la documentación extensiva
- Colaboración con el cliente sobre negociación contractual
- Respuesta al cambio sobre seguir un plan

Fábricas de desarrollo con seguridad integrada

Las fábricas de software con seguridad integrada deben tener prácticas de seguridad integrales y exhaustivas en toda la cadena de suministro del software aprovechando los principios de detección de comportamiento de confianza cero (*Zero Trust*) y se muestra en **Figura *4***.

Figura 4

Fases del ciclo de vida de DevSecOps



Nota. Fases del ciclo de vida de DevSecOps tomados de (Department of Defense USA, 2021)

Integración, automatización y pruebas / monitoreo continuo

Hace referencia al cambio hacia la Continua automatización de las operaciones, así como las pruebas y monitoreo continuo. Cada programa debe ser construido e implementado como un proceso con su puerta de control y prueba integrado. El monitoreo continuo también es necesario para poder hacer efectivo los requerimientos de confianza cero.

Infraestructura Inmutable

Realizar el cambio a una infraestructura inmutable utilizando la infraestructura como Código, Política como código y todo como código proporciona valor y seguridad en varias maneras. Se establece un principio de la configuración automatizada de infraestructura controlada mediante código. El código puede ser versión controlada, probada, revisión por pares y seguimiento de ejecución (logs).

Adopción de la nube inteligente

Se puede ver como un enfoque optimista que supone que la nube viene con una oferta capacidad computacional infinita, disponibilidad garantizada y menores costos operativos. El consumo y transporte de datos cade vez aumentan por lo que las arquitecturas de software deben estar en capacidad de adaptarse a estos nuevos requerimientos, así como diseñar las interfaces de programación de aplicaciones (API), estrategias de almacenamiento en cache.

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1. Resumen

En la propuesta mediante la metodología DevSecOps para el desarrollo de aplicaciones seguras se parte de la necesidad de contar con aplicaciones seguras y resilientes para lo cual se permite describir el proceso ágil de desarrollo metodológico integrando conceptos de seguridad informática conformando los equipos de trabajo multidisciplinares como desarrollo, seguridad y operaciones informáticas orquestando el trabajo conjunto en las distintas fases que lo componen y adaptándose a cada necesidad particular sin renunciar a los principios que rige la metodología DevSecOps propuesta y analizada la cual permite hacer una personalización de las herramientas y entornos a utilizar según las necesidades institucionales de acuerdo a su nivel de adopción y capacidad de producción pensando siempre que se encuentra orientado a ser fácilmente escalable para un despliegue rápido, oportuno y continuo en los tiempos requeridos garantizando un producto de software resiliente, siguiendo las fases del ciclo de vida en el desarrollo de DevSecOps y su cadena de suministro de software necesario en cada fase del desarrollo.

a. Palabras clave:

Desarrollo, integración, continua, seguridad, DevSecOps

2.2. Abstract

In the proposal using the DevSecOps methodology for the development of secure applications, we start from the need to have secure and resilient applications for which it is possible to describe the agile process of methodological development integrating concepts of computer security by forming multidisciplinary work teams as development, security and IT operations orchestrating the joint work in the different phases that compose it and adapting to each particular need without renouncing to the principles that governs the proposed and analyzed DevSecOps methodology, which allows a customization of the tools and environments to be used according to the institutional needs according to their level of adoption and production capacity, always thinking that it is oriented to be easily scalable for a fast deployment, timely and continuous deployment in the required times guaranteeing a resilient software product, following the phases of the DevSecOps development life cycle and its supply chain of software needed in each phase of development.

a. Keywords

Development, Integration, continue, security, DevSecOps.

2.3. Introducción

Para realizar la propuesta de desarrollo de aplicaciones informáticas seguras por definición, es decir, que desde la misma concepción del proyecto inicial de desarrollo se van a tener en consideración y noción de los conceptos relacionados con la ciberseguridad, permitiendo de esta forma que los equipos de las distintas áreas de las Tecnologías de la Información y Comunicación como desarrollo, seguridad y operaciones informáticas trabajen bajo una misma metodología sin tener mayor impacto en los tiempos de desarrollo y entrega de los productos finales.

Los conceptos expuestos se deben tener enfocados a la realidad nacional con las que se llevan adelante los proyectos de desarrollo tecnológico en la producción de software informático bajo una misma metodología y con la sugerencia de las herramientas que pueden estar al alcance de los equipos donde se aplicará DevSecOps, estos son herramientas de software libre que no exigen pago de licenciamiento por uso y además son altamente personalizables.

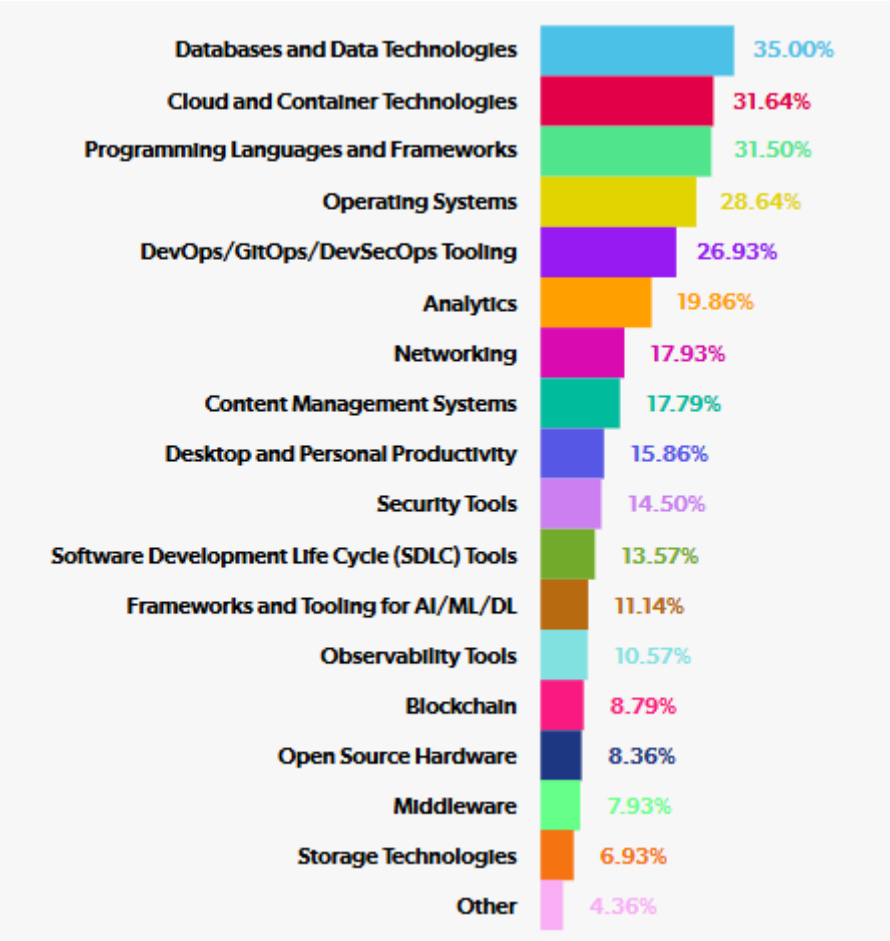
DevSecOps y el Software libre

Los nuevos conceptos que llegan, están inherentemente con un cierto grado de escepticismo e incertidumbre, Al ser DevSecOps un nuevo concepto que evoluciona a partir de DevOps para ampliar sus beneficios en el proceso de desarrollo de aplicaciones informáticas, la fuerza laboral presente en la institución que adopta la metodología propuesta, desde los ingenieros de desarrollo, profesionales no afines a los temas tecnológicos pero que sus actividades y funciones depende mucho de los servicios tecnológicos que se pone a su disposición, así como los cargos directivos aún pueden tener muchas dudas sobre la metodología en mención (Department of Defense USA, 2021).

El desarrollo dentro de las herramientas que pueden ser usadas para cumplir con la metodología DevSecOps tienen un alto componente de software libre lo cual permite aprovechar las ventajas conocidas por su tipo de licenciamientos y uso que se puede dar, esto incide directamente en el costo / beneficio que puede representar dentro de una institución realizar una implementación de estas características, según (Open Source Initiative (OSI), 2024) en su reporte anual del estado del software libre, 2024 (2024, *State of Open Source Report*), la inversión destinada a las tecnologías relacionadas con las herramientas para DevOps, GitOps y DevSecOps fue del 26,93 % del total de la inversión realizada en el año 2023 a los proyectos de software libre según se muestra en la **Figura *5*** Inversión en proyectos OpenSource a nivel global, 2023.

