FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

“IMPACTO AL INTEGRAR DEVSECOPS DURANTE EL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE EN LAS ORGANIZACIONES A NIVEL MUNDIAL 2023-2024”

SUSTENTADO POR:

LILIANA JAZMIN MEJIA PALMA

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

EL PROGRESO, YORO, HONDURAS, C.A.

ABRIL, 2025

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

IMPACTO AL INTEGRAR DEVSECOPS DURANTE EL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE EN LAS ORGANIZACIONES A NIVEL MUNDIAL 2023-2024

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JESUS RIGOBERTO RODRIGUEZ RIVERA

MIEMBROS DE LA TERNA:

CARLOS ROBERTO AMADOR ALVARENGA

JOSE RODOLFO SORTO BUESO

ANTHONY STEVE BARAHONA ESPINOZA

FACULTAD DE POSTGRADO

IMPACTO AL INTEGRAR DEVSECOPS DURANTE EL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE EN LAS ORGANIZACIONES A NIVEL MUNDIAL 2023-2024

Liliana Jazmín Mejía Palma

Resumen

El propósito de esta investigación es conocer el impacto al integrar DevSecOps durante el ciclo de vida de desarrollo de software en las organizaciones a nivel mundial en los años 2023 y 2024.

Se realizó el análisis de los datos de las fuentes secundarias seleccionadas, se establecieron dos hipótesis relacionadas con los factores de tiempo y costos se utilizó la prueba t y chi cuadrado para comprobar las hipótesis. Se identificó que si hay un impacto directo en los costos al tener un nivel ato de adopción de prácticas de DevSecOps donde se reduce considerablemente en comparación con las organizaciones que tienen un bajo nivel de adopción. Se identificaron los diez principales desafíos a los que se han enfrentado las organizaciones que han decidido adoptar DevSecOps. Se identificaron cuáles son los criterios que más toman en cuenta las organizaciones al seleccionar las pruebas de seguridad y cuáles han sido los cambios que se han tenido en las tasas de adopción de prácticas de DevSecOps.

Palabras claves: (Desarrollo, DevSecOps, Seguridad, Software)

GRADUATE SCHOOL

IMPACT OF INTEGRATING DEVSECOPS DURING THE SOFTWARE DEVELOPMENT LIFECYCLE IN ORGANIZATIONS WORLDWIDE 2023-2024

Liliana Jazmín Mejía Palma

Abstract

The purpose of this research is to understand the impact of integrating DevSecOps during the software development lifecycle in organizations worldwide in the years 2023 and 2024. Data from selected secondary sources was analyzed. Two hypotheses related to time and cost factors were established. The t-test and chi-square test were used to test the hypotheses. It was identified that there is a direct impact on costs with a high level of adoption of DevSecOps practices, which are significantly reduced compared to organizations with a low level of adoption. The ten main challenges faced by organizations that have decided to adopt DevSecOps were identified. The criteria most often considered by organizations when selecting security tests were identified, as well as the changes in the adoption rates of DevSecOps practices.

Palabras claves: (Development, DevSecOps, Security, Software)

DEDICATORIA

La presente investigación es dedicada a mi familia en especial a mi madre, a mi padre y mis hermanos que me han apoyado incondicionalmente a lo largo de mis estudios de postgrado.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por darme la oportunidad de culminar mis estudios dándome la sabiduría y la fuerza para afrontar cada desafío.

En segundo lugar, le agradezco a mi familia, a mi madre Cándida Palma por siempre apoyarme y darme motivación para culminar mis estudios de postgrado y a mis hermanos Wilmer, Karen y Sohany por siempre ayudarme y a mi padre Dolores Mejia.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

En la actualidad, la mayor parte de las organizaciones cuentan con un equipo interno o externo de desarrollo de software encargado de crear, mantener y actualizar los sistemas de información y además tienen la tarea de que los datos de los sistemas se mantengan seguros y no sean alcanzables o visibles para las personas no autorizadas, para ello es necesario la integración de DevSecOps durante todas las fases el ciclo de vida de desarrollo de software (Software Development Life Cycle o SDLC).

El SDLC, es un proceso completo y estructurado de innovación tecnológica que permite crear y diseñar software de calidad en el menor tiempo posible y a bajo costo, que incluye varias etapas como Planificación, Diseño, Desarrollo, Implementación, Pruebas y Mantenimiento. (Amazon Web Services, Inc., 2024; Check Point Software, 2024)

DevOps, surge de la unión de las palabras development(desarrollo) y operations (operaciones), es un conjunto de herramientas que ayudan a integrar los procesos que comparten el equipo de desarrollo de software y el de operaciones TI. Su enfoque es mejorar la comunicación y colaboración entre los equipos y la automatización de la tecnología. (Atlassian, 2024; Gartner, 2024; Redhat, 2022; Redondo et al., 2022a)

DevSecOps, Desarrollo, Seguridad y Operaciones se refiere a la integración de prácticas de seguridad a DevOps. Es un marco que sirve de referencia para la integración de seguridad en todo el SDLC, es cada vez más utilizado por los equipos de desarrollo para mantener la seguridad desde el inicio hasta el final del desarrollo de software. Incluye herramientas y procesos que aumentan la colaboración entre los equipos de desarrolladores de software, los equipos de seguridad y los equipos de operaciones de TI con el objetivo de crear software que pueda hacer frente a las amenazas actuales de ciberseguridad. (Amazon Web Services, Inc., 2024; Microsoft, 2024)

Esta investigación tiene como finalidad analizar cuál es el impacto en las organizaciones que integran DevSecOps en todo el SDLC: identificando que prácticas de DevSecOps se pueden integrar en cada fase del SDLC, analizando cómo esta integración nos permite reducir y optimizar los tiempos y costos de desarrollo de software relacionados con la identificación y corrección de vulnerabilidades, y conociendo como los equipos de desarrollo perciben y se adaptan a la integración de DevSecOps.

En el capítulo I, se presentarán los antecedentes y el planteamiento del problema que motiva la investigación. Se formularán las preguntas de investigación y se establecerán los objetivos de la investigación, tanto generales como específicos. Finalmente, se incluirá la justificación que explique la relevancia e importancia de la presente investigación.

En el capítulo II, se describirá el marco teórico que sustenta la investigación, se abordará el macro y microentorno, donde se explicara las condiciones externas e internas que influyen en el tema de investigación, se presentarán las teorías de sustento, las metodologías temáticas, se enumerarán las herramientas a utilizar, se definirá la conceptualización y el marco legal tanto nacional como internacional.

En el capítulo III, se detallará la metodología de la investigación, mencionando cuál es el enfoque y alcance de la investigación, se describirá la población, muestra y que técnicas de muestreo se utilizaron, los criterios para la selección de los datos, las hipótesis, las variables identificadas, las técnicas, los instrumentos y procedimientos aplicados, el plan de análisis, las fuentes de información que fueron seleccionadas y por último la matriz de congruencia metodológica.

En el capítulo IV, se detallarán los resultados y análisis de los datos, incluyendo una Descripción general del conjunto de datos, el proceso para la preparación y visualización de datos lo que forma parte del análisis exploratorio de los datos. Además, se incluye un breve informe del proceso de recolección de datos donde se mencionan las fuentes de información, los instrumentos utilizados, las dificultades encontradas y las consideraciones éticas.

En el capítulo V, se trata sobre las conclusiones y recomendaciones de la investigación después de haber realizado el análisis de los datos.

En el capítulo VI, se detallará la aplicabilidad de la aplicación mencionando el nombre de la propuesta, la justificación y alcance estableciendo los objetivos que tendrá la propuesta. Luego se detallará la descripción y desarrollo de la propuesta, las medidas de control y la planificación del cronograma y presupuesto de implementación.

1.2 ANTECEDENTES DEL PROBLEMA

A nivel mundial, han ocurrido muchos ataques a los sistemas de información de las organizaciones de diferentes rubros, financiero, comercial, educativo, etc.., ya sea ataques por personas externas o internas de la organización. Los hackers, ciberdelincuentes o personas que intentan ingresar a un sistema de la organización, aprovechan cualquier vulnerabilidad que puedan

encontrar en el software para intentar acceder a la información confidencial de la organización, ya sea para fines económicos, al robar o secuestrar información y pedir un beneficio económico a cambio, o para otros fines como dañar la reputación de la organización y detener u obstaculizar el desarrollo de las operaciones de la organización.

En el año 2021, los ataques cibernéticos se clasificaron el quinto riesgo más alto y se han convertido en un nuevo estándar para los sectores públicos y privados. En 2022, este riesgo siguió creciendo y se espera que para el 2025 los ataques se dupliquen. Los ataques aumentaron un 600% como resultado de la pandemia de COVID 19, ataques con el objetivo de robo y corrupción de los datos obligando a que las industrias adoptaron nuevas soluciones para la protección y seguridad de los datos. (Gutierrez, 2024)

Algunas estadísticas relevantes relacionados sobre la Ciberseguridad son: el 62,7% de las empresas creen que los ciberataques han aumentado desde el año 2020 debido a la pandemia de COVID-19. Un dato interesante es que a una compañía le toma aproximadamente 6 meses detectar una brecha de seguridad. Se proyecta que el daño relacionado a ciberataques llegará a los $10,5 trillones de dólares anuales para el 2025. El 86 por ciento de las brechas de seguridad tienen una motivación financiera. En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática. 63% de las intrusiones maliciosas en redes son resultado de datos de autenticación (nombres de usuario y contraseñas) que han sido comprometidos en otros ciberataques. Según una encuesta a organizaciones en Estados Unidos y el Reino Unido, la mayor preocupación de las empresas son las fugas o exfiltraciones de datos con un 36%, superando incluso al malware. (Magazine, 2018; Osborne, 2025; Prey, 2021)

Honduras ocupa el puesto 57 entre 108 países analizados por el CEI (Índice de Exposición a la Ciberseguridad), lo que implica que es el segundo país de América Central más expuesto a ataques cibernéticos, después de El Salvador. Muchos de los ataques son provocados por vulnerabilidades en los sistemas informáticos. (Hincapie, 2024)

En 2023 se registraron 1.8 millones de ataques dirigidos a sistemas tecnológicos de empras e instituciones hondureñas. En Centroamérica diariamente se reportan más de 500 ataques, de esa cantidad cerca del 20% son dirigidos a Honduras, algunos de los sectores más afectados son el gobierno, sector financiero, educación, call center y manufactura. (Zapata, 2024)

En Honduras, han ocurrido ataques de diversos tipos en su mayoría son ataques de

ramsomware, algunas de las que se han visto afectados por ataques de ciberseguridad ha sido Claro la cual es una de las empresas más grandes de telecomunicaciones el ataque ocasionó problemas en los servicios que ofrecen a sus clientes y parte de sus operaciones se vieron afectadas lo cual le generó pérdidas monetarias a la empresa, además de que posiblemente se logró acceder a información confidencial de los clientes. En los últimos años el número de ciberataques en Honduras ha ido incrementando en relación a los años anteriores, los ciberataques se han realizado a empresas privadas, públicas, con o sin fines de lucro. (Central, 2024; Grupo Kapa 7, 2024; Juan Carlos Rivera, 2023)

Por todo lo mencionado anteriormente, se hace necesario que las organizaciones donde existen áreas de desarrollo de software inicien a integrar prácticas DevSecOps en todas las fases del SDLC para poder mitigar vulnerabilidades desde el inicio hasta el final del desarrollo de software y de esta manera asegurar la integridad, confidencialidad y disponibilidad de la información que contienen sus sistemas informáticos.

Para comprender cuál es el impacto al integrar DevSecOps en todo el SDLC en una organización, se debe identificar que prácticas se pueden integrar en cada fase del SDLC, analizar cómo influyen en factores como tiempo y costos de desarrollo y conocer cómo los equipos de desarrollo perciben la integración de estas prácticas y como se adaptan a ellas.

1.3 PLANTEAMIENTO DEL PROBLEMA

DevSecOps en el SDLC es utilizado a nivel mundial por las organizaciones en especial por los equipos de desarrollo de software para evitar que se presenten vulnerabilidades en sus sistemas de información, reducir los ataques por personas u organizaciones malintencionadas que intentan acceder a datos e información confidencial, y para desarrollar software de calidad.

Esta investigación se enfocará en conocer cuál es el impacto que una organización puede lograr al integrar DevSecOps en todo el SDLC, cómo identificar las vulnerabilidades en el software desde el inicio de su desarrollo hasta la fase final, y conocer que beneficios se pueden obtener en cuanto a factores como el tiempo y costos de desarrollo de software. Además, busca mostrar cuál es la percepción de los equipos de desarrollo al integrar DevSecOps en el SDLC y cómo se adaptan a ellas.

Además, la integración de DevSecOps en el SDLC permite la creación de software con mayor calidad que pueda hacer frente a las amenazas y vulnerabilidades que se puedan presentar, para ello también se hace necesario conocer las amenazas y los tipos de ataques más comunes que se

han presentado últimamente para tomarlos en cuenta al momento de iniciar con SDLC.

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Cuál es el impacto en las organizaciones al integrar DevSecOps en el ciclo de vida de desarrollo de software y cómo los equipos de desarrollo perciben y adoptan estas prácticas?

1.4.2 PREGUNTAS ESPECÍFICAS

- ¿Qué prácticas de DevSecOps se pueden integrar en el desarrollo de software para identificar vulnerabilidades y mitigar amenazas que se puedan presentar cuándo el software se encuentre en producción?
- ¿Cuál es el impacto en el tiempo de entrega de desarrollo y los costos de desarrollo de software por la implementación de DevSecOps?
- ¿Cómo perciben y adoptan los equipos de desarrollo la integración de DevSecOps en el SDLC?

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

Analizar el impacto en las organizaciones al integrar DevSecOps durante el ciclo de vida de desarrollo de software y conocer como los equipos de desarrollo adoptan la integración de estas prácticas.

1.5.2 OBJETIVOS ESPECÍFICOS

- Identificar que prácticas de DevSecOps se pueden integrar en el desarrollo de software que ayuden a identificar vulnerabilidades y mitigar amenazas que se pueden presentar cuando el software se encuentre en producción.
- Analizar si la implementación de DevSecOps permite ahorrar en costos de desarrollo asociados a la identificación y mitigación vulnerabilidades en el software desde el inicio de desarrollo y verificar si el tiempo de entrega del desarrollo de software disminuye al implementar DevSecOps
- Conocer cuál es la percepción y adopción de DevSecOps por parte del equipo de desarrollo de la organización.

1.6 JUSTIFICACIÓN

En la actualidad, las organizaciones enfrentan el desafío de mantener un ritmo ágil de

entrega de software sin comprometer la seguridad. Si bien las prácticas tradicionales de DevOps han permitido acelerar los ciclos de desarrollo y despliegue, han dejado en evidencia limitaciones importantes cuando se trata de integrar la seguridad de forma temprana y eficaz. En muchos casos, los controles de seguridad se aplican en etapas finales del ciclo de vida del software, lo que implica mayores costos y riesgos si se identifican vulnerabilidades tardíamente.

En este contexto, DevSecOps representa una evolución natural y necesaria. A diferencia de DevOps, que se centra principalmente en la colaboración entre desarrollo y operaciones, DevSecOps incorpora la seguridad como un tercer pilar desde las primeras etapas del SDLC (Software Development Life Cycle). Esto permite que las vulnerabilidades se detecten y solucionen durante el diseño, codificación y pruebas, evitando costosos retrabajos posteriores y reduciendo significativamente los tiempos de respuesta ante incidentes de seguridad.

La integración de DevSecOps en el SDLC, es esencial para asegurar que el desarrollo de software genere sistemas de calidad que sea capaz de evitar y controlar los accesos no autorizados a la información, reduzca los ataques y pueda mitigar las vulnerabilidades que se pueden presentar.

Esta investigación es de suma importancia para conocer que prácticas de DevSecOps se pueden integrar desde la fase inicial hasta la fase final del SDLC y además analizar como los equipos de desarrollo de software perciben y se adaptan a la integración de estos tipos de prácticas.

La investigación también permitirá conocer cómo influye la integración de DevSecOps en factores cómo el tiempo y costos desarrollo de software, esto ayudará a que las personas que tengan acceso a la investigación puedan comprender que beneficios tangibles pueden obtener las organizaciones que deciden integrar DevSecOps en el SDLC.

La adopción de las prácticas de DevSecOps no solo mejora la seguridad del software, sino que ayuda en la optimización de los recursos en los procesos desarrollo, permitiendo entregas más rápidas y eficientes de productos de alta calidad, ya que permite automatizar prácticas como el escaneo de vulnerabilidades, las pruebas de seguridad y la implementación continua permitiendo a los equipos de desarrollo enfocarse en generar valor sin interrupciones innecesarias.

Dado a que la cantidad de ataques a la seguridad de los sistemas ha ido incrementando con el pasar de los años se hace necesario conocer como implementar DevSecOps en el SDLC incluyendo prácticas como el escaneo del software, pruebas de penetración, pruebas unitarias en los componentes, automatización de implementación, entre otras. Al hacerlo se busca que el software desde su creación y diseño sea robusto y seguro que puede hacer frente a las amenazas

actuales y a los ataques que se han presentado, garantizando así su seguridad una vez este implementado y en producción siendo utilizados por los usuarios finales. (Grupo Kapa 7, 2024)

La implementación de DevSecOps fomenta la colaboración entre los equipos de desarrollo, operaciones y seguridad para crear un entorno donde la seguridad sea una responsabilidad compartida. La seguridad se aborda desde el inicio del desarrollo de software lo que puede ayudar a los equipos a identificar y abordar problemas de seguridad de manera proactiva, en lugar de reactiva. Esto no solo mejora la calidad del software desarrollado, sino que también fortalece la confianza de los clientes y usuarios en los sistemas desarrollados.

CAPÍTULO II – MARCO TEÓRICO

En este capítulo, se analizará el macroentorno y microentorno de la adopción de DevSecOps las organizaciones en los diferentes países, las cuales les ayudan a identificar y mitigar las vulnerabilidades y de esta manera prevenir o poder hacer frente a ciberataques, además se identificarán las teorías de sustento que apoyan la importancia de conocer el impacto en las organizaciones que integran DevSecOps en el SDLC.

Además, se detallarán las metodologías que se utilizarán a lo largo de la investigación para conocer como implementar DevSecOps en el SDLC y que herramientas son necesarias para llevar a cabo la investigación.

2.1 MACROENTORNO

A nivel mundial, han aumentado los ciberataques a empresas de diversos rubros por vulnerabilidades o brechas encontradas en los sistemas de información.

Los problemas más comunes que han experimentado las empresas por un ciberataque son: pérdida, secuestro y robo de información, lo que también causa daño a la imagen y reputación de la empresa, y genera desconfianza de los clientes.

Según la Encuesta Global Data Protection Index (GDPI), un 55% de las organizaciones globalmente son conscientes que han experimentado ciberataques o incidentes relacionados con la ciberseguridad en los últimos 12 meses, lo que también ha generado pérdidas millonarias a cada organización. (Dell, 2024)

El Informe de Global Cybersecurity Index 2024 califica a los países en temas de ciberseguridad con una calificación máxima de 20 en 5 pilares: Marco Legal, Marco Técnico, Marco Organizacional, Capacidad de desarrollo y Marco de Cooperación. (ITU, 2024a)

Según este informe continentes como Europa y Asia son los que tienen mayor cantidad de países que se encuentran en el nivel de rendimiento T1: Modelo de conducta, el cuál es el nivel más alto de este índice, lo que indica que son países que han decido invertir y desarrollarse en temas de ciberseguridad y están preparados para enfrentar ciberataques.

En América, solamente Brasil y Estados Unidos se encuentran en el nivel de rendimiento T1: Modelo de Conducta, ambos países presentan los mejores índices de ciberseguridad con puntajes altos en cada uno de los 5 pilares evaluados por este índice.

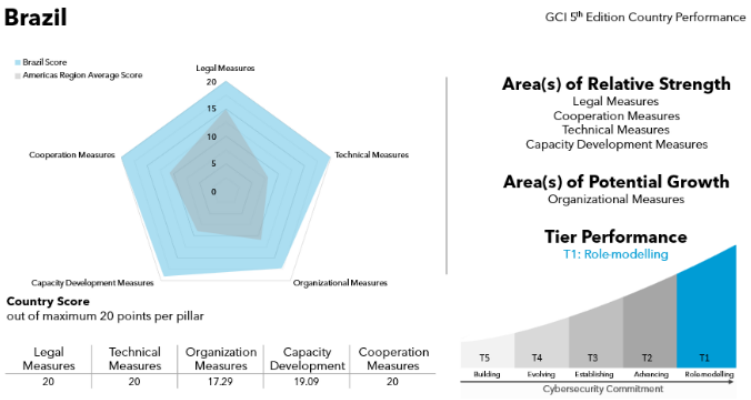


Figura 1. Índice Global de Ciberseguridad en Brasil, 2024.

Fuente: ITU, (2024).

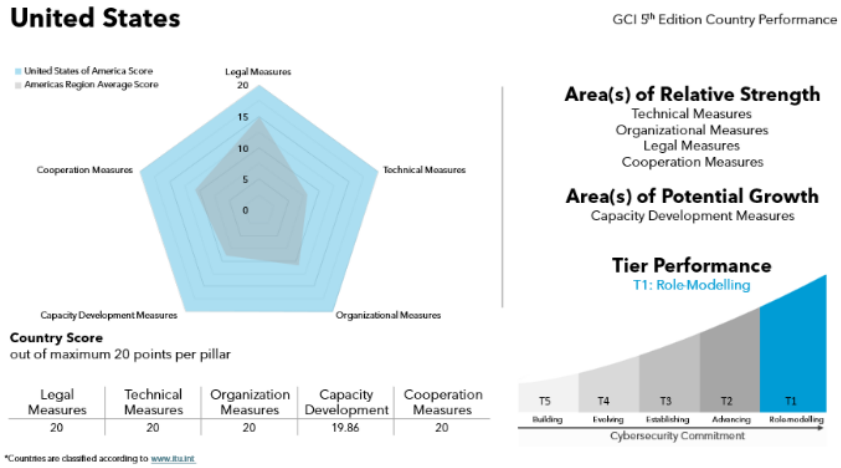


Figura 2 Índice Global de Ciberseguridad en Estados Unidos, 2024.

Fuente: ITU, (2024).

Aproximadamente el 70% de las empresas han estandarizado sus procesos de seguridad, según el "State of DevSecOps 2023 Report" de Synopsys (Synopsis, 2023)

Europa ha sido muy proactiva en la implementación de políticas de ciberseguridad, especialmente debido a regulaciones como el **RGPD (Reglamento General de Protección de Datos)**. Países como **Alemania**, **Reino Unido** y **Francia** tienen marcos de ciberseguridad bien establecidos, aproximadamente el **75%** de las organizaciones europeas adoptan medidas de seguridad integrales. Sin embargo, existen variaciones en el continente, algunos países del este enfrentan desafíos de inversión e infraestructura. (CrowdStrike, 2024; WEforum, 2023)

Asia presenta un panorama ciberseguro diverso. Países como **Japón**, **Corea del Sur** y

Singapur se destacan por su alto nivel de preparación en ciberseguridad, con aproximadamente el **70%** de las organizaciones en estas naciones implementando prácticas de seguridad robustas. Sin embargo, muchas naciones del sudeste asiático y sur de Asia enfrentan desafíos importantes, como una baja inversión en ciberseguridad, lo que las coloca en desventaja frente a los líderes globales. (CrowdStrike, 2024)

Según el informe de Economía de la ciberseguridad para los mercados emergentes, de 2014 a 2023 los ciberincidentes han crecido un promedio del 21%, con un aumento mayor en países de ingresos mediano alto donde la tasa de crecimiento es de 37% y para los países con ingresos bajos la tasa es de un 22%. Algunas de las casusas de estos aumentos han sido la pandemia de Covid-19 y la guerra entre la federación de Rusia y Ucrania. (Vergara Cobos, 2024)

El informe de Economía de la ciberseguridad para los mercados emergentes destaca que América Latina y el Caribe es la región que presenta el aumento más rápido de ciberincidentes divulgados con una tasa promedio de crecimiento anual del 25% de 2014 a 2023. Algunas de las causas son el incremento en un 145% de dispositivos con tecnología de internet de las cosas y a un aumento del 280% del comercio electrónico. (Vergara Cobos, 2024)

En su mayoría la causa de los ciberincidentes es por motivos financieros, a nivel mundial el 74% es por estos motivos, pero existen otros motivos como los que se detallan en la figura 3.

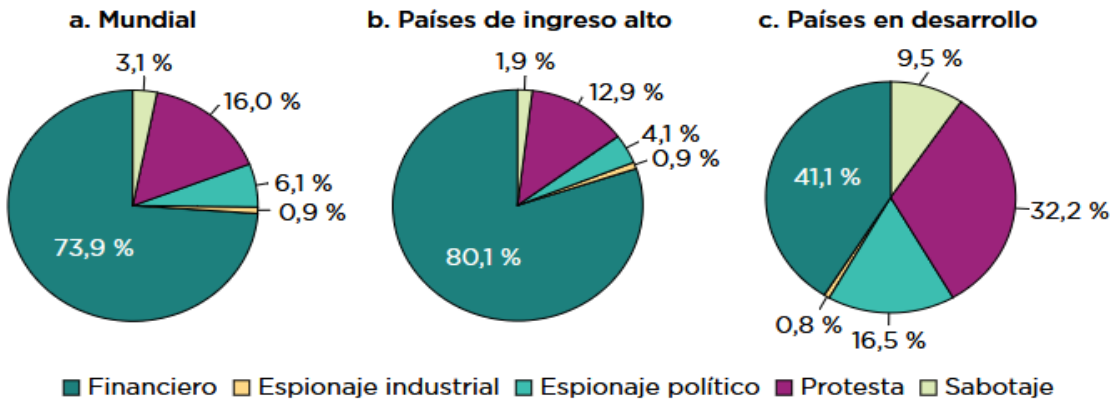


Figura 3. Distribución de los ciberincidentes divulgados

Fuente: (Vergara Cobos, 2024)

De 2021 a 2022 hubo un incremento del 80% en ciberincidentes divulgados, en particular, a países de Asia Central y Europa, como Italia, Polonia y Lituania en sectores públicos y sectores de la información y comunicaciones. (Vergara Cobos, 2024)

La siguiente figura muestra la distribución de los ciberincidentes durante el 2014 al 2023 por sector y por grupos de ingresos, se puede observar que los sectores más afectados han sido el sector de salud y atención social, la administración pública, los servicios educativos, el sector de información y comunicaciones y los servicios profesionales, científicos y técnicos. (Vergara Cobos, 2024)

Según el reporte del estado de la ciberseguridad 2025 de la empresa CheckPoint el sector que ha sido más atacado globalmente en el año 2024 es el sector de la educación con más de 3000 ataques semanales, en segundo luchar se encuentra el sector del gobierno con más de 2000 ataques semanales por lo que coincide con el informe de Economía de la ciberseguridad para los mercados emergentes con que uno de los sectores que son más atacados a nivel mundial es el sector gobierno.

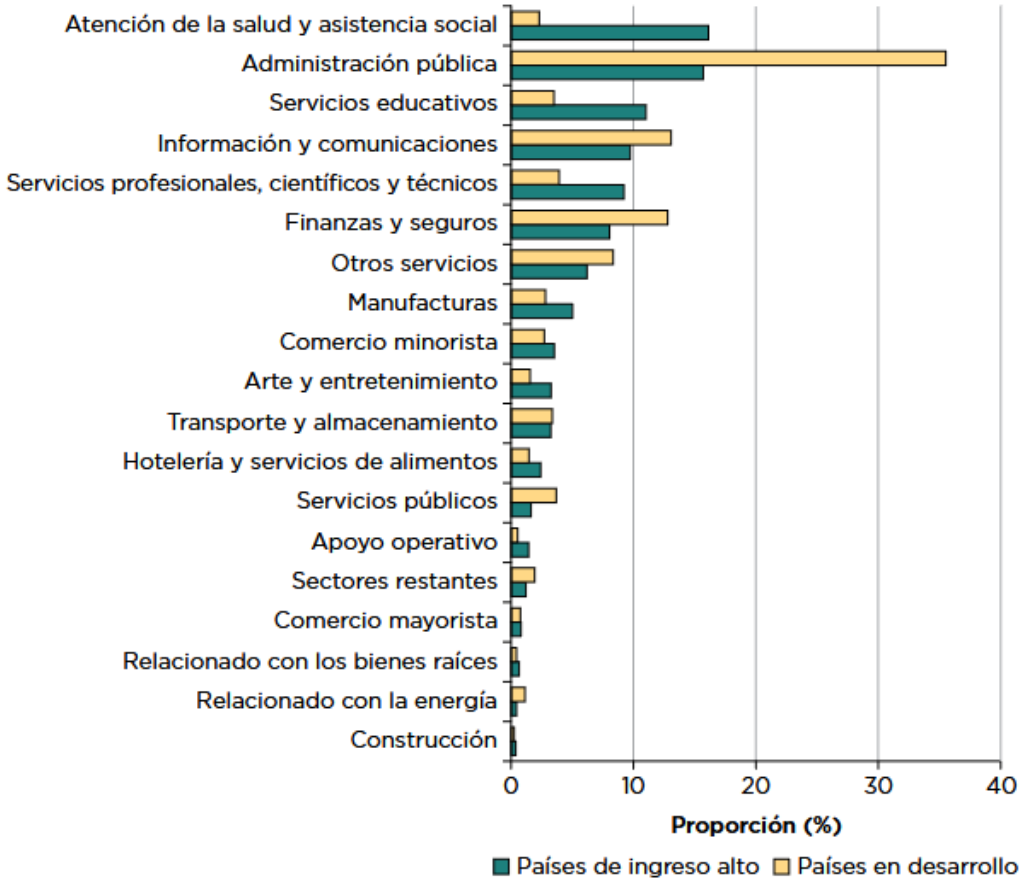


Figura 4. Porcentaje de los ciberincidentes divulgados por sector y grupo de ingresos, 2014-2023

Fuente: Vergara Cobos, (2024)

En este reporte también se menciona el sector del software donde también hay un aumento

del 109% en comparación con los ataques del año anterior con más de 100 ataques semanales. (Checkpoint, 2025)

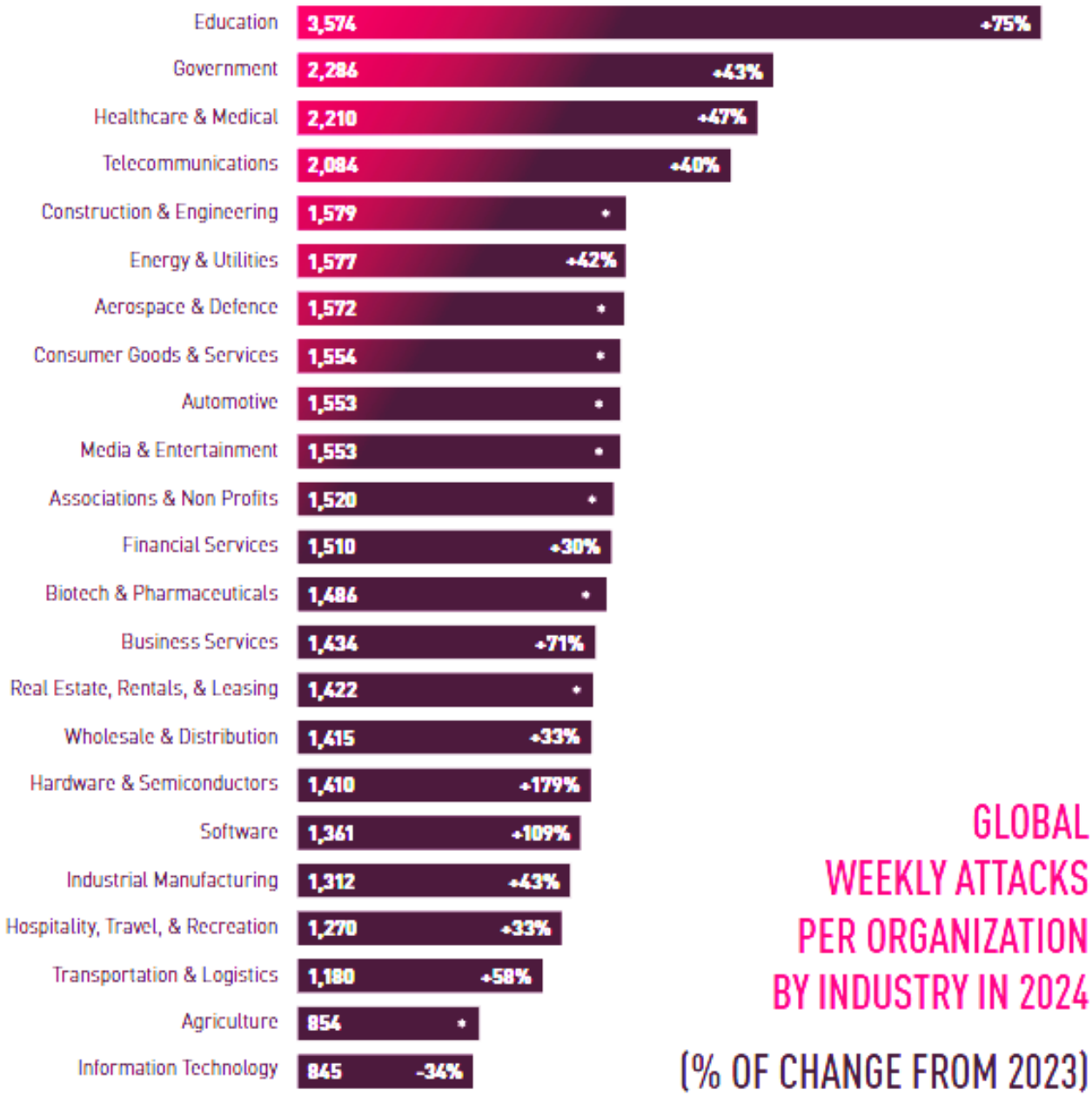


Figura 5 Ataques globales por industria en 2024
Fuente: (Checkpoint, 2025)

Los compromisos que cada país tiene con la ciberseguridad es un punto muy importante ya que reflejan el nivel de protección y son esenciales para poder mitigar el riesgo. Entre 2014 y 2023, los ciberincidentes se triplicaron en los países donde los niveles de compromiso con la

ciberseguridad son bajos y en los países con niveles de compromiso alto se duplicaron. (Vergara Cobos, 2024)

El costo que los ciberincidentes provocan en los países también ha aumentado con el pasar de los años, por ejemplo, el costo promedio de un ataque de ramsomware del año 2022 al 2023 aumento en un 13%. Un ejemplo del costo que un ciberincidente puede ocasionar a las empresas es el caso del ciberataque a NotPetya en 2017 que le generó pérdidas de 7300 millones de dólares para los consumidores. (Vergara Cobos, 2024)

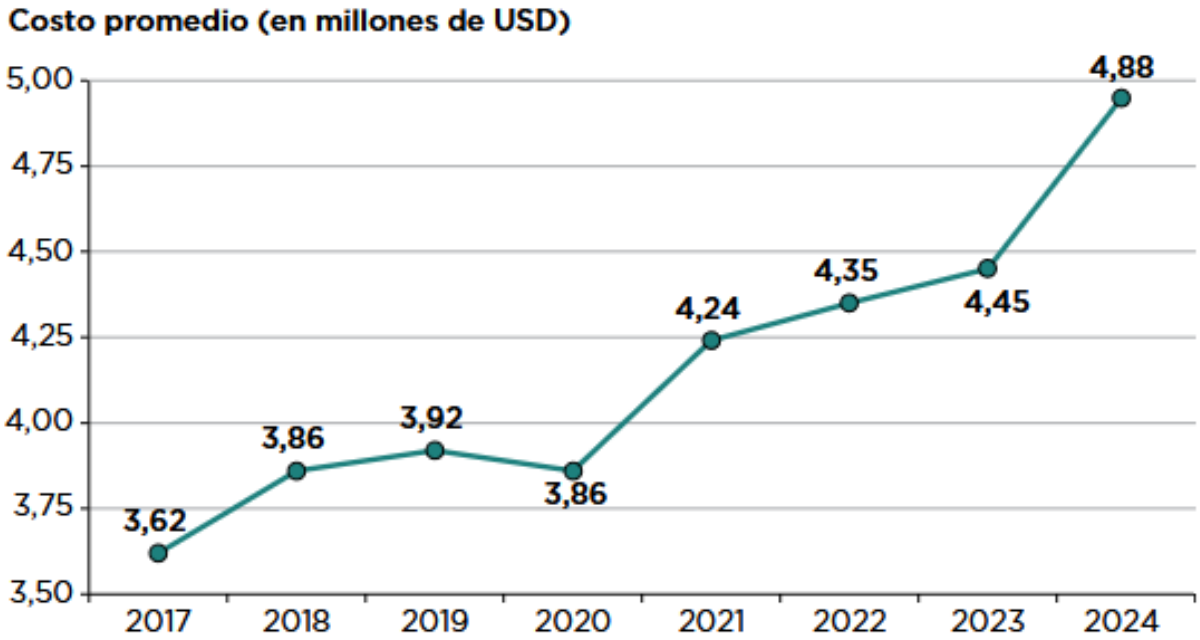


Figura 6. Costo promedio mundial de una filtración de datos, 2017-2024
Fuente: (Vergara Cobos, 2024)

Lockheed Martin Corp., una empresa estadounidense líder en el sector aeroespacial y que trabaja con el Departamento de Defensa y agencias federales, utiliza la plataforma DevSecOps de la empresa GitLab para desarrollar e implementar software de manera más eficiente, segura y rápida para miles de sus programas, obteniendo resultado de 90% menos tiempo dedicado a tareas de mantenimiento del sistema y 80 veces más velocidad en la compilación de pipelines de CI. (Gitlab, 2025)

La empresa Lockheed Martin Corp es una empresa con más de 10000 ingenieros de

software y gracias a utilizar y centralizar sus proyectos en la plataforma de GitLab ha logrado ahorrar cientos de horas al año y las entregas de software que antes eran mensuales se han convertido en entregas semanales, permitiendo a la organización responder a las solicitudes de los clientes con seguridad y rapidez. (Gitlab, 2025)