Figura 5

Inversión en proyectos OpenSource a nivel global, 2023

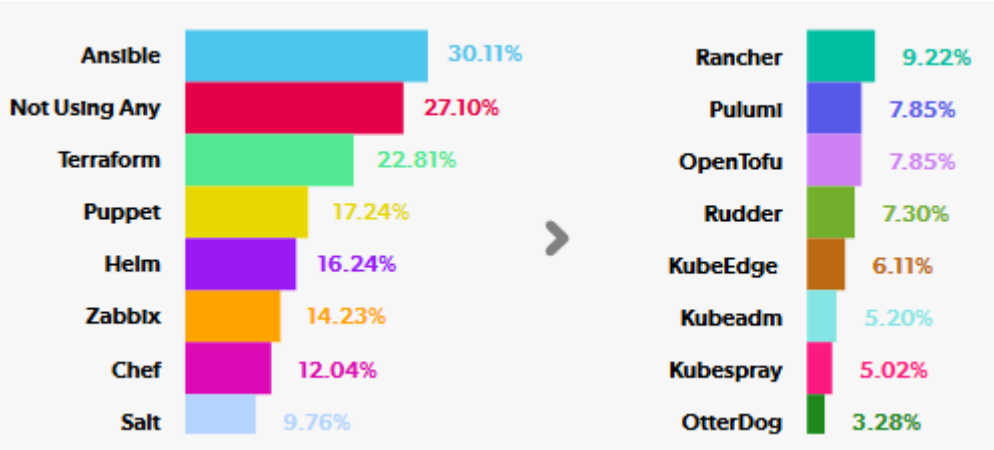


Tecnologías de Automatización y Configuración

Como se hizo mención en el apartado de análisis de resultados en la **Figura *6*** Tecnologías Open Source para automatización y configuración muestra uno de los puntos clave para poder realizar una buena implementación de la metodología DevSecOps, es el tema de la automatización de todo lo que sea posible dentro del ciclo de vida del proceso de desarrollo, de esta forma hacemos un análisis de las herramientas de software libre para la categoría de automatización y configuración, también conocido dentro de las organizaciones que tienen implementado como Infraestructura como Código o Ingeniería de Plataforma, es importante mencionar que las pequeñas y nuevas organizaciones posiblemente no tengan o no requieran de un entorno de automatización y configuración por lo que existe un porcentaje significativo de 27,10 % que aún no hacen uso de este tipo de herramientas, (Open Source Initiative (OSI), 2024).

Figura 6

Tecnologías Open Source para automatización y configuración



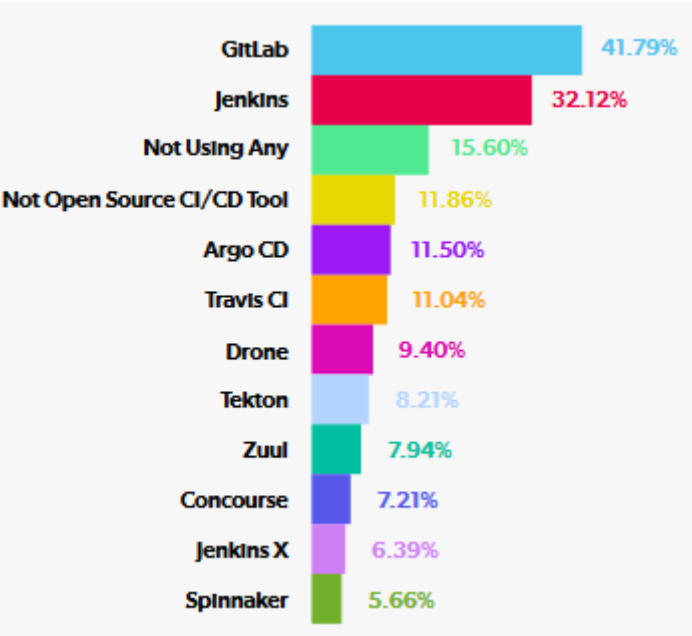
Es importante mencionar aquí que en las herramientas más utilizadas se encuentran tecnologías maduras con años de desarrollo y que tienen el apoyo de varias organizaciones como Ansible, Terraform y Puppet que se encuentran como las herramientas más usadas a nivel global, un tema particular que se puede mencionar es el cambio de licenciamiento de Terraform que desde el año anterior dejo de estar disponible como software libre y a partir de ese cambio se tiene disponible una bifurcación del proyecto con el código fuente de Terraform llamada OpenTofu según el gráfico 8 tiene un 7,85 %. En el informe se menciona que en regiones como América latina el uso de la herramienta Puppet asciende hasta el 23 %.

Tecnologías de CI/CD

Mientras las herramientas tecnológicas de software libre (*Open Source*) para la integración continua (CI) y despliegue continuo (CD) han sido utilizadas como una elección predeterminada para muchas organizaciones en el desarrollo de sus aplicaciones informáticas, aún existe un margen por mejorar en concepto de adopción de este tipo de tecnologías Agiles, ya que el 15,60 % a nivel global indica que no hace uso de este tipo de tecnologías CI / CD, **Figura *7***. Por resaltar que en este punto también se incluyen herramientas de tecnología CI/CD que no son software libre entre las que destacan Github, (Open Source Initiative (OSI), 2024).

Figura 7

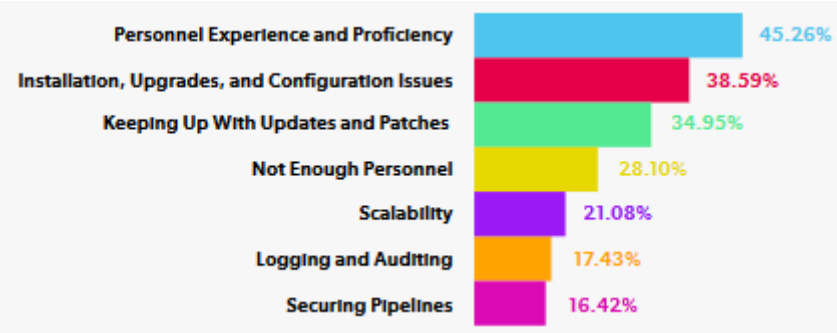
Tecnologías de software libre CI/CD



En el análisis también se realiza la consulta de los principales desafíos que tiene el uso de herramientas CI/CD destacando que ya falta de personal calificado y con experiencia representa un desafío importante para este tipo de tecnologías como muestra la **Figura *8***.

Figura 8

Principales desafíos de herramientas CI / CD



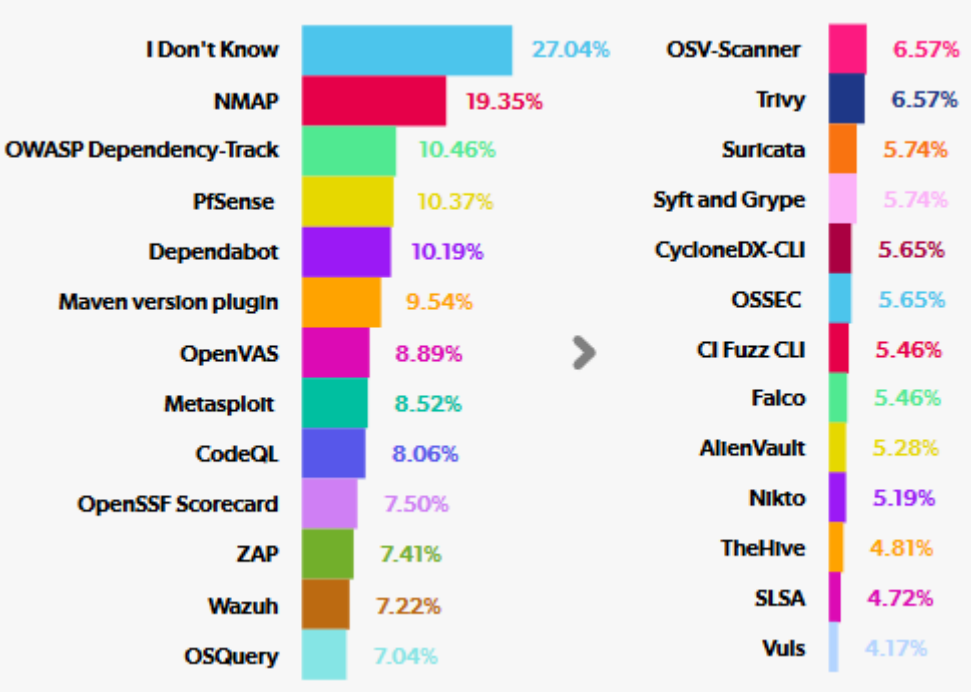
Tecnologías de Seguridad

En el tema de las tecnologías de seguridad informática de software libre (Open source) que existen una variedad de herramientas como escaner de vulnerabilidades, firewalls, analizadores de código fuente, entre otros es un área que está en constante crecimiento ya que se prioriza para las etapas de