Solo el 22% de las organizaciones encuestadas por Mezmo y Enterprise Strategy Group (ESG) actualmente cuentan con una estrategia formal de DevSecOps para la integración de la seguridad en el ciclo de vida del desarrollo del software. Las empresas que han adoptado una estrategia DevSecOps perciben claramente sus beneficios en términos de detección de amenazas (95%) y respuesta ante incidentes (96%). (IT Digital Security, 2022)

Organizaciones a nivel mundial han decido adoptar prácticas de DevSecOps para garantizar la seguridad en sus aplicaciones debido a que han recibido ciberataques que les ha ocasionado pérdidas millonarias por ejemplo Target experimentó un ciberataque que les costó millones en reparaciones a sus sistemas y también daños a la reputación, luego de este ciberincidente decidieron implementar DevSecOps para detectar vulnerabilidades desde las fases iniciales del SDLC lo que les ha permitido reducción de costos y evitar ciberincidentes.(OpenWebinars, 2024)

Debido a leyes como GDPR y la Ley de Privacidad del Consumidor de California que han exigido a las organizaciones elevar el nivel de protección de los datos de los usuarios, las empresas han adoptado cada vez más la metodología DevSecOps, ya que les permite integrar la seguridad y de esta manera cumplir con las normativas y leyes. El tamaño del mercado global de DevSecOps se valoró en USD 5.89 mil millones en 2024 y se proyecta que alcance los USD 52.67 mil millones para 2032, con una CAGR del 31,50% durante el período de pronóstico de 2025 a 2032. (Data Bridge Market Research, 2025)

La integración de la capa extra de seguridad que brinda la metodología DevSecOps en comparación con DevOps ha ayudado a las organizaciones a reducir las vulnerabilidades hasta en un 80%, por lo que DevSecOps se convierte en un enfoque esencial para impulsar el crecimiento del mercado porque ayuda a las organizaciones para entregar o desplegar software seguro de manera más rápida y continua. (Data Bridge Market Research, 2025)

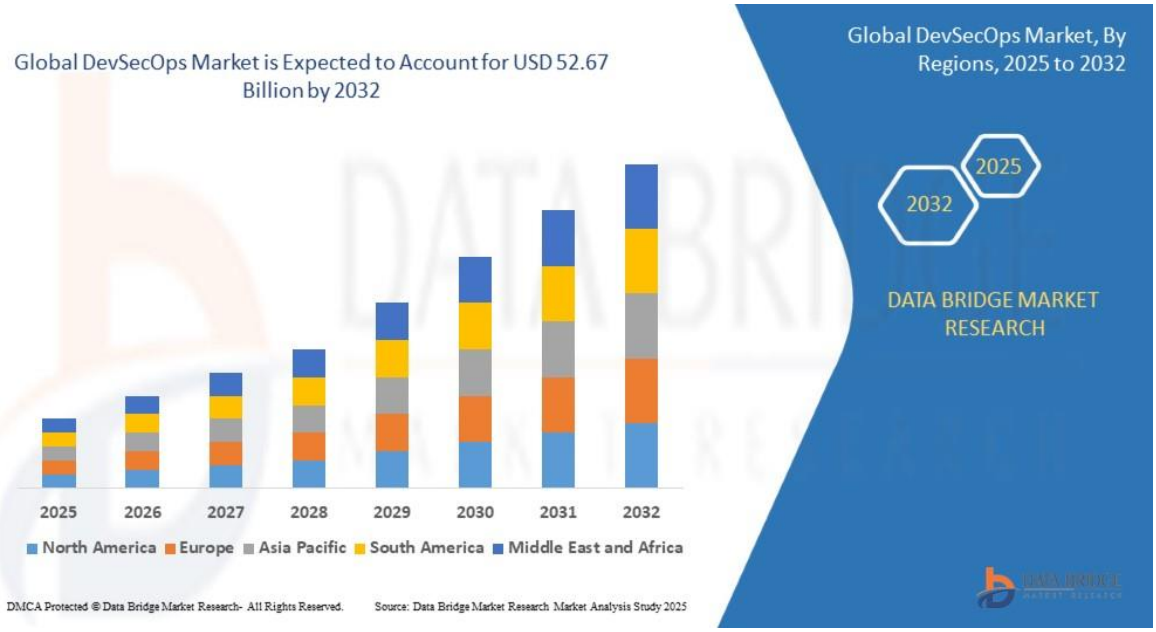


Figura 7. Tamaño del mercado de DevSecOps

Fuente: Data Bridge Market Research, (2025)

El uso de herramientas como GitLab, SonarQube, Snyk y Checkmarx ha permitido a las empresas automatizar la seguridad desde la fase de desarrollo. En países como Estados Unidos y el Reino Unido, más del 70% de las organizaciones han implementado herramientas de escaneo de código y análisis de seguridad en sus pipelines de integración continua (Fortinet, 2023).

En China y Japón, la adopción de DevSecOps ha estado impulsada por el avance de la industria tecnológica y la necesidad de proteger infraestructuras críticas contra ataques cibernéticos. Empresas como Alibaba Cloud y Fujitsu han desarrollado plataformas especializadas para reforzar la seguridad en aplicaciones web y móviles (Kaspersky, 2023).

En Estados Unidos, la seguridad del software está regulada por el NIST Cybersecurity Framework, que establece estándares y mejores prácticas para proteger infraestructuras digitales. Empresas del sector financiero, salud y tecnología han integrado DevSecOps para cumplir con regulaciones como la Ley de Protección de la Información del Consumidor de California (CCPA) y el Reglamento General de Protección de Datos (GDPR) en Europa (IMARC Group, 2023).

La Unión Europea ha establecido normativas estrictas en seguridad de datos, siendo el GDPR una de las regulaciones más influyentes a nivel mundial. Empresas en Alemania, Francia y España han adoptado DevSecOps como una estrategia clave para garantizar el cumplimiento de

estas leyes y evitar sanciones económicas por el mal manejo de datos personales (ESET, 2023).

En China, el gobierno ha implementado regulaciones como la Ley de Seguridad Cibernética, que exige a las empresas proteger la integridad de los datos mediante herramientas avanzadas de seguridad. En Japón y Corea del Sur, la integración de DevSecOps ha sido promovida por empresas tecnológicas líderes como Samsung, Sony y Hitachi, que buscan fortalecer la protección de sus infraestructuras digitales frente a amenazas cibernéticas (ManageEngine, 2024)

Los ataques cibernéticos han aumentado en frecuencia y sofisticación en los últimos años. Según un informe de IBM (2023), el costo promedio de una violación de datos en empresas que no utilizan DevSecOps asciende a USD 4,35 millones. La creciente amenaza del ransomware, phishing y ataques a infraestructuras críticas ha motivado a organizaciones de todo el mundo a adoptar estrategias de seguridad desde la fase inicial del desarrollo de software.

Uno de los principales desafíos en la implementación de DevSecOps es la falta de profesionales capacitados. Según Cybersecurity Ventures (2023), hay una escasez global de más de 3,5 millones de expertos en ciberseguridad, lo que dificulta la adopción masiva de DevSecOps en empresas que carecen de recursos para contratar talento especializado.

Las empresas líderes en tecnología han invertido en soluciones avanzadas de seguridad. En Estados Unidos y Europa, compañías como Microsoft, IBM y Google han desarrollado herramientas de análisis de código estático y dinámico, fortaleciendo la detección temprana de vulnerabilidades (Gartner, 2024)

En Asia y Medio Oriente, gobiernos y organizaciones han impulsado iniciativas de transformación digital para reforzar la seguridad en infraestructuras críticas, como el sector financiero y de telecomunicaciones.

La adopción de DevSecOps a nivel mundial ha sido impulsada por la creciente necesidad de proteger aplicaciones contra ataques cibernéticos. Aunque países como Estados Unidos, Reino Unido, Alemania, Japón y China han avanzado significativamente en su implementación, aún existen desafíos como la escasez de talento y la falta de estandarización en ciertas regiones.

El futuro de DevSecOps dependerá de la capacidad de las organizaciones para adaptarse a un entorno digital en constante evolución, donde la seguridad se convierte en un pilar fundamental del desarrollo tecnológico.

2.2 MICROENTORNO

En América Latina, existe un creciente aumento de ciberataques lo cual se convierte en una preocupación creciente para organizaciones de diferentes rubros incluyendo los gobiernos, esto se debe a la transformación digital que ha impulsado tanto la innovación, pero también la exposición a nuevas amenazas por vulnerabilidades que se pueden presentar en los sistemas de información. En Latinoamérica la metodología DevSecOps ha emergido para utilizarse como una estrategia clave para fortalecer la ciberseguridad**,** ya que permite la implementación de prácticas de seguridad desde las fases iniciales del desarrollo de software. (Ramirez, 2025)

En los últimos 10 años, el número de ciberdelincuentes en México y Latinoamérica ha aumentado en un 25% promedio anual, convirtiendo a la región en un blanco atractivo para ataques cibernéticos. Además, diversos factores como la baja inversión en ciberseguridad y el crecimiento acelerado del uso de dispositivos IoT sin medidas de protección adecuadas han contribuido al aumento de ciberincidentes. Según el jefe de investigación de ESET Latinoamérica, estos factores facilitan la actividad de los ciberdelincuentes, exponiendo a las organizaciones a ataques como ransomware, phishing y robo de datos. (Ramirez, 2025)

El desarrollo seguro de software ha tomado un papel fundamental en el contexto actual, donde las amenazas cibernéticas han aumentado significativamente. DevSecOps es una metodología que busca integrar la seguridad en cada fase del ciclo de vida del desarrollo de software, promoviendo la automatización y la detección temprana de vulnerabilidades. En América Latina, su adopción ha sido gradual, pero cada vez más empresas e instituciones reconocen la importancia de esta práctica para fortalecer la ciberseguridad (Microsoft, 2024)

La implementación de DevSecOps en América Latina está en una etapa emergente, con un crecimiento acelerado en los últimos años. Según un estudio de DevSecOps Latinoamérica (2023), más del 60% de las empresas en la región han comenzado a integrar seguridad en sus procesos de desarrollo de software, aunque solo un 30% cuenta con una estrategia completamente definida.

En el caso de Honduras, la adopción de DevSecOps es aún incipiente. Empresas del sector financiero y telecomunicaciones han liderado la implementación de esta metodología, impulsadas por la necesidad de proteger datos sensibles y cumplir con normativas de ciberseguridad (Fluid Attacks, 2022). No obstante, el país enfrenta desafíos como la falta de talento especializado y la escasa inversión en seguridad digital.

Algunos países han avanzado más en esta área. Por ejemplo, en Brasil y México, compañías como Nubank y Kio Networks han incorporado DevSecOps en sus procesos para mejorar la protección de datos y la respuesta ante incidentes de seguridad (ESET, 2023). Mientras tanto, en Argentina y Colombia, sectores como el comercio electrónico y la banca han experimentado un crecimiento significativo en el uso de herramientas automatizadas de seguridad (ManageEngine, 2024)

En muchos países, la regulación en materia de seguridad informática ha impulsado la adopción de DevSecOps. En Honduras, la Ley de Protección de Datos Personales y otras normativas han obligado a empresas a reforzar sus estrategias de ciberseguridad (BID, 2020). A nivel regional, Brasil lidera con la Ley General de Protección de Datos (LGPD), que ha motivado a organizaciones a integrar seguridad en sus procesos de desarrollo.

Un desafío importante para la adopción de DevSecOps es la falta de profesionales con conocimientos en seguridad y automatización. Según un informe de Fortinet (2022), el 45% de las empresas en América Latina enfrenta dificultades para encontrar expertos en ciberseguridad, lo que ralentiza la implementación de estrategias de seguridad en el desarrollo de software.

La implementación de DevSecOps requiere herramientas especializadas como análisis estático de código (SAST), análisis dinámico (DAST) y escaneo de contenedores. Sin embargo, muchas empresas en la región no cuentan con los recursos suficientes para invertir en estas soluciones (Mordor Intelligence, 2023). A pesar de esto, empresas en países como Chile y Perú han empezado a integrar plataformas como GitLab y SonarQube para mejorar la seguridad en sus procesos de desarrollo.

Las empresas que han adoptado DevSecOps han reportado múltiples beneficios, entre los que destacan:

- **Reducción de vulnerabilidades:** Implementar seguridad desde las primeras etapas del desarrollo disminuye significativamente los riesgos de ataques.
- **Automatización y eficiencia:** Herramientas de DevSecOps permiten detectar y corregir problemas de seguridad en tiempo real, evitando retrasos en los proyectos (Bambú Mobile, 2022).
- **Cumplimiento normativo:** Empresas en sectores altamente regulados han encontrado en

DevSecOps una solución efectiva para cumplir con estándares internacionales como ISO 27001 y NIST

- **Mayor confianza del cliente:** La seguridad de los datos se ha convertido en un factor clave para la reputación de las empresas, especialmente en sectores como la banca y el comercio electrónico (ManageEngine, 2024)

El avance de DevSecOps en América Latina y Honduras es un reflejo del crecimiento de la ciberseguridad en la región. Si bien su adopción ha sido más acelerada en países como Brasil, México y Argentina, en otras naciones aún existen desafíos como la falta de talento especializado y la baja inversión en tecnología.

La transformación digital en América Latina requiere estrategias de seguridad robustas, y DevSecOps se presenta como una solución clave para garantizar el desarrollo seguro de software. Con una adopción adecuada, las empresas en Honduras y otros países podrán mejorar su resiliencia ante ciberataques y fortalecer su competitividad en el mercado global.

Países de Centroamérica como Guatemala muestran un índice global de ciberseguridad de 39.99, el cuál lo ubica arriba de Honduras, pero aun así se encuentran en el mismo nivel de rendimiento T4: Evolución, lo que indica que está en plena evolución y todavía le falta para poder aumentar el índice de ciberseguridad.

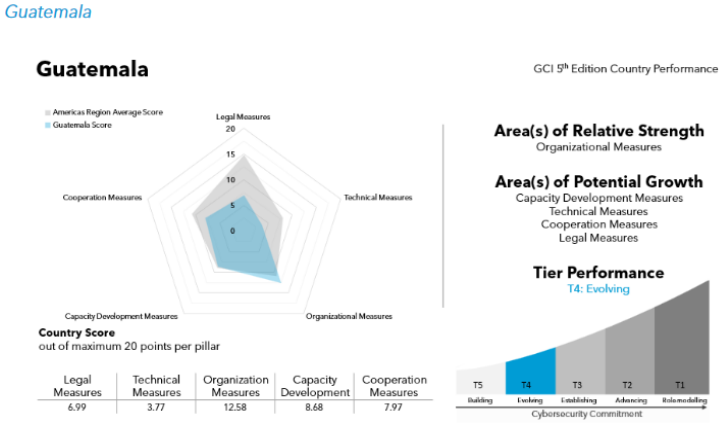


Figura 8. Índice Global de Ciberseguridad en Guatemala, 2024.
Fuente: ITU, (2024).

Costa Rica presenta un mejor índice y se sitúa en el nivel de rendimiento T3 Establecer y presenta puntajes en su mayoría arriba de 10 en cada uno de los 5 pilares del Índice Global de Seguridad.

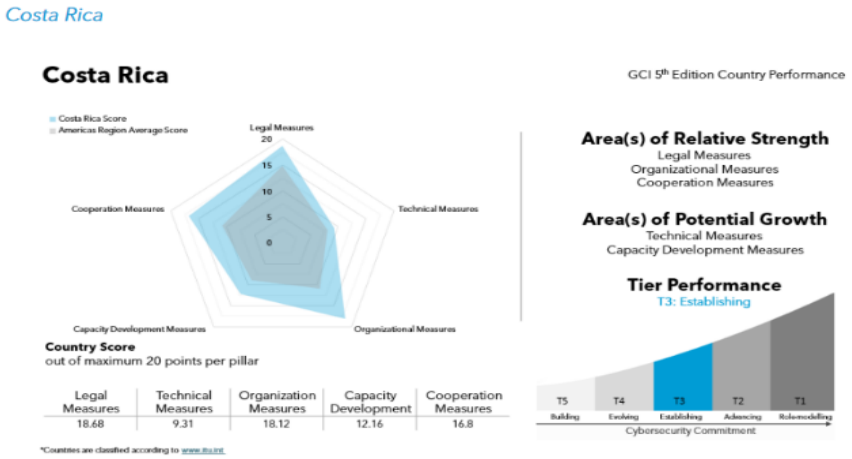


Figura 9. Índice Global de Ciberseguridad en Costa Rica, 2024.
Fuente: ITU, (2024)

Costa Rica ha avanzado en ciberseguridad, estableciendo marcos legales como la Ley N° 9048 de protección de datos personales y la Política Nacional de Ciberseguridad. El país ha creado instituciones como el CSIRT-CR para gestionar incidentes cibernéticos y ha impulsado la cooperación público-privada. Sin embargo, enfrenta desafíos como ataques de ransomware, brechas de seguridad en el sector público y privado, y desigualdades en la implementación de medidas de seguridad, especialmente entre las pequeñas y medianas empresas. A pesar de estos retos, Costa Rica sigue alineada con iniciativas regionales e internacionales para fortalecer la ciberseguridad. (GoLegal, 2024; MICITT, 2024)

En 2022, los organismos de estado en Costa Rica fueron atacados por el grupo de ramsomware Conti, lo que provocó que varios servicios y sistemas claves estuvieran inactivaos representando un costo económico estimado del 2.4% del PBI, según estimaciones del Banco Mundial. (Bocconi, 2025)

En Honduras, han aumentado los casos de ciberataques provocando pérdidas económicas en las organizaciones, uno de los ataques más comunes es el ramsomware ya sea de tipo cifrado o de bloqueo, este podría infectar a las computadoras transmitiéndose por un software inseguro o que no tenga las actualizaciones correspondientes. (Juan Carlos Rivera, 2023)

En el plan nacional de Gobierno Digital 2023-2026 se plantea como un objetivo en materia

de Seguridad en las comunicaciones: Desarrollar estrategias para mejorar la ciberseguridad nacional y la protección de los activos de la información, así como la coordinación institucional para la prevención y respuesta ante incidentes cibernéticos. (Gobierno de Honduras, 2023)

En Honduras, existen artículos en el Código Penal para la seguridad de las redes y de los sistemas Informáticos que castigan acciones como: Accesos no autorizados a sistemas informáticos, Daños a datos y sistemas informáticos y Ciberterrorismo o terrorismo electrónico. (Poder Legislativo Honduras, 2019)

Según el Índice Global de Ciberseguridad, en el año 2020 Honduras se ubicó en la posición 178 de 182 países con un índice de ciberseguridad global de sólo 2.2 de 100% y en el año 2024 obtuvo un puntaje global de 28.07 sobre 100. (ITU, 2020, 2024a)

En el informe presentado en el año 2024 del Índice Global de Ciberseguridad se menciona que Honduras se encuentra en plena etapa evolutiva para adoptar la ciberseguridad. De los cinco pilares que evalúa este índice donde obtuvo mayor puntaje es en el de Medidas Legales y donde obtuvo un puntaje de 0 es en medidas técnicas. (ITU, 2024a)

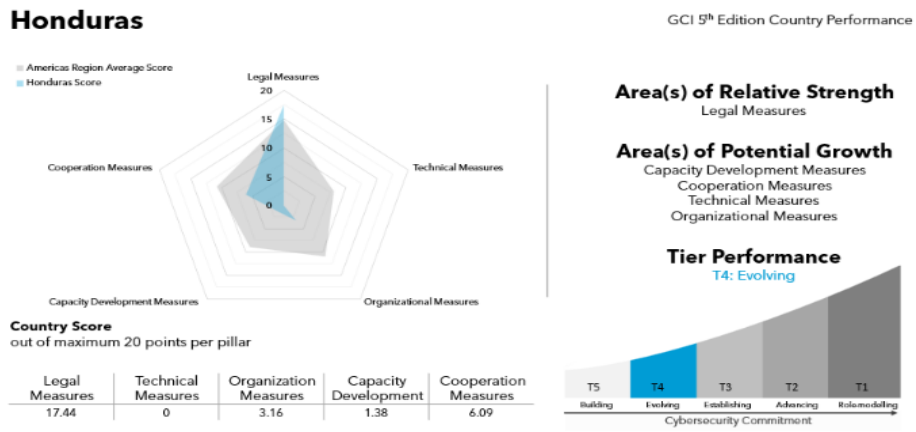


Figura 10. Índice Global de Ciberseguridad en Honduras, 2024.