desarrollo de aplicaciones informáticas, así como redes y operaciones. El dato preocupante aquí es que la mayoría de quienes respondieron a la pregunta de las herramientas de software libre que usan en su organización el 27,04 % **Figura *9*** indica que desconoce la implementación realizada, (Open Source Initiative (OSI), 2024).

Figura 9

Herramientas de software libre para seguridad



2.4. Metodología

En la investigación realizada mediante las metodologías descriptivas, se procedió a recolectar la mayor cantidad de información posible tomando en cuenta que también esta información debe cumplir con el rigor académico y científico con una base plenamente fundamentada que permita encontrar una propuesta viable adaptado a la realidad nacional del Ecuador y de forma más específica a los equipos de TICs del área de instituciones públicas sin que eso signifique que no se puede aplicar a las instituciones de otra naturaleza a las referidas en el documento.

Con la bibliografía investigada se puede tener una idea claro de la propuesta y el marco referencial que se debe seguir. En todos los equipos de trabajo puede diferir las herramientas utilizadas que se puede encontrar en las instituciones, el trabajo presentado no pretende ser una guía paso a paso de las herramientas específicas a usar para una implementación DevSecOps pues la metodología no habla de software específico en la metodología podemos encontrar conceptos relacionados con los ciclos

de vida, tiempos de entrega, plataforma de desarrollo que entre los equipos de trabajo tienen mucha más disparidad que se origina desde varias razones que escapan al análisis de la presente investigación.

Justamente aquí es donde se expone la valía de seguir una metodología de investigación bibliográfica, pues a nivel nacional no se tiene una infraestructura homogenizada propia que pueda ofrecer los servicios necesarios para todo tipo de proyectos de desarrollo informático y de esta forma poder realizar una encuesta que satisfaga y encause las necesidades de los equipos de desarrollo informático en las instituciones públicas y poder llegar a planear una metodología de DevSecOps.

Por otro lado, al realizar una revisión de la literatura existente, esta permite buscar y seleccionar la documentación entre los artículos, publicaciones, libros relevantes y referentes al tema de una metodología DevSecOps o unas primeras aproximaciones aclarando conceptos y refiriéndose a las experiencias de implementaciones o estudios realizados en otra parte de la geografía.

Se realiza el análisis de la información consultada, tomando las ideas y conceptos relevantes para el presente trabajo investigativo, estos conceptos que son aplicables al ámbito nacional de las instituciones gubernamentales sin llegar a sugerir unos pasos de forma específica al no estar orientado a un tipo específico de desarrollo o plataforma utilizada.

Toda la información que es extraída y organizada de la literatura consultada hace que podamos sintetizar los conceptos e interpretando con la línea investigativa planteada como objetivo en el presente trabajo, de esta forma contribuyen a dar respuesta al problema planteado con este trabajo de investigación.

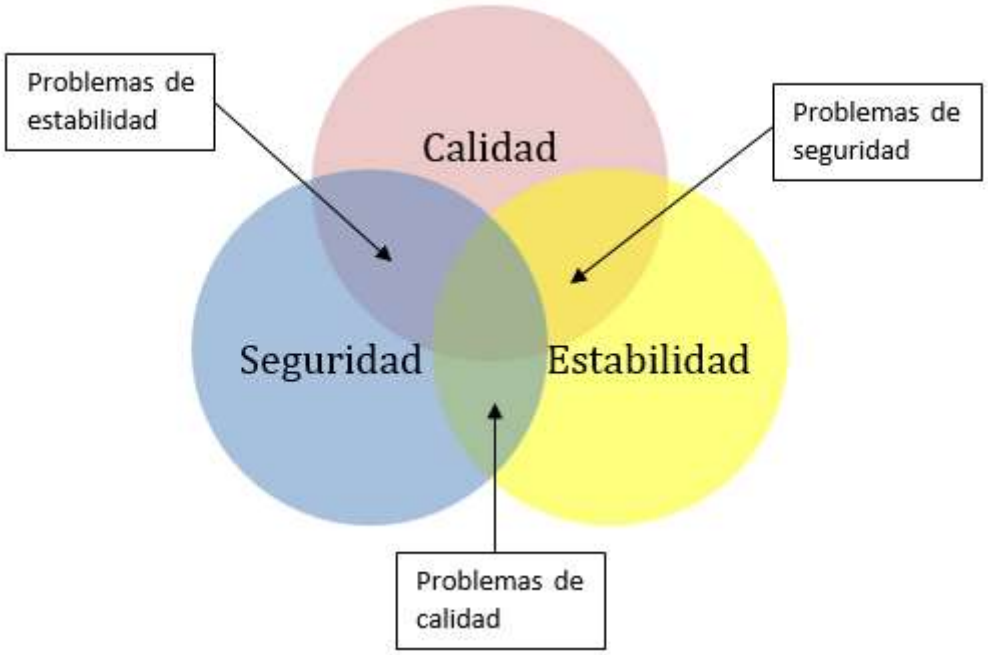
Para poder realizar esta investigación bibliográfica se consultó varias bases de datos bibliográficos, así como catálogos de bibliotecas en línea y repositorios de universidades que contengan trabajos de estudios publicados y que tengan relación con el tema que se está tratando de la metodología DevSecOps

Metodología DevSecOps

La metodología DevSecOps tiene un enfoque para el ciclo de vida del software de creación de equipos de trabajo multifuncionales que tienen evoluciones dispares como Desarrollo (Dev), Ciberseguridad (Sec) y Operaciones (Ops), esta unificación de los equipos de realiza mediante los principios del desarrollo ágil y adoptando una cultura de software resiliente que se logra mediante la calidad, estabilidad basada en la **Figura *10***.

Figura 10

Principales lineamientos de DevSecOps



Nota. Adaptado de (Department of Defense USA, 2021)

Seguridad. - Software seguro se puede mencionar que este tipo de software detecta y resiste a un ciberataque ofreciendo un grado de resistencia de supervivencia cibernética.

Estabilidad. - El software estable es el que funciona como se espera sin colgarse ni bloquearse y sea dinámicamente escalable a la demanda requerida.

Calidad. - un software de calidad maximiza la cobertura de los requerimientos de características del usuario y minimiza los defectos de funcionalidad.

Beneficios de adoptar DevSecOps

Reduce el tiempo de producción, reduce el tiempo promedio que toma el desarrollo de nuevo software desde las características que son requeridos hasta la ejecución en producción.

Incrementa la frecuencia de despliegue, incrementa la frecuencia de nuevas publicaciones que son desplegadas en un ambiente de producción

Reduce el tiempo de recuperación, reducción del tiempo promedio que toma identificar y solventar una falla después del despliegue en producción.

Reduce la taza de fallos, reducción de las probabilidades de la entrega de nuevas características entregadas a producción que resulten en una falla de operaciones.

Manejo automatizado de riesgos, Controles bien definidos para realizar la caracterización, monitoreo y mitigación de los riesgos a medida que se liberan los artefactos en cada fase, desde el diseño hasta la producción.

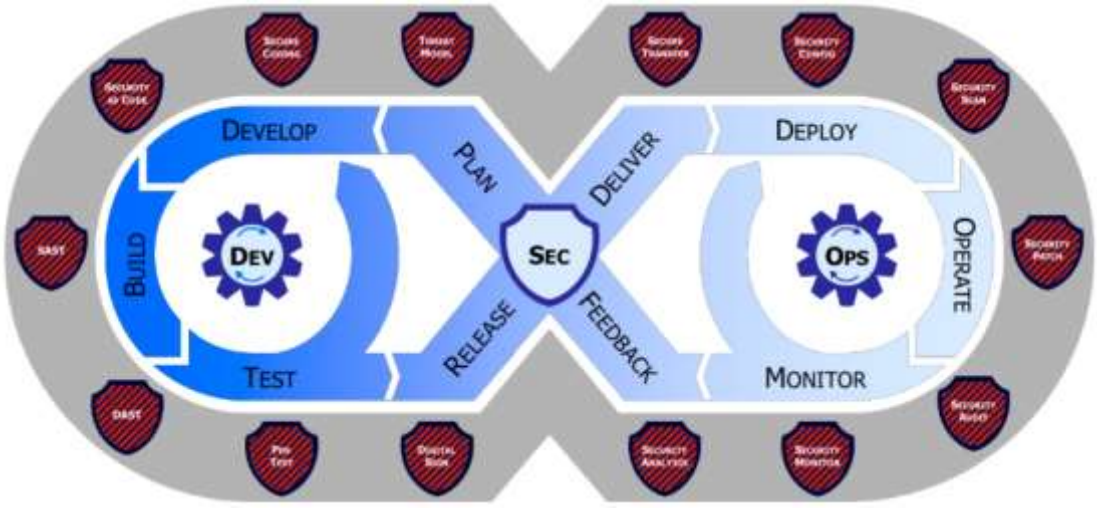
Ciberseguridad integrada, Software actualizado y parchado en cada entrega sin comprometer la funcionalidad de los artefactos.

Definición DevSecOps

En la guía de estrategia de DevSecOps del Departamento de Defensa de los Estados Unidos describe como unas prácticas culturales y técnicas dentro de una organización, de tal forma que estén alineados para reducir las brechas entre un equipo de desarrollo, un equipo de seguridad y un equipo de operaciones. Como se puede observar en **Figura *11*** adoptando mejores procesos mediante una colaboración diaria, flujos de trabajo agiles y series continuas de retroalimentación (Department of Defense USA, 2021).

Figura 11

Fases del ciclo de vida para DevSecOps



Nota. Ciclo de vida DevSecOps, tomado de (Department of Defense USA, 2021)

2.5. Resultados – Discusión

Ciclo de Vida de DevSecOps

Para poder adoptar la metodología DevSecOps dentro de las instituciones gubernamentales independiente del tipo de proyecto de desarrollo de aplicaciones en los diferentes equipos de trabajo es necesario garantizar un mínimo de representantes por cada área involucrada como ya hemos visto que se compone de Desarrollo, Operaciones y seguridad informática, que se encuentren comprometidos a realizar parte de los controles ,automatizaciones y monitoreo de la arquitectura utilizada como se muestra en la **Figura *11***.

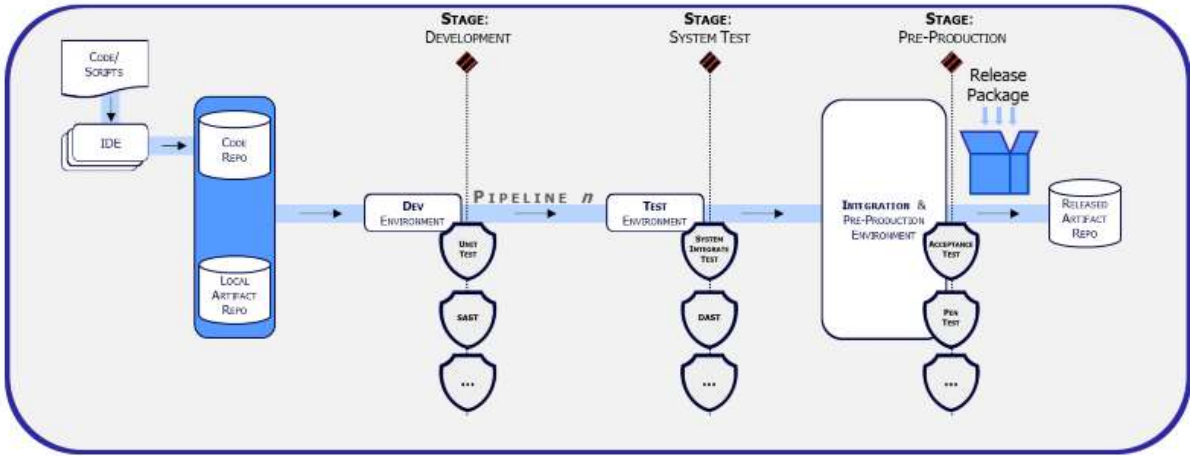
La metodología DevSecOps tiene iteraciones por diseño, esto quiere decir que el desarrollo de aplicaciones nunca finaliza y se encuentra permanentemente dentro del ciclo de vida del desarrollo con entregas cortas que se producen mediante unos procesos que pueden ser completamente automatizados o semiautomatizados con mínima intervención humana, de esta forma, se consigue acelerar la integración continua y la entrega continua, este ciclo es adaptable e incluye una serie de ciclos de retroalimentación que conducen a mejoras continuas en los procesos, (Department of Defense USA, 2021)

Pruebas de Seguridad

No existe una batería de pruebas de seguridad que satisfaga todos los escenarios, cada equipo de trabajo tiene sus propios requerimientos y restricciones, sin embargo los artefactos de software establecen puertas de control que son partes obligatorias al realizar un desarrollo aplicaciones informáticas en la **Figura *12*** muestra donde se debe ubicar cada una de las puertas de control en cada uno de los canales (*pipeline*) del proceso de desarrollo de software representadas por un rombo en la parte superior de la figura. Muestra además un flujo teórico e incompleto de los tipos de prueba en cada puerta a modo de ejemplo de los tipos de prueba en cada puerta, cabe recordar que estos canales pueden ser distintos y múltiples dentro de una colección concurrente de pruebas para maximizar la eficiencia.

Figura 12

Pruebas de Seguridad



Nota. tomado de (Department of Defense USA, 2021)

Las puertas de control son obligatorias, pero no se espera que todas sean completamente automatizadas desde el momento de iniciar con el desarrollo, por el contrario, casa requerimiento de desarrollo de aplicación tiene requerimientos únicos, tal como se lo realiza en las prácticas de desarrollo Ágil, esto hace que cada control requiera una intervención humana al inicio. El equipo de trabajo debe estar comprometido con la construcción de la automatización de las puertas de control, como muestra de mejores prácticas al inicio va a requerir mucha intervención por parte de los integrantes del desarrollo y gradualmente esta intervención decrecerá en favor de repeticiones automatizadas como parte de procesos de mejora continua.

Bucles de retroalimentación

Deben ser claros e identificables los ciclos de retroalimentación continua y se encuentran en seis ciclos diferentes. Como se visualizó en la en la **Figura *12***, existen tres puertas de control que están dentro de proceso CI/CD y dos puestas de control adicionales.

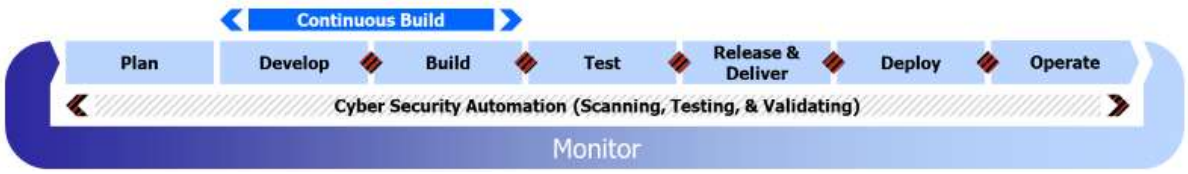
Compilación continúa

La compilación continúa en un ciclo o bucle de control que realiza su iteración entre las fases de desarrollo y compilado en una metodología DevSecOps como muestra la **Figura *13*** Compilación continua, si no se encuentra completamente satisfactorio la compilación debe ser devuelto al ingeniero que la envió para que solucione, sin una compilación exitosa, los pasos siguientes

no pueden avanzar ya que se encontraría incompleto y sin lógica, de aquí se puede tener la importancia de la retroalimentación.