Fuente: ITU, (2024).

A nivel regional, los servicios de ciberseguridad gerenciados han presentado un crecimiento importante dentro del mercado. En el reporte de Frost & Sullivan, se indica que en Honduras los servicios de ciberseguridad presentan para el año 2024 un crecimiento del 16% con relación al año pasado, con ingresos de USD 10.4 millones. (La Tribuna, 2024)

Honduras es el segundo país con más ciberataques en Centroamérica, siendo el Ransomware, Phishing y Swaping los principales tipos de ataques que ocurren en el país. Estos ataques se registran en su gran mayoría en industrias y sectores específicos como el de gobierno, banca, educación, manufactura y energía. (La Tribuna, 2024)

En cuanto a temas de educación sobre ciberseguridad en Honduras, algunas instituciones educativas como UNITEC están iniciando a incorporar en sus ofertas académicas programas educativos relacionados con la ciberseguridad, en este caso UNITEC ofrece una Maestría en Ciberseguridad.

En Honduras, el cibercrimen ha aumentado significativamente en los últimos años, por lo que es fundamental tomar medidas para prevenir ataques informáticos, por ello, un Pentesting continuo en Honduras es una de las estrategias más efectivas en la seguridad informática, que permite la evaluación de seguridad simulando ataques informáticos para detectar vulnerabilidades y errores en los sistemas y aplicaciones. (Dragon Jar, 2003)

Además, hay empresas que están ofreciendo cursos sobre DevSecOps para que las organizaciones o personas particulares puedan capacitarse y conocer sobre la seguridad y DevSecOps como DevSecOps Foundation (DSOF) Training in Honduras que ofrece cursos detallados para aprender cómo implementar las prácticas de seguridad para obtener beneficios comerciales. (Spoclearn, 2025)

En países de América Latina como Honduras, la implementación y adopción de la metodología DevSecOps es fundamental debido a factores como aumento de ciberataques, falta de regulaciones estrictas y un proceso de digitalización acelerada, pero estos países enfrentan diversos desafíos que limitan la adopción de DevSecOps, desafíos como una cultura organizacional tradicional , la falta de regulaciones estrictas en temas de ciberseguridad, falta de talento especializado, poca o nula inversión en herramientas especializadas para la automatización de seguridad y capacitación del personal, cuenta con muchos sistemas heredados la cual no es compatible con DevSecOps y además hay una percepción errónea sobre la complejidad en la implementación de DevSecOps.(Ramirez, 2025)

En la región latinoamericana, países como México, Brasil, Argentina y Chile han mostrado avances en la implementación de DevSecOps, principalmente en el sector financiero y gubernamental. Sin embargo, en naciones como Honduras, Guatemala y El Salvador, el desarrollo

de estas prácticas aún enfrenta desafíos relacionados con la infraestructura tecnológica, la inversión en ciberseguridad y la formación de talento especializado.

2.3 TEORÍAS DE SUSTENTO

2.3.1 GESTIÓN DEL DESARROLLO DE SOFTWARE

El objetivo principal de la gestión de desarrollo de software es asegurarse que las aplicaciones y sistemas desarrolladas sean de acuerdo con las necesidades presentadas por las partes interesadas donde se evalúan aspectos de funcionalidad, confiabilidad, que sea mantenible con el tiempo, cumplimiento y auditabilidad. (AXELOS, 2019)

Una de las actividades que incluye el desarrollo de software es:

- Pruebas de software: donde se deben realizar diferentes tipos de pruebas como: pruebas de componentes, pruebas unitarias, pruebas de integración, pruebas de regresión, pruebas de aceptación del Usuario y pruebas de seguridad que son las que nos ayudan a encontrar vulnerabilidades y de esta manera poder corregirlas o mitigarles.

El ciclo de vida del desarrollo de software incluye las actividades desde que se genera la idea, hasta la puesta en operación el software, incluyendo las fases de desarrollo, pruebas e implementación.

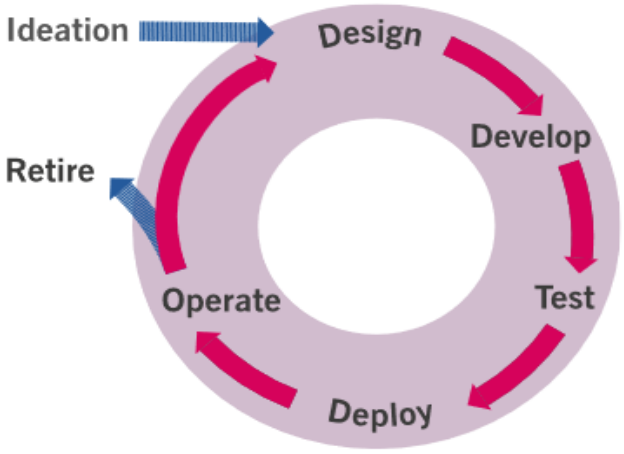


Figura 11. Ciclo de vida del desarrollo de software.

Fuente: AXELOS, (2019)

La gestión de desarrollo de software contribuye a la cadena de valor de ITII, principalmente,

en la actividad de obtener y construir, pero también influye en actividades como diseño y transición, mejora, planificación y entrega y soporte.

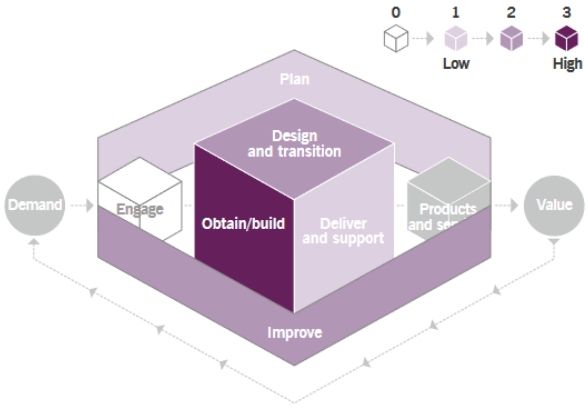


Figura 12.Contribución de la Gestión de Desarrollo de Software a las actividades de la Cadena de Valor ITIL.

Fuente: AXELOS, (2019)

Es importante comprender la Gestión de Desarrollo de Software, ya que al desarrollar nuevo software o actualizar software existente no sólo se trata de desarrollo sino también se ve involucrado el tema de calidad, entregarlo a tiempo, que sea un software que puede ser mantenible y escalable con el tiempo, además de que debe ser un software seguro que resguarde la información y no permita que este visible a cualquier usuario y que cumpla con las necesidades de las partes interesadas. (AXELOS, 2019b)

2.3.2 GESTIÓN DE RIESGOS

Riesgo es un evento que puede ocurrir y causar daño o pérdidas, o que puede generar obstáculos para que una organización no logre los objetivos. También, se define como un desconocimiento del resultado y se puede utilizar para medir la probabilidad de obtener resultados positivos y negativos. (AXELOS, 2019)

El objetivo de la gestión de riesgos es asegurarse que la organización entienda y pueda manejar efectivamente los riesgos. Esta gestión es fundamental para garantizar la sostenibilidad de una organización y generar valor a sus clientes. (AXELOS, 2019)

La gestión de riesgos tiene una contribución alta en la mayoría de las actividades de la cadena de valor, porque es importante identificar los riesgos para poder controlarlos o mitigarlos adecuadamente en el tiempo oportuno y evitar que causen daños graves en la organización.

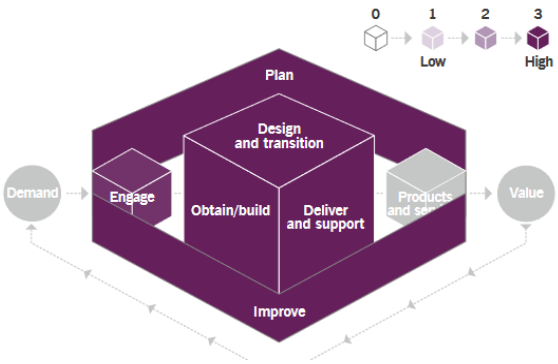


Figura 13. Contribución de la Gestión de Riesgos a las actividades de la Cadena de Valor ITIL.
Fuente: AXELOS, (2019)

La implementación de DevSecOps en el SDLC les permitirá a las organizaciones gestionar los riesgos que se pueden presentar al desarrollar software porque podrán identificar amenazas y vulnerabilidades desde que se inicie el desarrollo hasta la implementación evitando que sufran ciberataques o mitigando los riesgos que se pueden presentar cuando el aplicativo desarrollado este puesto en producción y utilizado por los usuarios finales.

2.3.3 GESTIÓN DE INCIDENTES

Un incidente se puede definir como una interrupción no planificada de un servicio o una reducción en la Calidad de un servicio. El objetivo principal de la gestión de incidentes es intentar minimizar el impacto negativo de los incidentes a través de una oportuna restauración del funcionamiento normal de un servicio en el menor tiempo posible. (AXELOS, 2019)

La gestión de incidentes permite a las empresas estar preparadas en caso de ocurrir una interrupción de su servicio, esta teoría se relaciona con la implementación de DevSecOps al SDLC porque es importante que el software creado sea capaz de evitar una interrupción de un servicio como por ejemplo al reducir la posibilidad de sufrir un ciberataque que puede provocar que una aplicación sea inaccesible para los usuarios e incluso cambiar archivos.

La gestión de incidentes contribuye altamente en actividades como entrega y soporte y atraer, pero también tiene una contribución más baja en actividades como diseño y transición, obtener y construir y mejora.

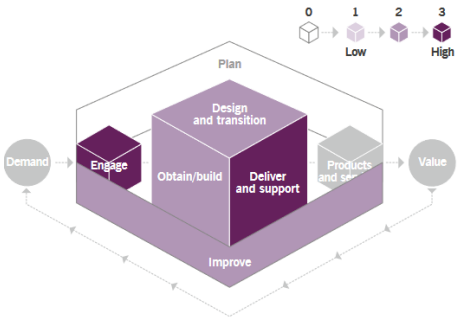


Figura 14. Contribución de la Gestión de Incidentes a las actividades de la Cadena de Valor ITIL.

Fuente: AXELOS, (2019)

2.3.4 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El propósito de la Gestión de Seguridad de Información es proteger la información necesaria para que la organización pueda llevar a cabo su negocio. Esto implica comprender y gestionar los riesgos para mantener la confidencialidad, integridad y disponibilidad de la información y otros aspectos relacionados con la seguridad de la información como la autenticación y el no repudio. (AXELOS, 2019).

La gestión de la seguridad de la información contribuye altamente en casi todas las actividades de la cadena de valor, solamente en la actividad de productos y servicios no contribuye, esto se debe a que en todas las actividades podemos generar información y es importante mantenerla segura.

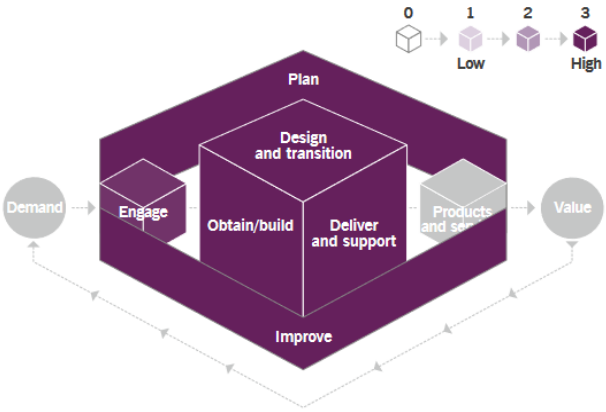


Figura 15. Contribución de la Gestión de la Seguridad de la información a las actividades de la Cadena de Valor ITIL.

Fuente: AXELOS, (2019)

El software en las empresas contiene información confidencial y secreta que no debe ser pública ni estar accesible para personas no autorizadas, por lo que se hace indispensable que las

organizaciones implementen seguridad en el SDLC para garantizar la Seguridad de la Información que contendrán cada software creado y puesto en producción.

2.3.5 CIBERSEGURIDAD

La ciberseguridad se ocupa de la protección de los activos digitales en los que se incluye las redes, el software y el hardware, además de la información que es procesada, almacenada o transportada en sistemas de información que se encentran interconectados. Se conoce como ciberseguridad al conjunto de técnicas, sistemas de gestión y otras medidas que pretenden proteger de incidentes deliberados o accidentales la información y los medios digitales que la tratan. (MANUEL, 2021)

La ciberseguridad se enfoca en tres principios fundamentales que forman la triada CID:

- **Confidencialidad**: La información debe ser accesible solamente para los usuarios autorizados.
- **Integridad**: La información debe mantenerse exacta no debe de sufrir cambios ni alteraciones.
- **Disponibilidad**: Los sistemas y la información deben estar siempre disponibles para las personas autorizadas.

Figura 16. Triada CID Ciberseguridad.

Fuente: García, (2024)

Las prácticas de DevSecOps que se implementan en el SDLC deben incluir los tres principios de la ciberseguridad porque debemos mantener la información siempre de manera confidencial que solo tenga acceso las personas autorizadas y delimitar el acceso por roles de

usuario, la información que se encuentra en los diferentes softwares desarrollados en las organizaciones debe mantenerse integra sin importar todas las transacciones o acciones que se realicen y también debe estar disponible siempre que se necesite.

2.4 METODOLOGÍAS TEMÁTICAS

2.4.1 DEVOPS

DevOps", es una combinación de los términos anglosajones “Development” y “Operations”, usada por primera vez por Yhens Wasna y Patrick Debois en su charla sobre "Infraestructura Ágil", en la Conferencia Agile 2008 en Toronto. El principal objetivo de DevOps es minimizar el tiempo de desarrollo de las aplicaciones y acelerar la liberación de nuevas funciones requeridas por los clientes. Esto a través de una comunicación constante y continúa entre los equipos de trabajo de desarrollo de aplicaciones (Dev) y de operaciones tecnológicas (Ops).(Redondo et al., 2022b)

Para Gartner, “DevOps representa un cambio en la cultura de Tecnologías de la Información (TI), que se centra en la entrega rápida de servicios de TI mediante la adopción de prácticas ágiles y ajustadas en el contexto de un enfoque orientado al sistema. DevOps hace hincapié en las personas (y la cultura) y busca mejorar la colaboración entre los equipos de operaciones y desarrollo. Las implementaciones de DevOps utilizan tecnología, especialmente herramientas de automatización que pueden aprovechar una infraestructura cada vez más programable y dinámica desde la perspectiva del ciclo de vida”. (Redondo & Cárdenas, 2022)

Figura 17. Ciclo de vida de DevOps

Fuente: (Redondo et al., 2022a)

DevOps, es una metodología que busca mejorar la eficiencia en cada etapa del ciclo de vida del desarrollo de software, por lo que es muy importante conocerla para poder implementar DevSecOps en el SDLC y de esta metodología deriva otra que es más enfocada en el tema de seguridad la cual es DevSecOps.

2.4.2 DEVSECOPS

Al igual que DevOps, DevSecOps es una metodología técnica y organizativa que combina flujos de trabajo de gestión de proyectos con herramientas de TI automatizadas. DevSecOps integra auditorías de seguridad activas y pruebas de seguridad en flujos de trabajo de DevOps y de desarrollo ágiles, a fin de integrar la seguridad en el producto, en lugar de aplicarla a un producto terminado. (Villamarín et al., 2023)

En cada una de las etapas del SDLC se debe de tener en cuenta la seguridad antes de pasar a la siguiente etapa. En lugar de aplicar la seguridad al producto final, tiene como objetivo tener la seguridad integrada en el producto aplicando el concepto de seguridad por diseño, lo que significa que la seguridad se toma en consideración desde el principio y durante todo el ciclo de vida del software que estemos desarrollando. (Villamarín et al., 2023)

Con DevSecOps, la seguridad debe aplicarse en cada etapa de la canalización típica de DevOps:

Planificación: En esta etapa se definen los requerimientos del cliente y el alcance del software a desarrollar. Entre las medidas de seguridad que se pueden implementar está un análisis de las posibles amenazas y vulnerabilidades y alinear los objetivos del software con las necesidades de seguridad de la organización desde el comienzo del proyecto.

Codificación y Construcción: Estas fases es donde el equipo de desarrollo realizar la escritura del código para el software a entregar, se implementan las funcionalidades solicitadas en cada aplicativo. En esta fase se pueden aplicar medidas de seguridad como revisión de código mediante herramientas que ayuden a identificar vulnerabilidad y errores en el código fuente, aplicar un sistema de control de accesos a la aplicación que limite a los usuarios a ver solo los módulos que necesiten y realizar pruebas de seguridad en el código durante el proceso de desarrollo para detectar problemas cono vulnerabilidades en librerías externas o inyecciones SQL.

Pruebas: Esta etapa es cuando el software es probado exhaustivamente para garantizar que cumple con los requisitos de funcionalidad, rendimiento y seguridad. Las medidas de seguridad que se pueden implementar son: pruebas de seguridad automáticas, evaluación de la configuración de seguridad y simulación de ataques.

Lanzamiento y Despliegue: En estas fases es cuando el software es preparado y puesto en el entorno de producción. Algunas medidas de seguridad que se pueden implementar son: revisión

de seguridad del entorno de producción, realizar un despliegue automatizado y seguro y asegurarse que este implementado correctamente un control de accesos y autenticación.