Figura 13

Compilación continua



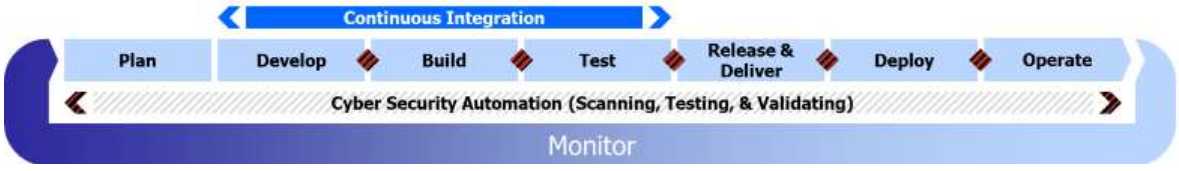
Los tipos comunes de retroalimentación en este bucle incluyen una compilación exitosa por la herramienta de compilado y una solicitud *pull* para crear la equivalencia de software de la integridad de dos personas, esta solicitud realizada en el ciclo de retroalimentación tiene como objetivo evaluar la arquitectura y estructura del software, identificando posibles regresiones que pueden introducirse de forma inadvertida para el desarrollador que está realizando el requerimiento de solicitud de fusión con la rama principal master así como identificar cualquier riesgo de seguridad o código confuso.

Integración Continua

La Integración continua (CI) es el ciclo de retroalimentación de iteración que se encuentra a través de las fases de DevSecOps de Desarrollo, compilado, y pruebas que se puede encontrar en la **Figura *14***. Posterior a que se complete de forma exitosa el ciclo de compilado continuo y solicitud de *pull* y fusión con la rama principal de desarrollo master, se ejecuta una serie de pruebas automatizadas, incluido un conjunto completo de pruebas de integración.

Figura 14

Integración Continua



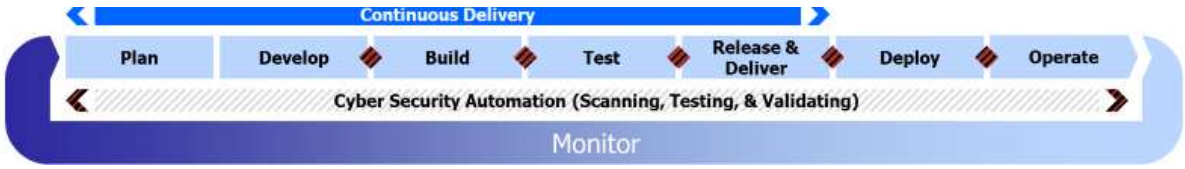
La ejecución automatizada de las pruebas de integración continua mejora la calidad de software al ser rápidamente identificados cuando una fusión con la rama principal falla produciendo excepciones, creando regresiones, corromper un API, etc.

Entrega Continua

El ciclo de retroalimentación de Entrega continua se lo realiza en las fases del ciclo de vida de DevSecOps desde plan, desarrollo, compilado, pruebas y entrega como se muestra en la **Figura *15*** Entrega Continua. El elemento más pertinente de resaltar en la fase es la Entrega que no significa que sea puesta en producción. Al encontrarse en esta etapa significa que el código ha sido escrito, revisado, fusionado con la rama principal y que ha pasado de forma exitosa todas las pruebas automatizadas. Esto puede hacer que puedan ser identificados con una versión dentro del código fuente en la herramienta de administración y despliegue en un repositorio de artefactos.

Figura 15

Entrega Continua



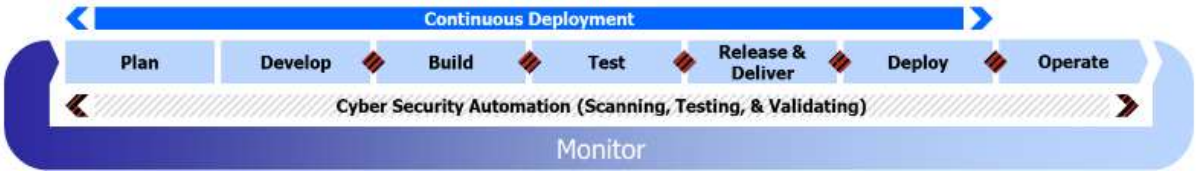
En este punto las características de los artefactos pueden ser desplegados y podrían implementarse sin que esto llegue a ser obligatorio, es una práctica común agrupar una serie de características en los artefactos de software para implementarlos en producción como una unidad.

Despliegue Continuo

El bucle o ciclo de retroalimentación de despliegue continuo se extiende desde plan, desarrollo, compilado, pruebas, entrega y despliegue dentro de las fases que comprende DevSecOps como lo muestra la **Figura *16***. La implementación es formalmente la acción de poner una o más funciones a producción de forma automatizada, este la primera puerta de control adicional fuera de los controles representados en el proceso CI/CD

Figura 16

Despliegue Continuo



Operación Continua

El ciclo de retroalimentación de operación continua inicia desde las fases de DevSecOps plan, desarrollo, compilado, prueba, entrega, despliegue y operación; como lo muestra la **Figura *17*** Operación Continua. La operación continua es una actividad enfocada en la disponibilidad, rendimiento y riesgo operacional del software.

Figura 17

Operación Continua

La disponibilidad es frecuentemente comparable con el concepto de acuerdo de niveles de servicio (SLA), las aplicaciones modernas se espera una disponibilidad cercana al cero de tiempo baja, es decir, un 99,99 % de disponibilidad del software (Department of Defense USA, 2021)

Monitoreo Continuo

Al final, incluido las fases de continuidad y retroalimentación que cubren por completo el ciclo de vida del DevSecOps deben permanecer en continuo monitoreo como lo muestra la **Figura *18*** Monitoreo Continuo. El monitoreo continuo recorre la totalidad del sistema de debe ser constantemente monitoreado y no solo como partes individuales, este enfoque nos asegura que los equipos no tengan opiniones erróneas sobre el software al observar los mínimos o máximos locales. Se monitorean todas las métricas agregadas desde el flujo de funciones hasta la puesta en producción.

Figura 18

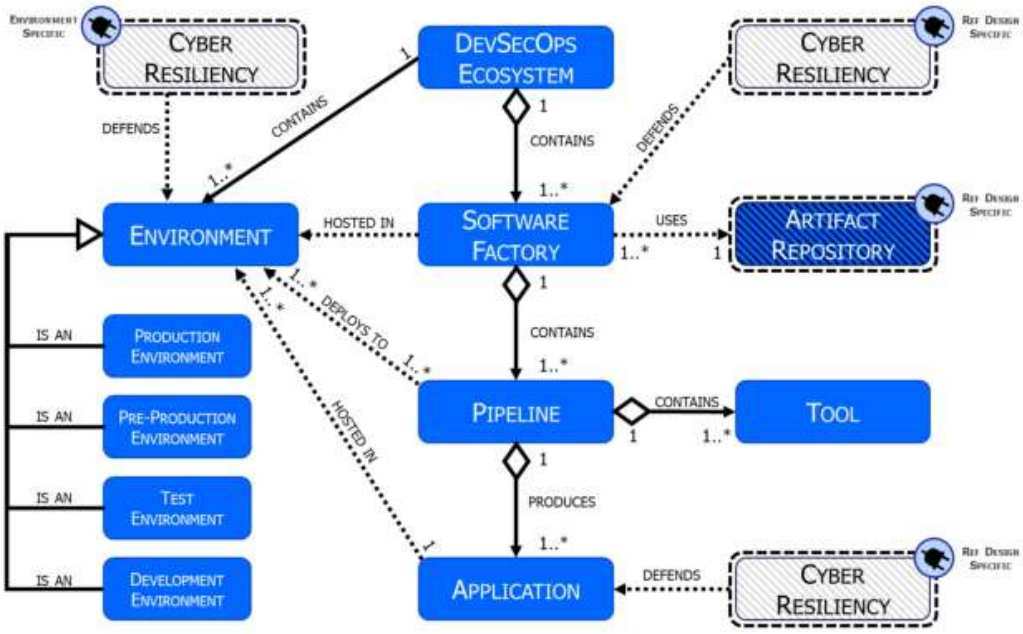
Monitoreo Continuo

Modelo Conceptual de plataformas DevSecOps

Cada plataforma de DevSecOps se compone de múltiples fábricas de software, varios entornos de desarrollo y herramientas, así como varias técnicas y herramientas de seguridad para el software resiliente en la **Figura *19*** se puede visualizar las relaciones entre estos y las cardinalidades esperadas.