Operación y Monitoreo: Estas fases es cuando el software ya está en producción y se debe realizar un monitoreo para garantizar su rendimiento, confiabilidad y seguridad. Algunas medidas de seguridad que se pueden implementar son: Monitoreo continuo de seguridad, monitoreo de logs, gestión de parches y actualizaciones, configuración adecuada de alertas y respuestas a incidentes y una evaluación continua de seguridad. (owasp, 2024; SANS Institute, 2024)

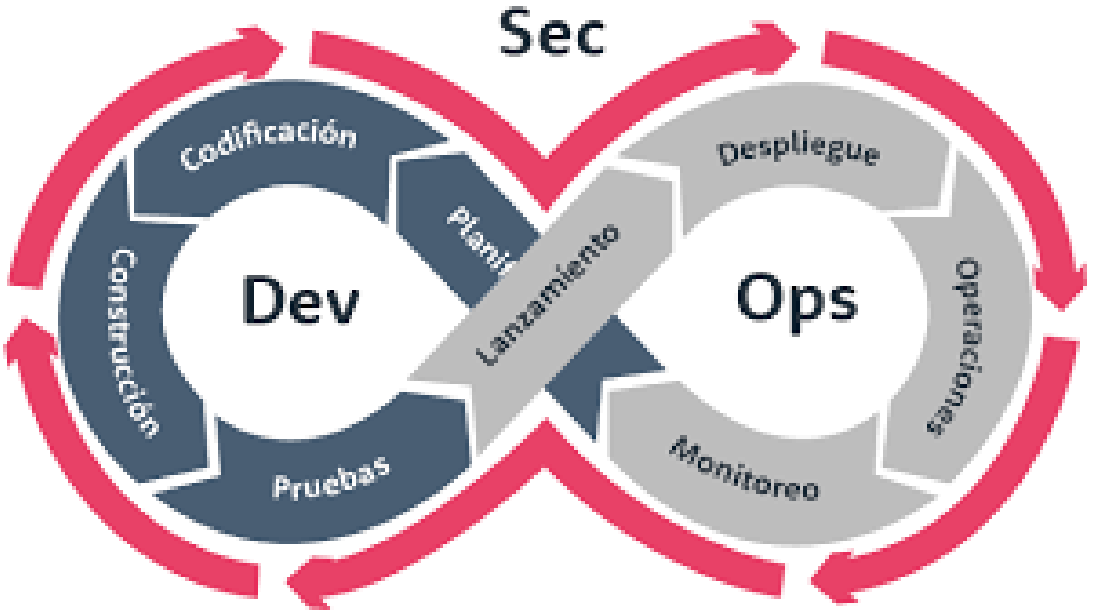


Figura 18. Ciclo de vida de DevSecOps
Fuente: Villamarín & Sánchez-Montañés, (2023)

2.4.3 ITIL V4

ITIL, son las siglas de Information Technology Infraestructura Library, esto se trata de la gestión de servicios de la tecnología de la información y la gestión de servicios de una organización que ofrece diferentes tipos de resultados. (Remache Típan, 2022)

ITIL 4 es una revisión al marco de trabajo más ampliamente aceptado a nivel mundial para la Administración de Servicios de TI (ITSM). Se compone de una guía comprensiva de como adoptar y adaptar las mejores prácticas de gestión. ITIL 4, está diseñado para garantizar un sistema flexible, coordinado e integrado para el gobierno y la gestión efectiva de los servicios habilitados para TI. (AXELOS, 2019b).

ITIL 4 proporciona un modelo operativo digital de extremo a extremo en la organización para la entrega y operación de productos y servicios habilitados por TI y permite que los equipos de TI continúen desempeñando un papel importante en la estrategia comercial del negocio.

ITIL 4 también proporciona un enfoque integral de extremo a extremo que integra marcos como Lean, Agile y DevOps. El objetivo de SVS (Sistema de valor de servicio) es asegurar que las organizaciones creen valor a través de uso y administración de productos y servicios.

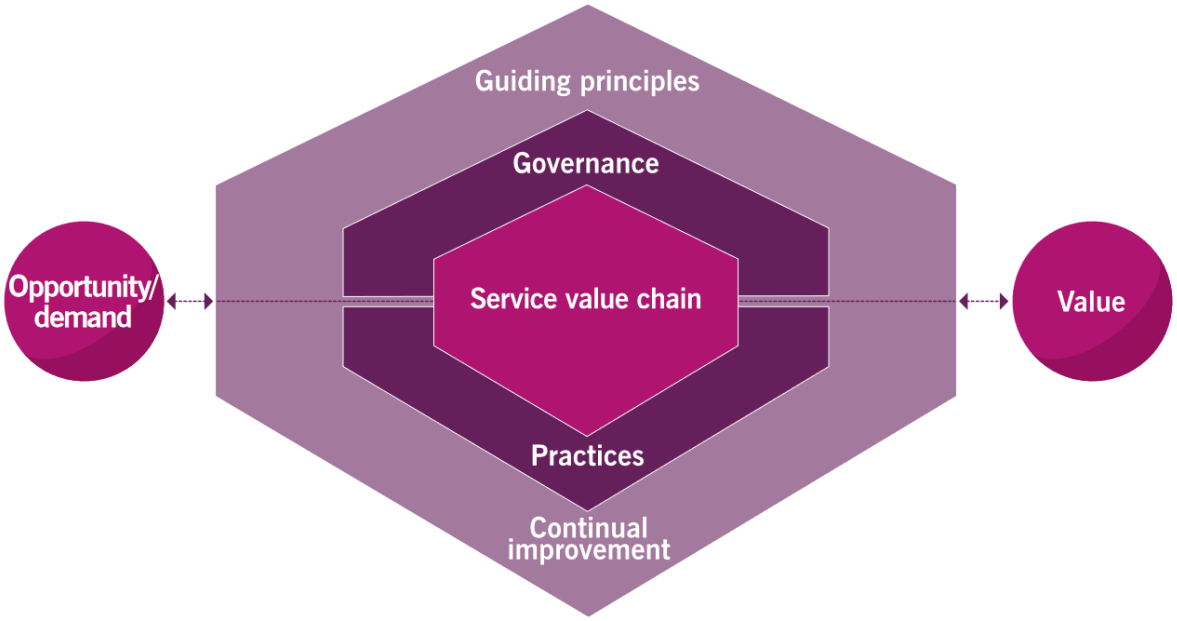


Figura 19. Estructura del Sistema del Valor del Servicio.
Fuente: AXELOS, (2019)

2.4.4 DAMA DMBOK

La gestión de datos se puede definir como el desarrollo, ejecución y supervisión de planes, políticas, programas y prácticas que tienen la tarea de entregar, controlar, proteger e incrementar el valor de los datos y la información a lo largo de su ciclo de vida. DAMA DMBOK es un marco de referencia que describe las áreas del conocimiento de la gestión de Datos (International, 2017b).

DMBOK, Data Management Body of Knowledge, es una colección de procesos y áreas de conocimientos para implementar las mejores prácticas para la gestión de datos. La guía Internacional DAMA proporciona conceptos y modelos para la estandarización de actividades, procesos, y mejores prácticas, describe los roles y responsabilidades en la gestión de los datos, detalla cuáles son los entregables y métricas que se deben aplicar y un modelo de madurez

(International, 2017a)

Agregar tabla comparativa entre las metodologías temáticas

Tabla 1. Tabla comparativa entre las metodologías

Metodología	Enfoque principal	Seguridad en el SDLC	Fortalezas	Limitaciones
DevOps	Integración entre desarrollo y operaciones	Considera la seguridad, pero usualmente se implementa al final del ciclo de desarrollo	Agiliza la entrega de software. Promueve automatización y colaboración	Seguridad no es prioritaria. Riesgo de vulnerabilidades si no se complementa con prácticas adicionales
DevSecOps	Seguridad integrada desde el inicio del desarrollo	Seguridad embebida a lo largo de todo el SDLC (desde diseño hasta producción)	Seguridad proactiva y automatizada Reducción de costos y vulnerabilidades Alta compatibilidad con prácticas ágiles y CI/CD	Requiere cambios culturales y técnicos Demanda inversión en automatización y capacitación
ITIL v4	Gestión de servicios de TI	Trata la seguridad como parte de la gestión de servicios (Gestión de la seguridad de la información)	Marco maduro y ampliamente adoptado. Enfoque estructurado de procesos	No está centrado en desarrollo de software. Seguridad más reactiva que preventiva.
DAMA DMBOK	Gobernanza de datos y gestión de información	La seguridad está centrada en la protección de datos y su ciclo de vida	Cobertura integral del ciclo de vida de los datos. Énfasis en privacidad y gobernanza	No aborda el desarrollo de software directamente. Falta integración con prácticas DevOps

Fuente: Elaboración Propia

Al realizar las comparativas entres estas 4 metodologías temáticas, DevSecOps es el marco más adecuado para abordar los desafíos actuales de seguridad en los sistemas de información ya que permite integrar la seguridad desde el inicio y la automatiza permitiendo realizar entregas rápidas, seguras y eficientes.

2.5 HERRAMIENTAS

2.5.1 LAPTOP

Se utilizará una laptop para llevar a cabo la investigación, ya que por medio de ella se buscará la información, se almacenarán los datos e información encontrada y además se instalarán

los programas y herramientas necesarios para realizar el análisis y minería de datos.

2.5.2 PYTHON

Python es un lenguaje de programación de alto nivel, reconocido por su sintaxis clara y legible que facilita su aprendizaje. Python es extremadamente potente y se utiliza en una variedad de aplicaciones, desde desarrollo web hasta análisis de datos y ciencia de datos. Python ha ganado terreno en la ciencia de datos gracias a su simplicidad y la variedad de bibliotecas que posee para el análisis de datos. (CodeSpaceAcademy, 2023)

Tabla 2. Comparativa de herramientas para análisis de datos

Característica	SAS	Python	R
Costo	Herramienta de Pago	Open.source y gratuito	Open.source y gratuito
Flexibilidad	Capacidades de visualización interactivas	Bibliotecas poderosas, pero requiere codificación	Opciones de visualización, pero requiere librerías
Bibliotecas	Limitado	Amplio exosistema de bibliotecas	Gran colección de paquetes estadísticos centradas en estadísticas avanzadas
Comunidad y Soporte	Gran soporte empresarial, pero menos comunidad abierta	Gran comunidad global y documentación abundante y recursos gratuitos	Comunidad activa en estadística pero menos extensa que la de Python

Fuente: Elaboración propia

Se decidió trabajar con Python para el análisis de los fatos por su flexibilidad, costo, amplio ecosistema de bibliotecas para realizar análisis avanzados y realizar representaciones gráficas de los resultados de los análisis. Además, cuenta con una comunidad activa y documentación gratuita.

2.5.3 KNIME

Es una plataforma de análisis de código abierto que cuenta con un gran conjunto de componentes y herramientas. Esta herramienta puede ser utilizada para realizar una carga de datos desde diferentes fuentes, permitiendo realizar el análisis de los datos, transformarlos y poder descargarlos a diferentes formatos (Bakos, 2013).

Tabla 3. Comparativa de herramientas para minería de datos

Característica	Knime	Alteryz	RapidMiner
Facilidad de uso	Interfaz gráfica de flujo de trabajo intuitiva	Interfaz un poco más compleja para usuarios novatos	Requiere tiempo para uso de su interfaz visual
Capacidad de análisis de datos	Ofrece un gran y potente conjunto de herramientas	Potente en la manipulación y preparación de datos, pero con menos herramientas que Knime	Capacidades enfocadas en la minería de datos

Flexibilidad	Posee una gran variedad de extensiones	Limitaciones con la integración de herramientas externas	Extensible, pero con soporte limitado

Fuente: Elaboración propia

Se utilizará Knime para realizar análisis de los datos encontrados de la investigación, para poder agruparlos y realizar transformaciones de los mismos, se seleccionó esta herramienta por su facilidad de uso, por poseer una capacidad amplia de análisis de datos y una gran variedad de extensiones-

2.5.4 POWERBI

Es una herramienta que permite cargar información de diversas fuentes como ser bases de datos relacionales, archivos de Excel y otras fuentes no estructuradas de datos, y permite crear informes completos con tablas, gráficos, indicadores que sean visualmente eficientes y permitan comunicar o compartir con otras personas dentro o fuera de la organización la información analizada (Polanco & Betancourt, 2022).

Tabla 4. Comparativa de Herramientas para Visualización de Datos

Característica	PowerBI	Tableau	Qlik
Integración	Integración fluida con Microsoft	Integración con Tableau Server	Integración con Qlik Cloud
Costo	Plan gratuito y planes de pago	Planes de Pago	Planes de Pago
Facilidad de uso	Fácil de usar	Curva de aprendizaje moderada	Curva de aprendizaje moderada
Conectividad de datos	Amplia conectividad con Excel, SQL etc.	Conexiones a múltiples fuentes de datos	Conexiones a múltiples fuentes de datos
Visualización	Gráficos interactivos y personalizables	Gráficos avanzados y personalizables	Visualizaciones interactivas

Fuente: Elaboración propia.

Para la visualización de los datos se utilizará la herramienta PowerBI, porque es muy útil, fácil de utilizar para crear gráficas que permitan visualizar de mejor manera el análisis de los datos y se puede utilizar con un gran conjunto de orígenes de datos.

2.6 CONCEPTUALIZACIÓN

2.6.1 SDLC

SDLC, ciclo de vida de desarrollo de software (Software Development Life Cycle) es una serie de etapas que se deben seguir para el proceso de desarrollo y revisión de un sistema de

información. Cada etapa es un segmento que contiene diversos tipos de actividades, cada etapa es completada en una secuencia determinada haciendo uso de herramientas tecnológicas (Everett et al., 2007).

2.6.2 SSDLC

SSDLC, Ciclo de vida de desarrollo de software seguro (Secure Software Development Life Cycle), es un conjunto de principios y pautas de diseño que deben aplicarse en el SDLC con el propósito de identificar, prevenir y solucionar posibles fallos de seguridad en el proceso de desarrollo y adquisición de aplicaciones. El objetivo es obtener software de alta confiabilidad y resistente contra ataques maliciosos, garantizando que el software desempeñe únicamente las funciones previstas, esté exento de vulnerabilidades, ya sean deliberadas o involuntarias, que se hayan incorporado en su ciclo de vida, y asegurando su integridad, disponibilidad y confidencialidad (AWS, 2023) (*García Clavijo & Betancur Gil*, 2023).

2.6.3 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de Tecnologías de la Información y comunicación, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2014) (Valencia Duque et al., 2017).

2.6.4 CIBERSEGURIDAD

La ciberseguridad está enfocada en la protección de la información y sistemas que se utilizan para almacenar o gestionar información y sus tres pilares fundamentales son la confidencialidad, la integridad y disponibilidad (Wilches, 2015).

2.6.5 MINERÍA DE DATOS

La minería de datos es un conjunto de técnicas encaminadas al descubrimiento de la información contenida en grandes conjuntos de datos. Se trata de analizar comportamientos, patrones, tendencias, asociaciones y otras características del conocimiento inmerso en los datos (Marqués, 2015).

Las técnicas de minería de datos, intentan obtener patrones o modelos a partir de los datos recopilados, las técnicas más representativas son las redes neuronales, regresión lineal, arboles de

decisión, reglas de asociación y agrupamiento (clustering).(Camana, 2016).

2.6.6 ITIL

ITIL es una guía para la gestión de servicios de TI, proporciona una orientación para las organizaciones que necesitan abordar nuevos desafíos en la gestión de servicios y quieren utilizar la tecnología moderna. Los componentes claves de ITIL son el sistema de valor de servicios SVS y el modelo de las cuatro dimensiones (AXELOS, 2019b).

2.6.7 SVS

El sistema de valor del servicio (Service Value System) representa como los componentes y actividades de una organización trabajan en conjunto para crear valor a través de los servicios habilitados por TI. La SVS facilita la integración y coordinación y ofrece una dirección fuerte, unificada y enfocada en el valor para las organizaciones (AXELOS, 2019b).

2.7 MARCO LEGAL NACIONAL E INTERNACIONAL

En esta sección se detallará el marco legal que incluye normativas, leyes, estrategias y estándares que han sido desarrolladas e implementadas tanto nacional como internacionalmente con la finalidad de garantizar la seguridad y privacidad de la información y del software desarrollado.

2.7.1 MARCO LEGAL NACIONAL

En el marco legal Nacional existen diferentes leyes y regulaciones que abordan los temas relacionados con la ciberseguridad y seguridad de la información. A continuación, se presentan algunas de las más relevantes, que son esenciales para guiar una implementación de prácticas seguras en el desarrollo de software y la protección de los datos e información que se incluyen en los sistemas informáticos.

Tabla 5. Marco Legal Nacional

Marco Legal	Impacto en la investigación
Código Penal de Honduras Articulo 398. Acceso no autorizado a sistemas informáticos (Poder Legislativo Honduras, 2019)	Este artículo establece que acceder de manera ilícita a sistemas, bases de datos o redes informáticas constituye un delito, y busca proteger la integridad, confidencialidad y disponibilidad de la información digital.
Código Penal de Honduras Articulo 399. Daños a datos y sistemas informáticos (Poder Legislativo Honduras, 2019)	Este artículo penaliza daños intencionales a datos y sistemas informáticos, impulsando a los desarrolladores a priorizar la seguridad en el desarrollo de software. Esto incluye implementar medidas contra manipulaciones, realizar auditorías regulares y proteger la integridad de la información.
Código Penal de Honduras Articulo 400. Abuso de	El Artículo 400 fomenta el desarrollo seguro al

dispositivos (Poder Legislativo Honduras, 2019)	requerir medidas de control para prevenir el uso indebido de dispositivos tecnológicos. Promueve la adopción de medidas de autenticación seguras, la identificación de actividades inusuales y la realización de pruebas de seguridad.
Código Penal de Honduras Articulo 401. Suplantación de identidad (Poder Legislativo Honduras, 2019)	El Artículo 401 del Código Penal de Honduras, al tipificar la suplantación de identidad, resalta la necesidad de robustecer la seguridad en el desarrollo de software, implementando autenticación fuerte y monitoreo de actividades para prevenir accesos no autorizados.
Decreto_130-2017	El Decreto 130-2017 establece el marco legal para la promoción de la industria de software en Honduras, creando incentivos fiscales y regulaciones para fomentar la innovación tecnológica. Este decreto impulsa el desarrollo de software local al facilitar la inversión, la formación de talento y la creación de empresas tecnológicas.
Normativa de Seguridad de Honduras	La normativa de seguridad en Honduras establece directrices que impactan directamente el desarrollo de software, exigiendo la implementación de medidas de protección de datos y ciberseguridad. Esto promueve la creación de aplicaciones más seguras, fomenta la confianza del usuario y minimiza riesgos legales, garantizando un entorno digital más seguro y responsable.
Reglamento de Ciberseguridad para Bancos	Este reglamento establece normas que buscan proteger la integridad y confidencialidad de la información que se maneja en las entidades financieras.
Ley de Protección de Datos Personales	La ley de Protección de Datos sirve para regular el manejo adecuado de la información personal, protegiendo derechos como el acceso, modificación y tratamiento de datos.