Figura 19

Modelo Conceptual de Plataformas DevSecOps



A modo de ejemplo se muestra las actuales plataformas que adoptan una metodología de DevSecOps para el diseño referencial.

Arquitectura Kubernetes

La arquitectura Kubernetes en marco de DevSecOps es compatible para orquestar una colección de contenedores y su pila de seguridad informática que proporciona un monitoreo basado en “cero confianza” (*zero trust*) con detección de comportamiento.

Arquitectura de proveedores de servicios gestionados

Ecosistemas que ofrecen un completo ambiente enfocado en DevSecOps, El servicio administrado se encarga de los aspectos de parchado y seguridad del núcleo del entorno, que también se encuentra habilitado para un crecimiento mensual en caso de requerir y entornos de desarrollo (IDE) con características avanzadas como configuración, administración de repositorios, herramientas de compilado y en su mayoría basado en la nube

Arquitecturas Sin código RPA

Se define la necesidad de que sean escalables a cualquier tipo de requisitos operativos que necesite el software. Se producen avances rápidos en arquitecturas y herramientas de automatización de procesos robóticos *Robotic Process Automation* (RPA) con poco código o sin código, aun no existe un diseño referencial de metodología DevSecOps para este tipo de entornos.

Arquitectura sin servidor

La arquitectura sin servidor o *serverless* se confía en hardware totalmente administrado y escalable de una forma que permita al desarrollador de aplicaciones informáticas enfatizar en los procesos del negocio sobre la arquitectura, la arquitectura sin servidor está madurando rápidamente, con ofertas comerciales y bibliotecas de código abierto que se conectan a este tipo de ecosistemas, como la pila de kubernetes.

Validación de especialistas

Para realizar la validación requerida, se acude a profesionales que cumplan con la premisa del estudio investigativo realizado, es decir, profesionales que cuenten con la experiencia adecuada dentro de las distintas disciplinas mencionadas en la elaboración del presente documento como: Desarrollador de software y Operaciones tecnológicas, que son parte de las tecnologías de la Información y comunicación; además. Contar con experiencia profesional en los equipos de trabajo de instituciones gubernamentales que es hacia donde se encuentra dirigido el análisis.

Se valida que el objetivo del presente estudio investigativo cumple con los indicadores de Impacto, aplicabilidad, conceptualización, actualidad, calidad técnica, factibilidad y pertinencia, de acuerdo con el criterio emitido por los profesionales consultados, cuya ficha de aporte y validación se encuentra en el Anexo 2.

CONCLUSIONES

Se realiza el análisis de las distintas implementaciones de la metodología DevSecOps y que pueden ser adaptables dentro de los equipos de trabajo de las instituciones gubernamentales por lo que se determina que es una metodología aplicable en los entornos descritos al cumplir con los elementos que se necesitan para el desarrollo seguro.

Se realiza una evaluación de los distintos enfoques utilizados para realizar una aproximación a las metodologías de desarrollo seguro, buscando puntos de similitud con los equipos de trabajo e implementaciones realizadas que permitan realizar una transición planificada y controlada, de esta forma se realiza también una investigación de las metodologías de desarrollo Ágil y DevOps que son la base de donde surge el concepto de DevSecOps.

Se formula la propuesta con base a la investigación bibliográfica realizada con respecto a la metodología DevSecOps y en función de los hallazgos encontrados en los trabajos consultados cuidando que no hayan perdido la vigencia ya que al tratarse de la tecnología se tiene una evolución muy rápida de los conceptos aplicables, así como de las herramientas utilizadas para poder realizar esta implementación.

Se puede indicar el impacto que se tiene al aplicar una metodología DevSecOps dependiendo del nivel de madurez que tengan en los equipos de trabajo de las instituciones gubernamentales, pues en función de la experiencia y metodologías aplicadas que tengan al momento de adoptar un enfoque DevSecOps este tendrán un mayor o menor impacto y los beneficios de aplicar un ciclo de desarrollo propuesto serán claramente identificables evitando los reprocesos y mejorando los tiempos de respuesta y entrega.

RECOMENDACIONES

Para una implementación más personalizada y adaptada a la realidad de cada institución se requiere el compromiso de los involucrados en realizar el análisis empezando desde el nivel jerárquico superior llegando hasta los analistas que realizan la implementación de la metodología de desarrollo seguro DevSecOps.

Una implementación más exitosa que implique un menor impacto en las responsabilidades y tiempos de respuesta es necesario capacitar a los equipos de trabajo desde el momento que se encuentra realizando el estudio para la adopción de las metodologías seguras propuestas en el presente trabajo investigativo, así como nominar un líder que se encargue de realizar la planificación adecuada marcando los hitos necesarios para lograr una implementación exitosa.

Para la propuesta de la adopción de metodologías DevSecOps se debe observar que no se hayan perdido la vigencia de los conceptos y su aplicabilidad. Observando que las herramientas con las que se realiza la implementación tengan un adecuado soporte y puedan ser escalables con el paso del tiempo.

Medir el impacto una vez implementado la metodología DevSecOps y realizar controles periódicos de la metodología ajustando los requerimientos de acuerdo con las necesidades institucionales de cada organización gubernamental e implementar las nuevas tecnologías y conceptos con cada ciclo de desarrollo, así como socializando los beneficios obtenidos.

BIBLIOGRAFÍA

De Dios, M. (28 de enero de 2024). *WAM Global*. https://www.wearemarketing.com/es/blog/metodologia-scrum-que-es-y-como-funciona.html#

Department of Defense USA. (2021). *Enterprise DevSecOps Fundamentals.*

Department of Defense USA. (2021). *Enterprise DevSecOps Strategy Guide.*

Díaz, O., & Muñoz, M. (2018). Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización Mexicana. *RISTI, Revista Ibérica de Sistemas e Tecnologias de Informação*(26), 43-53. https://doi.org/https://doi.org/10.17013/risti.26.43-53

Elez, A., & López, J. (2023). Introducción a DevSecOps para la mejora de los procesos de desarrollo de software con herramientas Open Source. *Repositori Institucional (O2)*.

Fontela, C., & Paez, N. (2022). Hacia otro modelo de proceso de desarrollo de software. *Revista INNOVA*(10).

Gobierno Ecuador. (enero de 2024). *Catálogo de oferta nacional de software*. https://www.softwarepublico.gob.ec/listado-de-software-ecuatoriano/

Gobierno Ecuador. (26 de 02 de 2024). *Software Público*. https://www.softwarepublico.gob.ec/

Google Gemini. (08 de marzo de 2024). Gemini. *Prompt de la Inteligencia artifical de Google*.

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI Revista Ibérica de Sistemas y Tecnologías de Información*(E3). https://doi.org/10.17013/risti.e3.1-15

Naciones Unidas. (2023). *Informe de los Objetivos de Desarrollo Sostenible.* https://www.un.org/sustainabledevelopment/es/

Naupas Humberto, Valdivia Marcelino, Palacios Jesus, Romero Hugo. (2018). *Metodología de la investigación Cuantitativa - Cualitativa.*

Ñaupas, A., Valdivia, M., Palacios, J., & Romero, H. (2018). *Metodología de la investigación Cuantitativa - Cualitativa.* Ediciones de la U.

Open Source Initiative (OSI). (2024). *State of Open Source Report.*

Pachacuti, M. (2021). DevSecOps, Estado del Arte en el Contexto Boliviano. *Revista PGI*(7), 72-75.