Fuente: Elaboración Propia

2.7.2 MARCO LEGAL INTERNACIONAL

A nivel internacional, el marco legal sobre la protección de los datos y ciberseguridad está conformada por diversas normativas, reglamentos y leyes que buscan establecer estándares globales con el objetivo de garantizar la seguridad de la información y la privacidad de los datos de los usuarios en el entorno digital. A continuación, se destacan algunas de las normativas:

Tabla 6. Marco Legal Internacional

Ley / Normativa / Reglamento	Impacto en la investigación

Norma ISO 27001	Esta norma establece un marco de referencia para implementar, mantener y mejorar un sistema de gestión de seguridad de la información (manzanelli, 2023c)
Norma ISO 27034	La norma ISO/IEC 27034 tiene un enfoque en la Seguridad de la información en las aplicaciones, esta norma apoya a las organizaciones en el camino de asegurar que las aplicaciones protejan la información confidencial y sean seguras (manzanelli, 2023b)
Norma ISO 29119	La norma ISO 29119 es un conjunto de estándares internacionales que definen los procesos, técnicas y documentación necesarios para llevar a cabo pruebas de software efectivas (manzanelli, 2023a)
Reglamentación General de Protección de Datos (GDPR) de la unión europea	Es una de las leyes más avanzadas del mundo. Esta ley establece un conjunto de normas estrictas para la protección de los datos personales de los ciudadanos europeos (Reglamento general de protección de datos, 2016)
La ley de Ciberresiliencia en la unión europea	Tiene como objetivo proteger a los clientes y las organizaciones que compran o utilizan productos o software con un componente digital. La Ley aborda el nivel inadecuado de ciberseguridad inherente a muchos productos o las actualizaciones de seguridad inadecuadas de dichos productos y software (Unión Europea, 2024)
Estrategia de Ciberseguridad del Departamento de Defensa de Estados Unidos	La Estrategia de Ciberseguridad del Departamento de Defensa de Estados Unidos es un marco que busca proteger los sistemas y datos del país frente a amenazas cibernéticas. Esta estrategia impacta en el desarrollo de software al exigir que se implementen prácticas de seguridad desde las etapas iniciales del ciclo de vida del software, garantizando que las aplicaciones sean más seguras y resistentes a ataques. (Nist, 2024; Oficina del Director Nacional Cibernético | La Casa Blanca, 2023)
ITIL v4	ITIL 4 no es una ley, pero si es un estándar ampliamente reconocido y adoptado a nivel internacional para la gestión de servicios TI. La adopción de ITIL 4 facilita el cumplimiento de normativas legales o regulatorias relacionadas con la gestión de servicios de TI, como las normas ISO/IEC 20000 o GDPR

Fuente: Elaboración propia

CAPÍTULO III – METODOLOGÍA DE LA INVESTIGACIÓN

En este capítulo se describen la metodología a utilizar para realizar la presente investigación sobre el impacto de la implementación de DevSecOps en el SDLC, se mencionará el enfoque a utilizar y el alcance que tendrá la investigación, se mencionará el diseño de la investigación que incluye describir cuál será la población y la muestra que se utilizará. Se establecerán los criterios de inclusión y exclusión que se tomarán en cuenta para asegurar la relevancia de la información.

Además, se describirán las hipótesis, se detallarán las variables de estudio, se mencionarán las técnicas, Instrumentos y procedimientos aplicados a la investigación, las fuentes que fueron utilizadas y la matriz de congruencia.

3.1 CONGRUENCIA METODOLÓGICA

3.1.1 MATRIZ DE CONGRUENCIA METODOLÓGICA

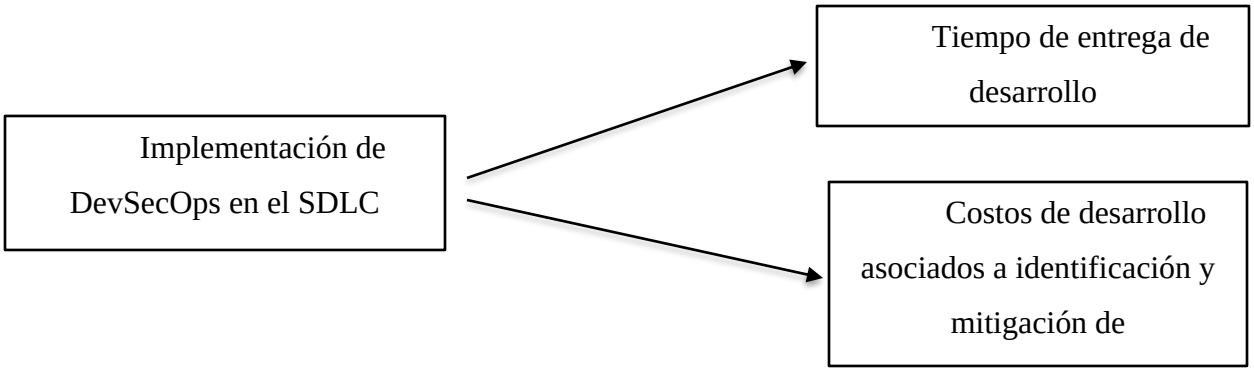
En la siguiente tabla se muestra la matriz de congruencia metodológica de la investigación, la cual es una herramienta clave para asegurar la alineación entre los objetivos, las preguntas de investigación, las variables, la metodología y los instrumentos utilizados. Esta matriz permite visualizar de manera clara como cada elemento de la investigación se relaciona, garantizando que todos los elementos estén en coherencia y contribuyan al logro de los objetivos planteados.

Tabla 7. Matriz de Congruencia Metodológica

Nombre de la Investigación	Problema	Pregunta(s) de Investigación	Objetivos de la Investigación	Metodología	Instrumentos	Variables	Indicadores
Impacto al integrar DevSecOps durante el ciclo de vida del desarrollo de software en las organizaciones a nivel mundial 2023-2024	A nivel mundial, han ocurrido muchos ataques a los sistemas de información de las organizaciones de diferentes rubros, financiero, comercial, educativo, entre otros, ya sea ataques por personas externas o internas de la organización. Los hackers, ciberdelincuentes o personas que intentan ingresar a un sistema de la organización, aprovechan cualquier vulnerabilidad que puedan encontrar en el software para intentar acceder a la información confidencial de la organización.	**General** ¿Cuál es el impacto en las organizaciones al integrar DevSecOps en el ciclo de vida de desarrollo de software y cómo los equipos de desarrollo perciben y adoptan estas prácticas? **Específicas** ¿Qué prácticas de DevSecOps se pueden integrar en cada fase del ciclo de vida de desarrollo de software para identificar vulnerabilidades y mitigar amenazas que se puedan presentar cuándo el software se encuentre en producción? ¿Cuánto se puede disminuir el tiempo de entrega de desarrollo y cuánto se puede ahorrar en costos de desarrollo de software? ¿Cómo perciben y adoptan los equipos de desarrollo la integración de DevSecOps en el SDLC?	**General** Analizar el impacto en las organizaciones al integrar DevSecOps durante el ciclo de vida de desarrollo de software y conocer como los equipos de desarrollo adoptan la integración de estas prácticas . **Específicos** Identificar que prácticas de DevSecOps se pueden integrar en el desarrollo de software que ayuden a identificar vulnerabilidades y mitigar amenazas que se pueden presentar cuando el software se encuentre en producción. Mejorar la identificación de vulnerabilidades en el software que permitan en costos de desarrollo. Disminuir el tiempo de entrega del desarrollo de software. Conocer cuál es la percepción y adopción de DevSecOps por parte del equipo de desarrollo de la organización.	Enfoque mixto, cualitativo y cuantitativo; Alcance descriptivo.	**Metodológicos**: Encuestas: 2024 Global DevSecOps, SANS 2023 DevSecOps Survey y Global State of DevSecOps 2024 **Tecnológicos**: Laptop, Planner, Jira, Knime, PowerBI	**Independientes** Implementación de DevSecOps en el SDLC **Dependientes**: Tiempo de entrega de desarrollo Costos de desarrollo asociados a identificación y mitigación de vulnerabilidades	Número de medidas implementadas Porcentaje de etapas del SDLC con al menos una práctica de DevSecOps implementada. Tiempo transcurrido en cada fase del SDLC. Costo de corrección de errores relacionados con la seguridad del software

Fuente: Elaboración propia.

3.1.2 ESQUEMAS DE VARIABLES DE ESTUDIO



3.1.3 OPERACIONALIZACIÓN DE LAS VARIABLES

Para el desarrollo de la presente investigación se han identificado las variables claves que serán el objeto de análisis. A continuación, se presenta la tabla que detalla la operacionalización de estas variables. En ella se incluye aspectos como el tipo de variable, la definición conceptual y operacional, así como los indicadores, dimensión y escala de medición de cada variable.

Tabla 8. Operacionalización de las variables

Variable	Tipo	Definición conceptual	Definición Operacional	Indicador	Dimensión	Escala de medición
Implementación de DevSecOps en el SDLC	Independiente	Prácticas de DevSecOps que se implementan en cada etapa del ciclo de vida del desarrollo de software	Porcentaje de etapas del SDLC en las que se DevSecOps, evaluadas mediante herramientas o cuestionarios estructurados.	Número de medidas implementadas Porcentaje de etapas del SDLC con al menos una práctica de DevSecOps implementada.	Seguridad en fases del SDLC	Ordinal (Bajo <50, , Alto>=50)
Tiempo de entrega de desarrollo	Dependiente	Período transcurrido desde el inicio del desarrollo hasta la entrega del software.	Tiempo transcurrido desde el inicio del desarrollo hasta la entrega del software.	Tiempo transcurrido en cada fase del SDLC.	Tiempo de desarrollo de cada fase del SDÑC	Escala de razón (Tiempo en días)

Costos de desarrollo asociados a identificación y mitigación de vulnerabilidades	Dependiente	Recursos monetarios totales que se necesitan para completar el desarrollo de software relacionados a la identificación y mitigación de vulnerabilidades.	Total de gastos directos e indirectos, incluyendo costos de herramientas, formación del personal y tiempo invertido, asociados a actividades relacionadas con la identificación y mitigación de vulnerabilidades durante el desarrollo.	Costo de corrección de errores relacionados con la seguridad del software	Costos de mitigar vulnerabilidades.	Escala de razón (Costo en Lempiras)

Fuente: Elaboración propia.

3.1.4 HIPÓTESIS

En esta investigación se busca establecer una relación entre la implementación de prácticas DevSecOps y los ahorros en tiempo y costos asociados al desarrollo de software en específico los relacionados con la identificación y mitigación de vulnerabilidades.

Este apartado de la investigación se enfoca en formular hipótesis específicas que permitan evaluar como la adopción de DevSecOps puede generar beneficios tangibles para las organizaciones, en esta investigación se formularon dos hipótesis que tienen relación con el tiempo de entrega del desarrollo de software y la disminución de costos operativos, que son dos variables muy importantes para conocer el impacto de integrar DevSecOps en el ciclo de vida de desarrollo de software.

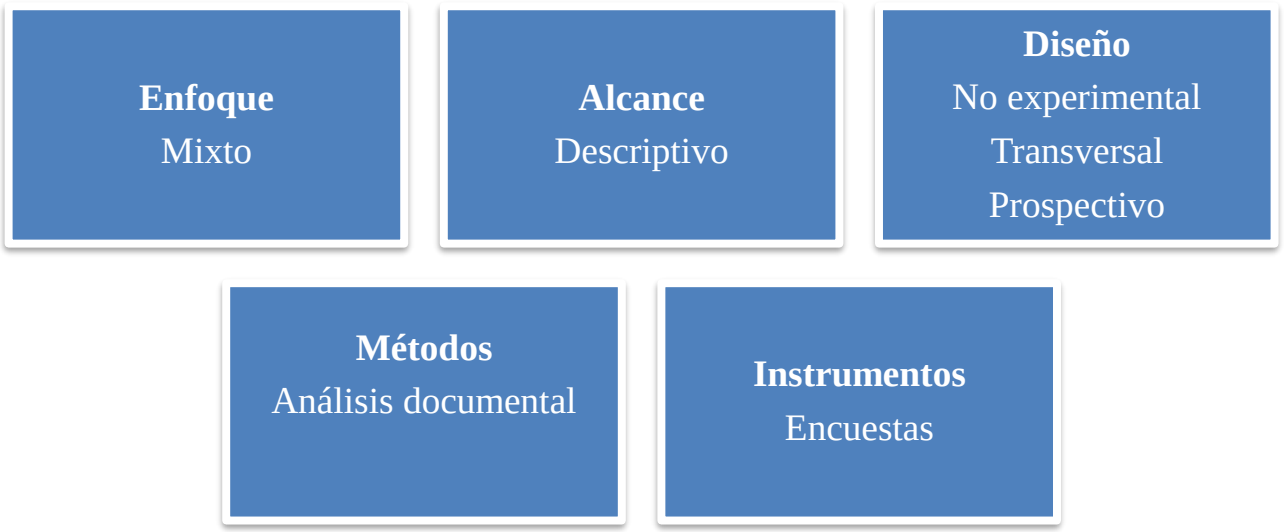
Tabla 9. Hipótesis

Variable	Hipótesis Nula (H_0)	Hipótesis Alternativa (H_1)
Tiempo de desarrollo	El tiempo de entrega del desarrollo no disminuye al implementar DevSecOps a lo largo del SDLC.	El tiempo de entrega del desarrollo disminuye al implementar DevSecOps a lo largo del SDLC.
Costos de desarrollo	El costo relacionado con el desarrollo de software, al identificar y mitigar vulnerabilidades desde el inicio del desarrollo, no disminuye cuando se implementa DevSecOps en el SDLC	El costo relacionado con el desarrollo de software, al identificar y mitigar vulnerabilidades desde el inicio del desarrollo, disminuye cuando se implementa DevSecOps en el SDLC

Fuente: Elaboración propia.

3.2 ENFOQUE Y MÉTODOS

En el siguiente gráfico se muestra el enfoque y los métodos de la presente investigación.



3.2.1 ENFOQUE DE LA METODOLOGÍA

En esta investigación se utilizará un enfoque mixto, este enfoque combina elementos de los enfoques cuantitativo y cualitativo, con el objetivo de utilizar las fortalezas de ambos enfoques y así obtener una comprensión más completa del problema investigado. (Hernández-Sampieri et al., 2018; Romero et al., 2023)

El enfoque será mixto, cuantitativo porque se utilizarán datos estadísticos de las fuentes que proporcionan porcentajes y promedios de las respuestas a las preguntas realizadas y cualitativo porque se explorarán las experiencias y puntos de vista de los equipos de desarrollo de software que han implementado e interactuado con DevSecOps durante todo el SDLC.

3.2.2 ALCANCE DE LA METODOLOGÍA

La presente investigación tendrá un alcance descriptivo porque se analizarán los datos encontrados para conocer el impacto de implementar DevSecOps en el SDLC, se realizará la interpretación de los datos para tener una visión clara e integral de las respuestas obtenidas en cada una de las encuestas y reportes que se utilizarán como fuentes de información.

El alcance descriptivo permite realizar una investigación detallada, clara y precisa para

entender mejor el contexto y las variables involucradas.

Además, la presenta investigación cuenta con un alcance experimental ya que se establecerán hipótesis relacionadas con las variables que se identificaron y se realizarán las pruebas necesarias para lograr concluir acerca de ellas

3.2.3 DISEÑO DE LA INVESTIGACIÓN

El diseño de la presente investigación es **no experimental** porque no hay manipulación de las variables. Los datos utilizados son de fechas especificas desde el año 2023 y año 2024 por lo que la investigación tiene un diseño **transversal.** Al analizar datos de encuestas realizadas en años anteriores la investigación presenta un diseño **retrospectivo** ya que se utilizarán los datos recolectados en el pasado para analizarlos en el presente.

3.3 DISEÑO DE LA INVESTIGACIÓN

3.3.1 POBLACIÓN

La población para esta investigación es de **6618 encuestados y** en la tabla siguiente se muestra el detalle por cada una de las fuentes utilizadas y está compuesta por las personas y organizaciones a nivel mundial que participaron en las encuestas seleccionadas como fuentes de información. Estas encuestas incluyen datos provenientes de sectores como desarrollo de software, manufactura, servicios financieros, telecomunicaciones, entre otros, donde se ve involucrado un equipo de desarrollo de software y organizaciones de diferentes tamaños y de diversos países a nivel mundial.

La población de cada una de las encuestas y reportes a utilizar está integrada de la siguiente manera:

Tabla 10. Detalles de la Población

Nombre de la Encuesta	Cantidad de Encuestados
2024 Global DevSecOps Report	5,315 (GitLab, 2024)
SANS 2023 DevSecOps Survey	363 (Allen et al., 2023)
Global State of DevSecOps 2024	1000 (Blackduck, 2024)
Total	6,618 encuestados

Fuente: Elaboración propia.

3.3.2 MUESTRA

Se utilizará toda la población, todos los datos disponibles, porque las fuentes encontradas no muestran una segmentación o clasificación clara por categorías como país o industria en las respuestas a cada una de las preguntas que conforman la encuesta. En su lugar, los datos recolectados se muestran de forma general lo que limita la posibilidad de realizar un análisis más

detallado. Por esta razón, es necesario trabajar con el conjunto completo de loa datos, garantizando una visión integral, aprovechando al máximo la información disponible y evitando posibles sesgos derivados de una segmentación que no se encuentra disponible.

Al trabajar con toda la población pueden existir ciertas limitaciones como una mayor complejidad en el análisis ya que se requerirá mayor tiempo para analizar todos los datos, además el análisis pude centrarse en promedios generales y no identificar patrones de subgrupos o categorías. Aunque en esta investigación se utilizará la totalidad de los datos disponibles, es importante considerar que la representatividad de los resultados depende de la metodología de recolección utilizada en las encuestas originales.

Se trabajará con toda la población, pero se seleccionarán solo las preguntas que ayuden a responder con las preguntas de investigación y a cumplir con los objetivos propuestos.

3.3.3 TÉCNICAS DE MUESTREO

En esta investigación se trabajará con toda la población por lo que no se utilizarán técnicas de muestreo. Esto se debe a que en la información encontrada en las fuentes consultadas presenta los datos de las respuestas de los encuestados son presentados de manera general y no segmentadas en categorías. Además, las características de los datos recolectados son preseleccionados según los criterios de los estudios originales de las fuentes consultadas.

3.4 CRITERIOS DE SELECCIÓN DE LOS DATOS

En la tabla siguiente, se presentan cuáles serán los criterios de inclusión y exclusión que se emplearán para seleccionar los datos que se analizarán a lo largo de la investigación. Estos criterios son esenciales para garantizar la relevancia y calidad de los datos recopilados, asegurando que la información seleccionada sea pertinente y representativa al problema de la presente investigación.

Los criterios de inclusión ayudan a identificar los datos que cumplen con los requisitos del análisis y los de exclusión a eliminar aquellos que no cumplan.

Tabla 11. Criterios de selección de los datos

Criterio	Inclusión	Exclusión
Actualidad de la información	Datos de los últimos 5 años del 2020 al 2024	Datos que sean antes del 2020
Entidades de selección	Encuestas o reportes de personas y organizaciones que tengan relación con equipos de desarrollo de software	Encuesta o reportes de personas y organizaciones que tengan relación con equipos de desarrollo de software
Relevancia del tema	Encuestas o reportes relacionados con el tema DevSecOps	Encuestas o reportes que no aborden aspectos relacionados con el tema DevSecOps
Tamaño de la	Encuestas o reportes que contengan datos de	Encuestas o reportes que contengan sólo

entidad	empresas de diferentes tamaños.	datos de empresas del mismo tamaño
Fuente de información	Encuestas realizadas por empresas relacionadas con el desarrollo de software o implementación de DevSecOps	Encuestas realizadas por empresas no relacionadas con el desarrollo de software o implementación de DevSecOps

Fuente: Elaboración propia.