Rajapakse, R., Zahedi, M., Shen, H., & Babar, A. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology, 141*. https://doi.org/https://doi.org/10.1016/j.infsof.2021.106700

Ramos, A., & Reclade, P. (2022). Balanceo y despliegue de carga en aplicaciones web mediante Kubernetes. *REVISTA ODIGOS, 3*(2), 75-89. https://doi.org/https://doi.org/10.35290/ro.v3n2.2022.585

RedHat. (15 de Marzo de 2023). *¿Qué es DevSecOps? Seguridad integrada dentro de DevOps*. https://www.redhat.com/es/topics/devops/what-is-devsecops

Salas Ocampo, D. (febrero de 2024). *Investigalia.* https://investigaliacr.com/investigacion/investigacion-biografica-narrativa/

ANEXOS

ANEXO 1

Catálogo de Software gubernamental

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
1	Propietario	INTERPRO	.Net (C#, Visual Basic.Net)	ISSOLUCIONES CIA. LTDA.	info@interpro.ec Teléfono: 07 410 7091 Dirección: Jose Enrique Rodo S/N y General Artigas
2	Propietario	COBUS BPM	C#, Javascript	COELLAR BURBANO SISTEMAS CIA. LTDA.	pcoellar@cobus.com.ec Teléfono: +593 9 9816 0114 Dirección: Autopista medio ejido S/N
3	Propietario	e-GOB	Java, Python, Ruby	TERRITORIOS INTELIGENTES -IT CIA.LTDA.	info@territoriosinteligentes.net Teléfono: +593 9 7936 7333 Dirección: Chaullabamba, Urb. Los Nogales
4	Propietario	ATLAS	Java, Android	ELECSOFTISA CIA.LTDA.	atlas@elecsoftisa.com Teléfono: +593 9 98737278 Dirección: Final de la Calle Sin Nombre y Princesa Pacha
5	Propietario	PayPhone	C#, Angular, NodeJS, Javascript, PHP, .Net Core, Blazor	ECUAPAYPHONE C.A.	info@livepayphone.com Teléfono: -593 9 5866 6066 Dirección: Pedro Calderón de la Barca, entre Gustavo Adolfo Becker y Francisco de Orellana
6	Código Abierto	Sistema Web Integral de Riesgos Financieros RISKWEB	Lenguaje PHP, Java Script, HTML	WEBCOOPEC SYSTEM CIA.LTDA.	juancarlosgc02@gmail.com Teléfono: +593 9 8406 9462 Dirección: Conocoto, La Salle 2 calle Carchi y Chimborazo s-22
7	Propietario	RED CAPITAL - Software empresarial	IFML, Java, JavaScrpt, Json, SQL	REDCAPITAL S.A.S.	gerencia@redcapital.ec Teléfono: +593 9 9958 7298 Dirección: Tránsito Amaguaña y Emiliano Zapata

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
8	Propietario	CG/Web ERP Financiero Administrativo y Personal	.Net lenguaje C# y ASP.net	INFORMACION TECNOLOGICA DEL ECUADOR LUXEINFORM S.A.	veronica.alarcon@itdelecuador.com Teléfono: +593 9 9629 4484 Dirección: Av. Orellana E2-08 y Av. 10 de Agosto Edif. “EL CID” 8vo Piso
9	Código Abierto	KGESTIONA - KSISCAT	PHP, JAVASCRIPT, JQUERY	SANDOVAL PASPUEL JOSE ANDRES	jasapas@hotmail.com Teléfono: +593 9 9854 19316 Dirección: Av. Cardenal de la Torre pasaje Pilalo
10	Código Abierto	ORIGAMI GT (Gestión Total) (Programa de ordenador) (Software)	JavaEE, Java Server Faces, Primefaces	TECH2GO S.A.	tech2gosa@gmail.com Teléfono: 04 6011847 Dirección: Cdla. Simón Bolívar 5to pasaje 2A NE MZ 5 SL 88 y Av. de las Américas
11	Propietario	SYSOP – PLATAFORMA DE APROVISIONAMIENTO AUTOMATICO DE ELEMENTOS DE RED.		IDROVO CASTANEDA XAVIER ESTEBAN	xavieridrovo@gmail.comTeléfono: +593 9 8417 0646Dirección: Portales De Misicata N9
12	Código Abierto	SOFTLIDER ERP (SAGA)	PHP, React sobre Node js / Ambiente Web /	SOFTLIDER CIA. LTDA.	fabian.mendieta@saga.ec Teléfono: +593 9 8311 0596 Dirección: Av. del Estadio y Florencia Astudillo Junto a PYCCA
13	Propietario	Sistema de Gestión Empresarial ERP OLYMPO	Phyton con base de datos SQL Postgres 9.3 o superior.	PROTELCOTELSA S.A.	administracion@protelcotelsa.com Teléfono: +593 9 9843 8182 Dirección: Gregorio Bobadilla N37-128 y Juan Jose Villalengua
14	Propietario	SWITCH TRANSACCIONAL ITRANS e ITCONSOLE	JAVA, XML, JSF (Primefaces version 10),	G2C - INTEGRADORES S.A.	william.castro@g2cintegradores.net Teléfono: +593 9 9791 6630

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
			Maven, EJB		
15	Propietario	eDoc (Facturación Electrónica)	C#, NetFramework, NetCore, Javascript	GURUSOFT S.A.	maite.mora@guru-soft.com Teléfono: +593 9 6025 0366 Dirección: Av. de las Américas 510 Edificio Sky Building Piso 4 Oficina 409
16	Propietario	DBTOOL	JAVA, JSF, PRIMEFACE	DPSOFT SERVICES CIA. LTDA.	gerencia@dpsoft.co Teléfono: +593 9 9522 1252 Dirección: San Ignacio E10-25 y San Javier
17	Propietario	Acosux	Java Empresarial, Angular.	OBINTE WEB SERVICES OWS CIA.LTDA.	gerencia@obinte.com Teléfono: +593 9 8724 1608 Dirección: Vela 907 y Kleber Franco
18	Propietario	ADPIN	VISUAL STUDIO .NET , JAVA	INTRIAGO CRESPO DAVID ALFREDO	davidintriagoc@hotmail.com Teléfono: +593 9 9188 4160 Dirección: Av. Sucre y Homero López
19	Propietario	ERP CABILDO	PLSQL , JAVA, JAVASCRIP PHP, PYTHON , PGSQL	RISHARD PROFESIONALISMO CIA. LTDA.	wlasan@hotmail.com Teléfono: +593 9 5984 4980 Dirección: Nuñez de Balboa OE2- 140 y Juan de Piñas
20	Propietario	DIGIFILE	Angular 7 y Base de Datos MongoDB	RICAURTE RAMIA NELSON DAVID	jparreno@dox-ec.com Dirección: Urdenor 2 Mz 244 Solar 4
21	Propietario	AXIS	Oracle Internet Developer Suite, Oracle PL/SQL, HTML, JSON, JQuery, XML, Android Studio y Java	YOVERI S.A.	cdelcampo@yoveri.com.ecDirección: Km.1.5 Via Samborondón Edificio Samborondón Business Center

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
					lmolina@onlycontrol.com
22	Propietario	ACCESS CONTROL	Visual 6.0	ONLY CONTROL S.A. CONONLY	Teléfono: 04 6003559 Dirección: Urdesa Central, Circunvalación Norte No. 413 Entre calle 5ta y 6ta MZ. 16a lmolina@onlycontrol.com
23	Propietario	TIME CONTROL	Visual Basis 6.0	ONLY CONTROL S.A. CONONLY	Teléfono: 04 600 3559 Dirección: Urdesa Central, Circunvalación Norte No. 413, entre calle 5ta y 6ta MZ. 16a sfalconi@logiciel-ec.com
24	Propietario	LogiFlow Plataforma de procesos de negocio	.NET	LOGICIEL CIA LTDA	Teléfono: +593 9 8443 9578 Dirección: Lugo N24-267 y Vizcaya. Edificio DESTRO piso 3 sfalconi@logiciel-ec.com
25	Propietario	GAF Gestión de Activos Financieros	ILERPG/400 y CL/400.	LOGICIEL CIA LTDA	Teléfono: +593 9 8443 9578 Dirección: Lugo N24-267 y Vizcaya. Edificio DESTRO piso 3
26	Propietario	ECUFAC ERP	PHP, JAVASCRIPT, AJAX, PYTHON para Linux y C# para Windows, MySQL	ESPIN AGUIRRE FERNANDO JAVIER	jespin@sairexsol.com Teléfono: +593 9966 49162 Dirección: Corazón de Jesus 205 y Galápagos
27	Propietario	Caiman Inmunizador Antimalware	Scripting, Visual Basic	CANO HOLGUIN JAIRO CARLOS	jairocano@debianware.com Teléfono: +593 9930 98401 Dirección: Cdla. La Atarazana Mz. M4 #18
28	Propietario	ONLY BITÁCORA	VISUAL BASIC 6.0	ONLY CONTROL S.A. CONONLY	rrhh@onlycontrol.com Teléfono: 046003559 Dirección: Urdesa Central, Circunvalación Norte No. 413 entre calles 5ta y 6ta
29	Propietario	SIGE	Visual Studio, Java, PHP, B4X	ALVARADO BRAVO JAVIER ESTUARDO	jalvaradobravo@hotmail.com Teléfono: +593 9984 23257