3.4 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

En este apartado, se describirá la técnica, instrumentos, procedimientos y plan de análisis, utilizados para recopilar y analizar los datos en la presente investigación, proporcionando una visión clara y objetiva del enfoque metodológico utilizado en la investigación.

3.4.1 TÉCNICAS

El **análisis documental** es la técnica que se utilizará para el análisis de los datos. Esta técnica ayudará a recopilar y analizar la información actualizada y relevante de que se encuentra en los documentos digitales como son los reportes y encuestas relacionadas con la implementación de DevSecOps en el SDLC (Hernández-Sampieri et al., 2018)

Se seleccionó la técnica de análisis documental por las siguientes razones:

- **Alcance global**: Permite recolectar datos de encuestas sobre implementación de DevSecOps en el SDLC publicadas en los sitios web de las empresas internacionales como GitLab, SNAS y BlackDuck, lo que asegura contar con un alcance global sobre el problema de investigación.
- **Confiabilidad de los datos**: Las encuestas fueron realizados por organizaciones relacionadas al desarrollo de software y la implementación de DevSecOps lo que garantiza la calidad de los datos.
- **Eficiencia**: Este enfoque optimiza tiempo y recursos, ya que no requiere la creación de instrumentos propios.

3.4.2 INSTRUMENTOS

En la investigación, se utilizarán solo fuentes secundarias por lo que no se diseñaron instrumentos propios. Las encuestas seleccionadas actúan como los instrumentos claves, ya que proporcionan datos sobre la implementación de DevSecOps en las organizaciones a nivel global. Estas encuestas fueron realizadas por organizaciones como Gitlab, SANS y Blackduck, que están relacionadas con el desarrollo de software y la implementación de DevSecOps.

Tabla 12. Encuestas

Nombre de la Encuesta	Técnicas de muestreo
2024 Global DevSecOps Report	Participaron 5315 profesionales de 39 países (GitLab, 2024). La encuesta fue distribuida a través de canales como redes sociales y correo electrponico de Gitlab.
SANS 2023 DevSecOps Survey	Los 363 participantes de la encuesta de este año representan un conjunto muy diverso de roles, industrias y tamaños de organización (véase la Figura 1). Como era de esperar, muestran una fuerte preferencia por la seguridad, ya que el 34 % de los encuestados desempeña algún tipo de función de seguridad directa. El administrador/analista de seguridad es, con diferencia, el rol más común, con un 10,2 %. Los roles de desarrollo, como desarrollador de aplicaciones, arquitecto de la nube, ingeniero de software e ingeniero de DevOps, también están bien representados, con un 21 %. Sin embargo, el rol más representado en la encuesta es el de gerente de negocios, con un 13 % de los encuestados, lo que demuestra claramente que DevSecOps se reconoce ampliamente como una preocupación empresarial, no solo como un problema técnico. Los roles de gestión y ejecutivos, incluido el de gerente de negocios, representan el 40 % de los encuestados (incluidos gerentes de seguridad y cumplimiento, gerentes de versiones de análisis de calidad [QA], altos ejecutivos y gerentes/directores de TI). (Allen et al., 2023)
Global State of DevSecOps 2024	Las conclusiones del informe "Estado global de DevSecOps 2024" se basan en una encuesta exhaustiva que Black Duck® encargó a Censuswide, una consultora internacional de investigación de mercados. En la encuesta participaron 1000 desarrolladores de software, profesionales de seguridad de aplicaciones (AppSec), CISO e ingenieros de DevOps de varios países e sectores. Este informe proporciona información crucial sobre el estado actual de las prácticas de DevSecOps y las pruebas de AppSec. Ofrece un análisis exhaustivo de tendencias, desafíos y oportunidades, y ofrece información práctica para las organizaciones que buscan mejorar sus prácticas de DevSecOps. (Blackduck, 2024)

Fuente: Elaboración propia.

3.4.3 PROCEDIMIENTOS

El procedimiento a seguir para el desarrollo de esta investigación será:

- Búsqueda de información: Buscar información actualizada sobre la implementación de DevSecOps en el SDLC en las organizaciones para identificar reportes o encuestas sobre DevSecOps utilizando palabras clave como DevSecOps, seguridad en SDLC y DevSecOps en desarrollo de software en bases de datos como Google Scholar, Google Libros, ResearchGate y los sitios oficiales de organizaciones relevantes al tema de investigación.
- Selección de datos: Seleccionar encuestas o reportes de acuerdo a los criterios de inclusión definidos, actualidad de la información, relevancia del tema, tipo de fuente

de información.

- Análisis preliminar: Verificar los datos encontrados e identificar las variables de estudio mediante las metodologías utilizadas para garantizar la calidad de los datos.
- Procesamiento de los datos. Para el análisis e interpretación de los datos se utilizará herramientas como KNIME para importar los datos recolectados, realizar el procesamiento y análisis exploratorio de los datos y PowerBI se usará para generar visualizaciones interactivas que permitan identificar tendencias y patrones clave. Se utilizará las normas APA versión 7 para citar las fuentes de información consultadas.

3.4.4 PLAN DE ANÁLISIS

El plan de análisis para esta investigación se basa en un alcance descriptivo y en la utilización de un enfoque mixto, que combina tanto datos cualitativos como cuantitativos, para garantizar la precisión y confiabilidad de los resultados. A continuación, se detallan las fases específicas para el plan de análisis.

Tabla 13. Plan de análisis

Fase	Descripción	Herramientas	Objetivo
Recolección y selección de Datos	Se buscará información relacionada con la implementación de DevSecOps Selección de los datos más relevantes.	Sitios web oficiales de empresas relacionadas con DevSecOps como: Gitlab, SANS y BlackDuck.	Recolectar información actualiza sobre la implementación de DevSecOps en el SDLC
Procesamiento de los datos	Revisión de los datos para asegurar su calidad y confiabilidad.	KNIME	Asegurar que los datos sean de calidad y confiables.
Análisis descriptivo	Análisis de los datos recolectados para conocer la relación entre las variables.	KNIME y Python	Analizar los datos y encontrar la relación entre las variables de estudio
Análisis inferencial	Pruebas de hipótesis entre las variables encontradas	Pruebas de hipótesis	Explicar el impacto que tiene la implementación de DevSecOps en el SDLC
Interpretación de los resultados	Elaborar informe de los resultados del análisis. Elaborar gráficas para interpretar los resultados obtenidos.	PowerBI Word	Dar a conocer los resultados del análisis.

Fuente: Elaboración propia.

3.5 FUENTES DE INFORMACIÓN

Las fuentes de información juegan un papel fundamental dentro de la investigación, porque son los elementos esenciales a partir de los cuales se recopila y analiza la información necesaria para responder a las preguntas y cumplir con los objetivos de la investigación planteados. Estas fuentes pueden ser primarias o secundarias, las primarias son encuestas, entrevistas o

experimentos, por otro lado, las secundarias incluyen documentos, reporte, artículos o estudios previos.

3.5.1 FUENTES PRIMARIAS

En el desarrollo de esta investigación no se utilizarán fuentes primarias.

3.5.2 FUENTES SECUNDARIAS

Las fuentes secundarias que se utilizarán para la presente investigación son encuestas que fueron aplicadas a empresas y personas que pertenecen a diferentes industrias de diferente tamaño de países a nivel mundial.

Las 3 fuentes de información que se utilizarán son:

- 2024 Global DevSecOps Report, es una encuesta realizada por la empresa GitLab,
- SANS 2023 DevSecOps Survey, encuesta realizada por la empresa SANS y,
- Global State of DevSecOps 2024, encuesta realizada por la empresa Blackduck.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se presentan los resultados obtenidos a partir de la recolección y análisis de los datos, con el objetivo de proporcionar una compresión integral y detallada de los hallazgos más significativos. El análisis comenzará con una exploración inicial de los datos, abordando aspectos clave como la descripción general del conjunto de datos, el proceso de limpieza y preparación de los mismos, y las herramientas de visualización de datos utilizadas.

A lo largo del capítulo se detallará el informe completo del proceso de recolección de datos, incluyendo las fuentes de información consultadas, los instrumentos empleados para la recopilación, así como las dificultades encontradas durante el proceso. Se presentarán los resultados cuantitativos obtenidos, analizando los datos de acuerdo con los objetivos planteados en la investigación. El análisis también abordará las implicaciones de los resultados y cómo contribuyen al tema de investigación.

Se detallará la interpretación de los hallazgos más relevantes y destacando aquellos que tienen un impacto significativo en el tema de investigación. Además, se considerarán las limitaciones del estudio,

4.1 ANÁLISIS EXPLORATORIO DE DATOS (EDA)

4.1.1 DESCRIPCIÓN GENERAL DEL CONJUNTO DE DATOS

Se utilizarán los datos de las 3 fuentes de información seleccionadas las cuales son reportes y encuestas relacionadas con DevSecOps en los años 2023 y 2024. De estas fuentes se tomarán las preguntas más relevantes y que ayuden a cumplir con los objetivos de la presente investigación.

La población está compuesta por un total de 6618 encuestados que contestaron cada uno de los reportes y encuestas que son utilizados como fuentes secundarias, la muestra a utilizar será toda la población para poder realizar un mejor análisis ya que los datos no poseen una división por categorías o por registro por cada encuestado lo que dificulta poder determinar una muestra.

Los encuestados pertenecen a diversos países alrededor del mundo como ser Estados Unidos, Alemania, Australia, Canadá, Japón, India, entre otros, las organizaciones a las que pertenecen los encuestados son de diversos tamaños teniendo desde 24 empleados hasta más de 1000 empleados y de rubros como desarrollo de software, telecomunicaciones, servicios financieros, Gobierno, Salud, entre otros. Además, el puesto de trabajo al que pertenecen son

diversos de las áreas de desarrollo de software, operaciones y seguridad que son las tres áreas que se ven involucradas en la implementación de DevSecOps.

La estructura de los datos de los diferentes reportes está dada por preguntas y respuestas donde en las respuestas se indican las categorías que podía seleccionar el encuestado y el porcentaje de encuestados que seleccionó cada una de las categorías.

Dentro de las preguntas podemos encontrar datos sobre:

- Los criterios de seguridad más utilizados para decidir que pruebas de seguridad ejecutar.
- Las tasas de adopción de los años 2021-2023 de las diferentes prácticas de DevSecOps
- El número de herramientas de seguridad que utilizan las organizaciones.

Estas 3 preguntas ayudarán a cumplir el primer objetivo ya que nos ayudarán a conocer que prácticas de seguridad son aplicadas y mayormente adoptadas y saber qué criterios son considerados más importantes para decidir ejecutar pruebas de seguridad.

- La relación que existe entre el tiempo para entrega y desarrollo del software y las pruebas de seguridad.
- Los costos relacionados con la brecha de datos y la comparación entre las organizaciones que tienen un alto nivel de adopción de DevSecOps contra las que tienen un bajo o nulo nivel de adopción de esta metodología.

Estas 2 preguntas ayudarán a cumplir con el segundo objetivo para identificar si el tiempo y costos disminuyen en las organizaciones que deciden adoptar e implementar DevSecOps.

- Los desafíos que se enfrentan al implementar y adoptar DevSecOps.
- El conocimiento que tienen los miembros de la organización sobre temas de seguridad.

Estas 2 preguntas ayudarán a conocer la percepción y adopción de DevSecOps por parte del personal de las organizaciones que ha estado involucrado directamente con la implementación de esta nueva metodología.

4.1.2 LIMPIEZA Y PREPARACIÓN DE LOS DATOS

Para realizar la limpieza y preparación de los datos se utilizaron las herramientas de Knime y PowerBI, las cuales ayudarán a poder analizar los datos de una mejor manera y poder presentarlos en tablas y gráficas que sean visualmente agradables y fáciles de comprender.

Tabla 14. Valores nulos

Pregunta	Mean(P...	Median...
Costo de la brecha de datos	4.38	4.38
¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	16.667	11.945
¿Aproximadamente qué porcentaje de sus proyectos, ramas y repositorios se incluyen en su cola de pruebas de seguridad de aplicaciones?	16.668	14.62
¿Cuál de las siguientes afirmaciones describe mejor la manera en que se agregan nuevos proyectos, ramas o repositorios a la cola de pruebas de seguridad de su aplicación?	20	22.4
¿Está seguro del enfoque de su organización hacia la seguridad de las aplicaciones?	25	17
¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	20	18.04
¿Qué afirmación describe mejor su enfoque para analizar y limpiar los resultados de las pruebas de seguridad de publicaciones?	20	25.27

Fuente: Elaboración Propia

En la tabla anterior se puede observar que **no hay ningún valor faltante** en las respuestas de cada una de las preguntas utilizadas para realizar el análisis de los datos.

En la siguiente tabla se observan los resultados de una pregunta del reporte Global State of DevSecOps 202, como se puede visualizar la suma total de los porcentaje**s es mayor a 100%,** lo cual es un **valor atípico** porque debería ser 100% representando el porcentaje completo de los encuestados, pero esto se debe a que los encuestados tuvieron la posibilidad de seleccionar más de una categoría al responder la pregunta, por lo que si se considerará el análisis de los resultados porque es una pregunta que proporciona datos muy valiosos para conocer qué criterios son tomados en cuenta para seleccionar prácticas de seguridad.

Tabla 15. Resultados Pregunta sobre los criterios para realizar pruebas de seguridad

¿Cuál de los siguientes criterios tiene en cuenta su organización al determinar qué pruebas de seguridad de aplicaciones ejecutar y cuándo hacerlo?	
Categoria	**Porcentaje de Encuestados**
Sensibilidad de datos	36.77
Pácticas de terceros	35.88
Facilidad de configuración	35.38
cumplimiento normativo	34.99
Entorno de producción	33.99
Certificación de seguridad	33.70
Criticidad de la app	32.80
Frecuencia de lanzamiento	30.82
Publicación de vulnerabilidades	29.34
No aplica	2.78
Total	**306.45**

Fuente: Elaboración Propia

Otras de las preguntas del reporte Global State of DevSecOps 2024 donde la suma total de los porcentajes si da un 100% debido a que en esta los encuestados solo podían seleccionar una opción de las presentadas.

En esta pregunta también se observa una opción donde el encuestado podía indicar que no tenía suficiente visibilidad para estimar la cantidad de herramientas, esta opción es importante porque permite conocer que en algunas organizaciones no todos los empleados están informados sobre que herramientas de pruebas de seguridad utilizan.

Tabla 16. Resultados Pregunta sobre Cantidad de herramientas de pruebas de seguridad

¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	
NumeroHerramientas	**Porcentaje de encuestados**
1 - 5	9.32
6 - 10	33.50
11 - 15	33.30
16 - 20	14.57
21+	3.86
No puedo estimar la cantidad	5.45
Total	**100.00**

Fuente: Elaboración Propia

Para la presente investigación se utilizarán los datos de las preguntas donde el resultado del total de encuestados es 100 para garantizar una consistencia en los datos, y evitar interpretaciones erróneas ya que las preguntas donde la suma total del porcentaje de encuestados es mayor a 100 indica que podían seleccionar más de una respuesta, pero siempre se incluirán las preguntas que sumen más de 100% pero se realizará un análisis diferente se utilizarán porque proporcionan datos relevantes para la presente investigación.

Al realizar el análisis de los datos de las respuestas de cada pregunta se tomará en cuenta las categorías de las respuestas que pueden ser consideradas como respuestas de no certeza como por ejemplo las respuestas: no estoy familiarizado en cómo se agregan, no puedo estimar la

cantidad, no puedo evaluar la relación con precisión, etc., aunque estas respuestas presenten un porcentaje mínimo de los encuestados, su inclusión es importante para ofrecer una visión precisa y completa de las respuestas.

Los datos presentados en la figura y tabla siguientes son los resultados de la pregunta ¿Cuál de las siguientes afirmaciones describe mejor la manera en que se agregan nuevos proyectos, ramas o repositorios a la cola de pruebas de seguridad de su aplicación?, al ser datos que están categorizados para sacar la media se ordenaron las categorías y se le asignó un valor.

Tabla 17. Resultados Pregunta de Cómo se agregan las Pruebas de Seguridad

Orden	Categoria	Porcentaje
0	No estoy familiarizado con cómo se agregan	4.37
1	Manualmente	28.74
2	La mayoría manualmente; algunos automáticos	6.14
3	La mayoría automáticamente; algunos manuales	22.40
4	Automáticamente	38.35
10		**100.00**

Fuente: Elaboración Propia

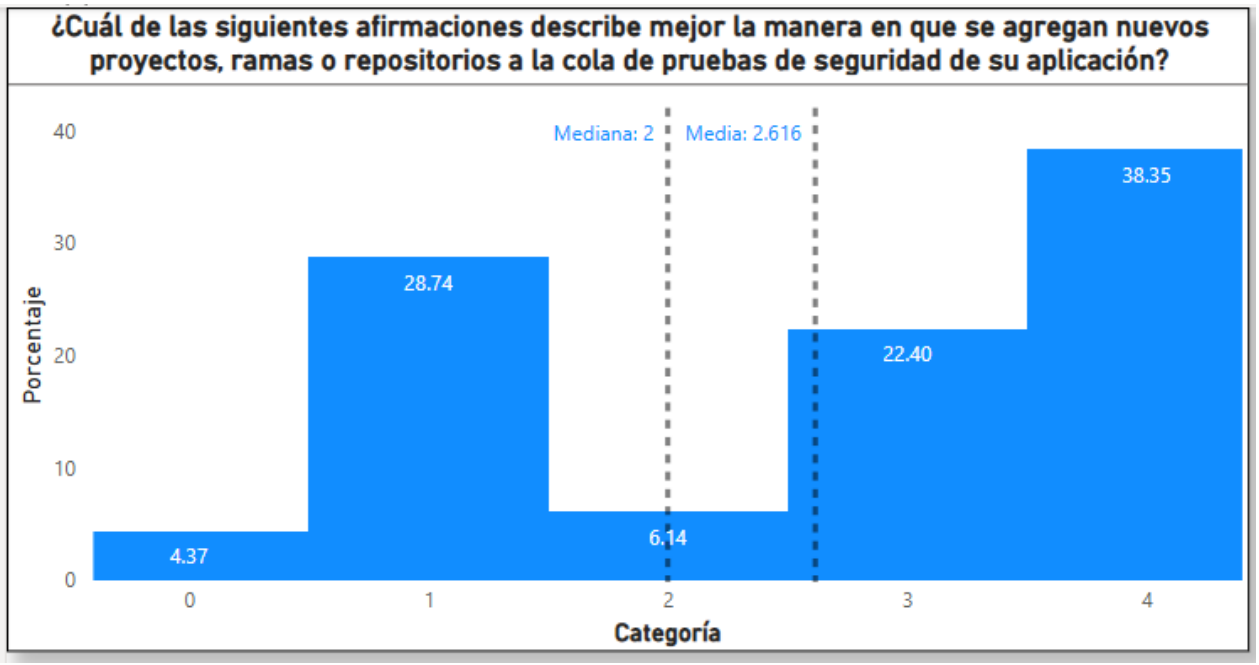


Figura 20. Resultados Pregunta de Cómo se agregan las pruebas de seguridad

Fuente: Elaboración Propia

Con este resultado se está analizando la variable de las pruebas de seguridad y de cómo estas son agregadas en el SDLC. La media ponderada es igual a **2.616** lo que indica que en promedio las respuestas se encuentran entre las categorías 2 y 3 y de manera más cercana a la categoría 3 por lo que las respuestas indican que las pruebas se agregan mayormente de manera automática, aunque hay algunas que todavía se agregan manualmente.