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
					Dirección: Batán 7-42 y Unidad Nacional
30	Propietario	Full-Time Web 2.7 Versión Cerrada	Java (Aplicacion), SQL y Groovy (Reporteria), C# (Modulo de descarga), Java (Reloj Virtual)	CASA LUIS PAZMIÑO IMPORT & EXPORT S.A.	joseluis@casapazmino.com.ec Teléfono: +593 9870 05431 Dirección: Grecia N32-85 y Av. Mariana de Jesus
31	Propietario	Konnet.app	Framework Ruby on Rails.	BIM SOLUCIONES I.C. S.A.	gerencia@bimsoluciones.comTeléfono: +593 9804-16278Dirección: Av. Naciones Unidas y Nuñez de Vela
32	Propietario	The Q-NOW Asistente Digital para Sistemas de Gestión Empresariales	PHP - Framework Laravel, Javascript, HTML - CSS	OLLAGUE GONZALEZ LUIS STALIN	imaginamerica@gmail.com Teléfono: +593 9977 39918 Dirección: Francisco Andrade Marín E6-140
33	Propietario	SmartSuite	C# Javascript, HTML5, CSS3	VITERI SANCHEZ JUAN SIMON	jsviteri@gmail.com Teléfono: +593 9 9863 7439 Dirección: Av. República el Salvador N35-164 y Suecia
34	Propietario	SIO SISTEMA DE GOBIERNO DIGITAL	PHP	TECHREV S.A.S.	jlorences@knights.ucf.edu Teléfono: +593 9 9160 0766 Dirección: Torres Bellini
35	Propietario	SISTEMA INTEGRADO GEOGRAFICO CATASTRAL Y ORDENAMIENTO TERRITORIAL (SIGCOT)	El lenguaje de desarrollo: ASP .Net (C#) ambiente MVC, HTML, Javascript y CSS Entorno de desarrollo integrado: Asp.NET MVC	HERNANDEZ CHILAN JOSE RAMON	joseher72@hotmail.com Teléfono: +593 9 8651 3778 Dirección: Cdla. El Maestro Calle Isabel Vera Loor y Segunda Transversal

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
36	Propietario	AS2 ERP	JAVA 8.x	ASINFO-SOFTWARE & DESARROLLO S.A.	estefania.morales@grupoasinfo.com Teléfono: +593 9 8327 3423 Dirección: Alberto Guerrero N34-30 Y Federico Páez
37	Propietario	MEDIO INFORMÁTICO DE CONTROL Y ADMINISTRACIÓN DE LA RECAUDACIÓN	FRAMEWORK SCRIPTCASE EN PHP Y MYSQL	CAPTHOT CAPACITACIÓN TALENTO HUMANO Y TECNOLOGIA S.A.	birivera@gmail.com Teléfono: +593 9 9802 4748 Dirección: Rábida y Santa Maria
38	Código Abierto	RISKWEB	Linux, Apache, Php, JavaScript, Mysql	GUAYASAMIN CATTANI JUAN CARLOS	juancarlosgc02@gmail.com Teléfono: +593 9 8406 9462 Dirección: calle, García Moreno 88 y Espejo
39	Código Abierto	Software Autoradio SWM G01	Aplicación principal: JavaFirmware: C	ALTERNATIVE REPLACEMENT CAR SOLUTIONS ALTERNACARS S.A.	crivadeneira@alternacars.comTeléfono: +593 98779 8321Dirección: Antonio Játiva S8-300 y Juán de Alcázar
40	Código Abierto	SOFTWARE PARA AUTORADIO GREAT WALL WINGLE 7	Aplicación principal: Java, MCU: C	ALTERNATIVE REPLACEMENT CAR SOLUTIONS ALTERNACARS S.A.	crivadeneira@alternacars.com Teléfono: +593 98779 8321 Dirección: Antonio Játiva S8-300 y Juán de Alcázar
41	Código Abierto	Sistema de Gestión Ambiental	PHP, JAVASCRIPT, REACT, JQUERY, AJAX, HTML, JAVA	ASQUI POMA JAIME EDUARDO	eduardoasqui@gmail.com Teléfono: +593 9 9609 0939 Dirección: Pichincha y Chimborazo

N°	Modalidad	Nombre del software	Lenguaje de programación	Proveedor	Contacto
42	Propietario	Aptimo Inteligencia Empresarial e Institucional	Lenguaje PHP Framework Laravel, y Angular con base de datos SQL Postgres 12 o superior.	TODOTEK S.A.	jpcorrea@todotek.net Teléfono: +593 9 9300 9182 Dirección: Av. Fco. de Orellana Urdenor 1, Mz 106, Villa 9
43	Propietario	ERPMunicipal	Java JEE, Angular, Springboot, Ionic	SISTEMAS INFORMATICOS TECNOPRO CIA. LTDA	babendan@tecnopro.net Teléfono: +593 9 9959 6214 Dirección: Shyris y Suecia
44	Propietario	XPERTUS WEB - ACTIVOS FIJOS	ASP. Net, C#, SQL Server Express	VASQUEZ FLORES GERMAN PATRICIO	pvasquezf@yahoo.com Teléfono: +593 9 9565 0947 Dirección: Jose Viteri SN y Giovanni Calles
45	Propietario	DBTWICE	SQL, PLSQL, Java, javascript, Phyton	REDPARTNER S.A.	alexandra.cevallos@red-partner.com Teléfono: +593 2600 7777 Dirección: Av. 12 de Octubre N24562 y Cordero
46	Propietario	Zero POS	PHP, C#, Angular, Flutter	CODE STRUCTURE SOFTWARE & SOLUTIONS FOR BUSINESS S.A.	info@code-structure.com Teléfono: +593 98435 3273 Dirección: La Bota N6834 Y Av. Lorena Ambimanay
47	Propietario	METRIX - Lectura Inteligente de Medición	Javascript, Flutter	SUPTELEC S.A.	pbarrera@supertel.com.ec Teléfono: +593 9 9582 7109 Dirección: La Pradera N-38 y Av. Diego de Almagro

ANEXO 2

Validación de especialistas

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Miguel Llumihuasi

Título obtenido
Ingeniero en Sistemas Informáticos
Cédula de Identidad
1002352753
E- mail
miguel.llumihuasi@asambleanacional.gob.ec
Institución de Trabajo
Asamblea Nacional
Cargo
Líder de Infraestructura y Operaciones Tecnológicas - CGTIC
Años de experiencia en el área
13

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales.

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*					
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		***X***			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	***X***				
Total		*25*	*8*			

Observaciones:

Una conceptualización adecuada y pertinente al concepto de desarrollo seguro.

Recomendaciones

Se puede ampliar la aplicabilidad citando casos de uso específicos.

Lugar, fecha de validación: Quito, 08 marzo de 2024

Firma del especialista

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Diego Guzmán

Título obtenido
Ingeniero en Computación
Cédula de Identidad
1712941002
E- mail
diego.guzman@caces.gob.ec
Institución de Trabajo
Consejo de Aseguramiento de la Calidad de la Educación Superior
Cargo
Desarrollador de Software
Años de experiencia en el área
11

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	***X***				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		***X***			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***X***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	***X***				
Total		*25*	*8*			

Observaciones:

Se puede aplicar varios enfoques del desarrollo seguro que no necesariamente son útiles para todos los equipos de trabajo por lo que no se puede realizar generalizaciones a partir de la documentación.

Recomendaciones

El estudio como se encuentra planteado no solo sería aplicable a entidades del gobierno sino también a instituciones del sector privado.

Lugar, fecha de validación: Quito, 08 marzo de 2024

Firma del especialista