La moda sería la categoría 4, ya que es el valor con mayor porcentaje con un 38.35%, la mediana sería la categoría 2 que es la que se encuentra en medio de las 5 categorías. La desviación estándar es de 1.543 lo que indica que los valores están dispersos en 1.543 unidades con respecto a la media por lo que los datos no se dispersan mucho alrededor de la media.

Análisis de la relación entre el tiempo y las pruebas de seguridad en la implementación de DevSecOps

Para realizar este análisis se seleccionó la pregunta que trata el tema de la relación entre el tiempo de entrega y desarrollo de software y la implementación de pruebas de seguridad indica que en promedio los encuestados consideran que las pruebas ralentizan entre ligera y moderadamente el tiempo de entrega y desarrollo de software, ya que al realizar el cálculo de la media pondera el valor obtenido es 2.59 lo que indica que se encuentra entre la categoría 2 y más cerca de la categoría 3.

Los resultados de esta pregunta indican que si existe una relación entre el tiempo de entrega y desarrollo de software y las pruebas de seguridad que son aplicadas al software siendo la categoría las pruebas ralentizan moderadamente la que más porcentaje de encuestados respondió y la categoría 0 de no certeza que indica que el 5.25 % de los encuestados no pueden evaluar la relación entre las pruebas de seguridad y el desarrollo y entrega de software por lo que no se siente lo suficientemente informados o seguros para emitir una respuesta.

Según las respuestas a esta pregunta los encuestados consideran que si hay un impacto importante y considerable en el tiempo de entrega y desarrollo de software al aplicar pruebas de seguridad en las aplicaciones ya que solo un 14.47%, 5.25% de no pueden evaluar la relación y un 9.22% las pruebas no ralentizan, no conocen o consideran que no hay un impacto significativo.

Tabla 18. Resultados Pregunta Relación pruebas de seguridad y desarrollo/entrega de software

Orden	Categoria	Porcentaje
0	No puedo evaluar la relación con precisión	5.25
1	Las pruebas no ralentizan	9.22
2	Las pruebas ralentizan ligeramente	24.68
3	Las pruebas ralentizan moderadamente	42.81
4	Las pruebas ralentizan gravemente	18.04

Fuente: Elaboración Propia

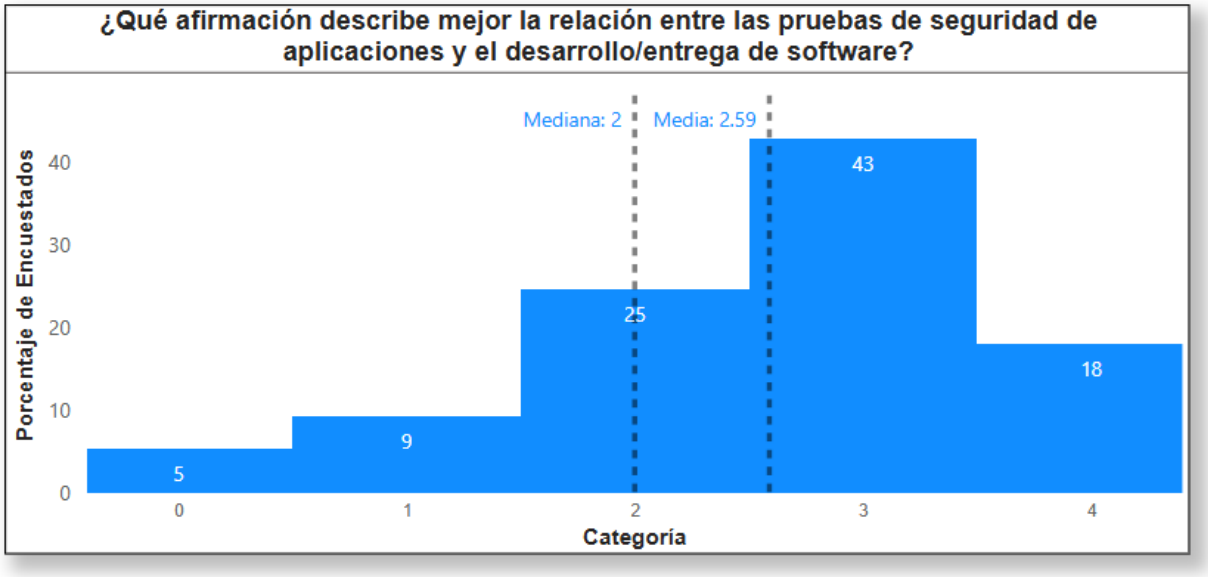


Figura 21. Resultados Pregunta Relación pruebas de seguridad y desarrollo/entrega de software

Fuente: Elaboración Propia

Análisis de la relación entre los costos y el nivel de adopción de DevSecOps

En la siguiente tabla y figura se muestran la relación que existe entre el costo y el nivel de adopción de DevSecOps por parte de las organizaciones, haciendo uso los datos obtenidos de la fuente secundaria que se seleccionó.

Se construyó una matriz de correlación para analizar la relación entre estas 2 variables. El

resultado obtenido fue de -1.00 lo que indica que hay una correlación lineal negativa perfecta. Esto sugiere que, en los datos observados, a mayor nivel de adopción, menores son los costos asociados. Es decir, cuando las organizaciones presentan un alto nivel de adopción, tienden a reducir significativamente sus costos.

Sin embargo, es importante destacar que esta correlación se basa en solo dos observaciones, por lo que no se puede afirmar con certeza que exista una relación estadísticamente válida entre ambas variables. A pesar de ello, la tendencia es evidente en los datos analizados: las organizaciones con un nivel de adopción alto reportaron una reducción superior al 30% en los costos relacionados con la brecha de datos.

Tabla 19. Costos vs Adopción de DevSecOps

Costos vs adopción de DevSecOps	
Categoría	**Costo en millones de USD**
Bajo	5.22
Alto	3.54

Fuente: Elaboración Propia

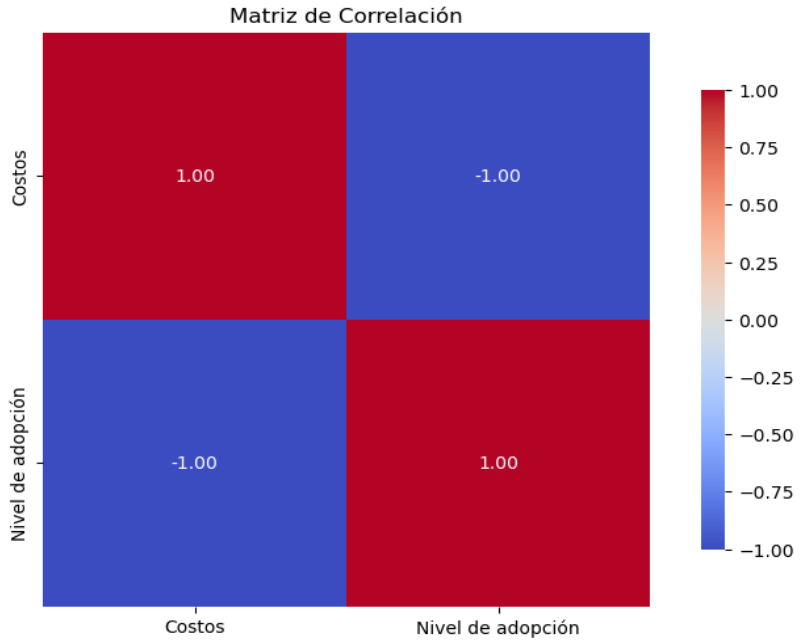


Figura 22 Relación entre Costos y nivel de adopción de DevSecOps.
Fuente: Elaboración Propia

4.1.3 VISUALIZACIÓN DE DATOS

La figura siguiente muestra los criterios que utilizan las organizaciones para determinar cuándo y que pruebas de seguridad de aplicaciones se deben ejecutar, según los resultados de la encuesta el criterio que toman más en cuenta las organizaciones para realizar pruebas de seguridad a las aplicaciones es la **Sensibilidad de la información**, pero hay otros criterios que están muy cerca del porcentaje del primero criterios como mejores prácticas recomendadas por organizaciones de terceros o facilidad de configuración de las pruebas de seguridad.

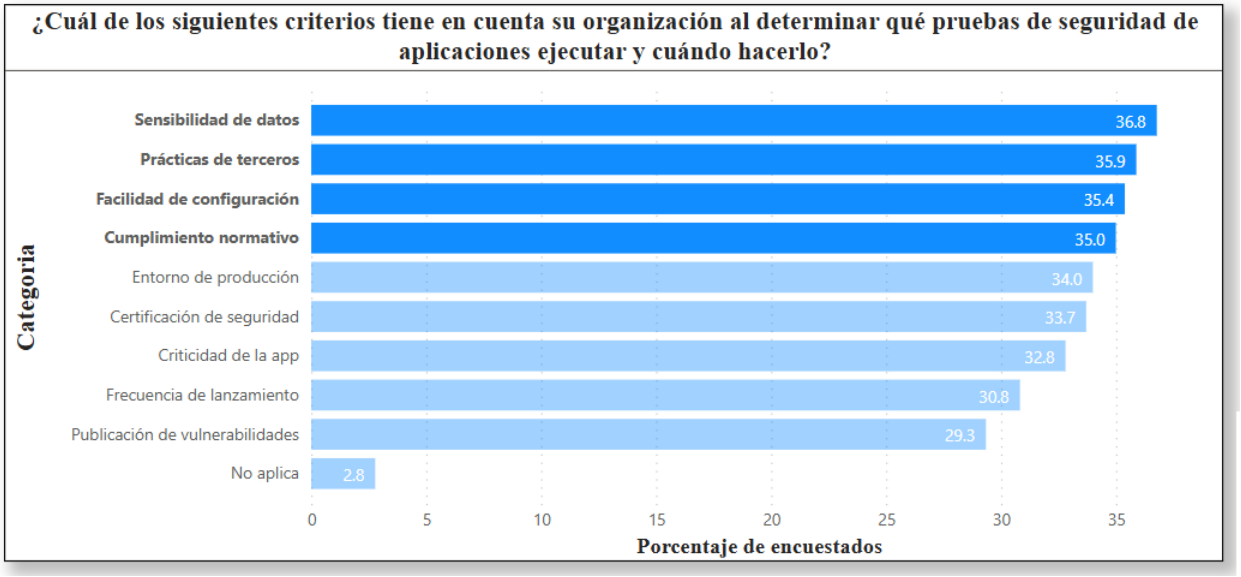


Figura 23. Resultados Pregunta sobre criterios para realizar pruebas de seguridad
Fuente: Elaboración Propia

Al analizar los resultados de esta pregunta se puede observar que los criterios que las organizaciones toman más en cuenta son la información que contienen o va a manejar el software desarrollado para seleccionar que tipos de pruebas de seguridad deben ser aplicadas además toman en cuenta las recomendaciones de empresas de terceros que son expertos en temas de seguridad.

Según la encuesta y como se visualiza en la figura siguiente la mayoría de los encuestados utilizan entre 6 y 15 herramientas y un porcentaje del 5.45 no tienen la visibilidad para estimar la cantidad de herramientas que utiliza la organización, lo que indica que las organizaciones si están haciendo uso de herramientas para garantizar la seguridad en el software que es desarrollado, pero que todavía hay personal que no es consciente de que herramientas de seguridad se utilizan.

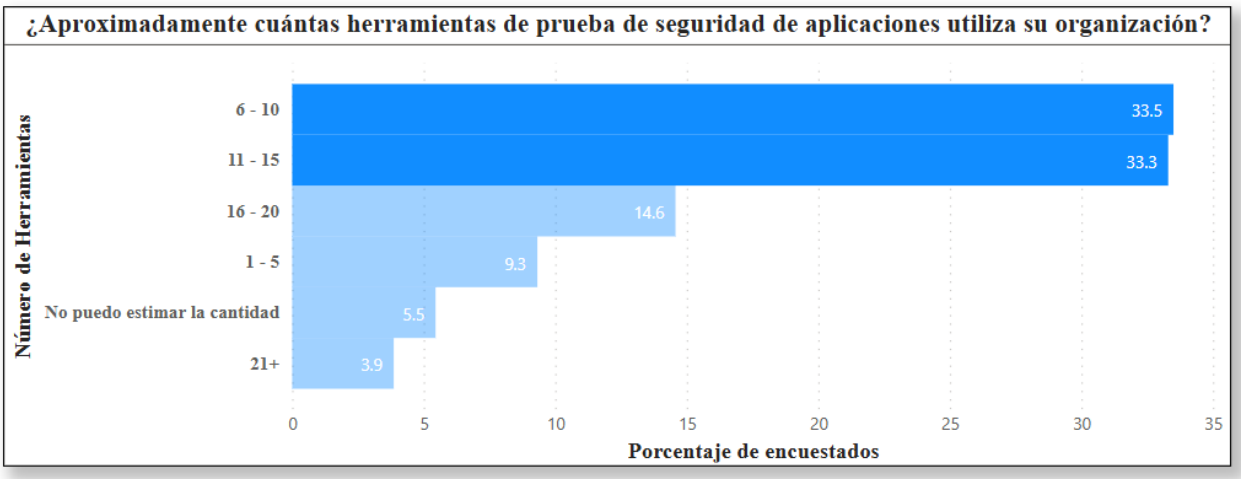


Figura 24. Resultados pregunta sobre cantidad de herramientas utilizadas

Fuente: Elaboración Propia

En la siguiente figura se visualizan los resultados de la pregunta ¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software? y se puede observar que el 42.81% de los encuestados respondieron que **Las pruebas de seguridad de aplicaciones ralentizan moderadamente el desarrollo y la entrega** seguidos del 24.68% que respondieron **Las pruebas de seguridad de aplicaciones ralentizan ligeramente el desarrollo y la entrega**¸ por lo que la mayoría de los encuestados consideran que las pruebas de seguridad en las aplicaciones ralentizan de ligeramente a moderadamente el desarrollo de software y la entrega del mismo.

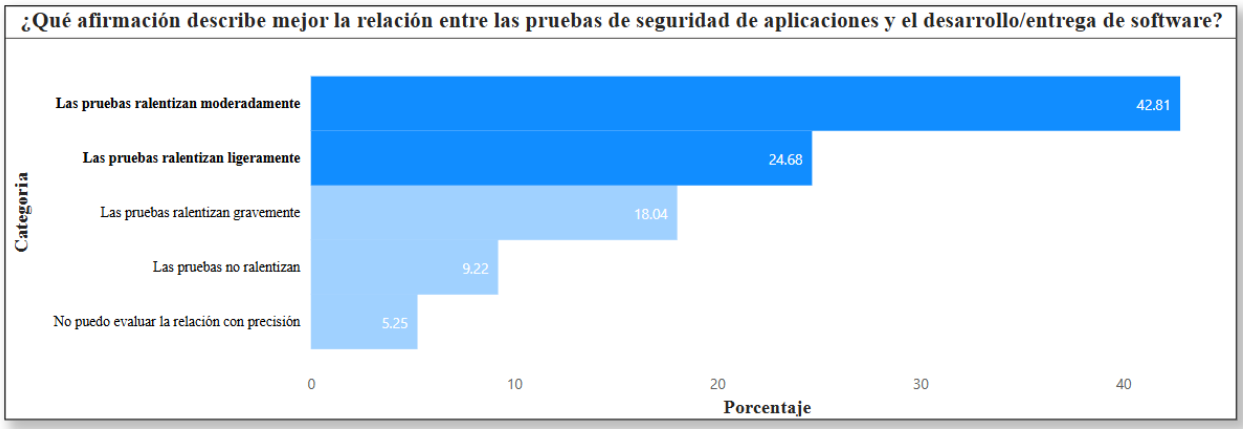


Figura 25. Resultados Pregunta sobre relación entre pruebas de seguridad y tiempo de entrega de software

Fuente: Elaboración Propia

En la pregunta ¿Está seguro del enfoque de su organización hacia la seguridad de las

aplicaciones? podemos observar que el 60% de los encuestados si conocen y están seguros del enfoque de su organización en cuanto la seguridad de las aplicaciones y solo un 13% no está seguro y un 6% no sabe el enfoque, lo que indica que las organizaciones a las que pertenecen los encuestados se preocupan por la seguridad en las aplicaciones y porque los empleados conozcan el enfoque que deben seguir.

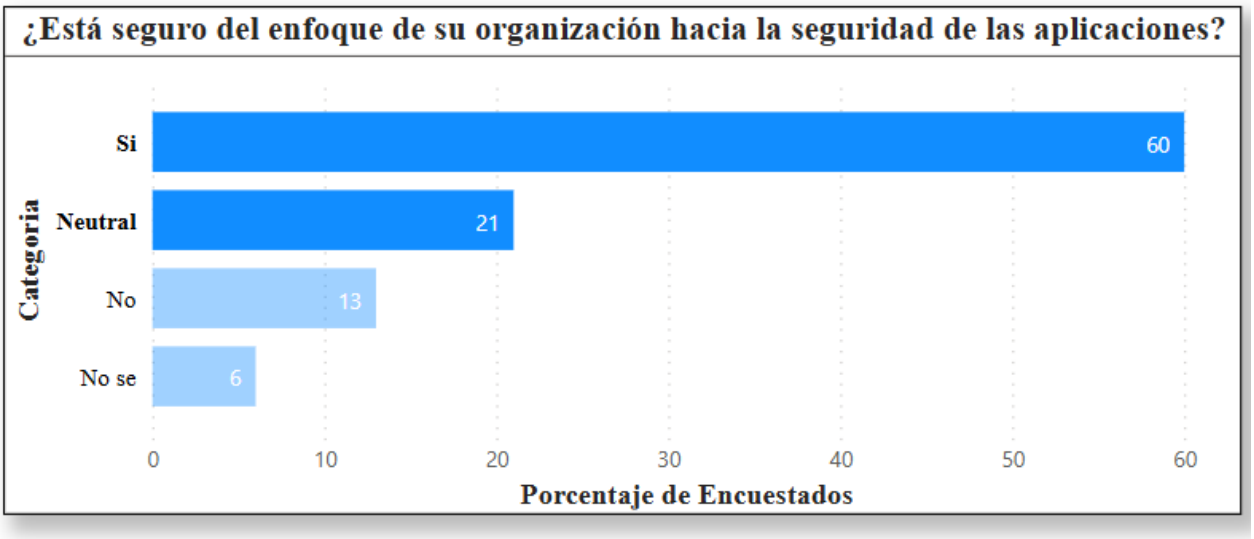


Figura 26. Resultados Pregunta sobre el enfoque de seguridad en la organización
Fuente: Elaboración Propia

4.1.4 CONCLUSIONES DEL EDA

La mayoría de los encuestados respondieron que las organizaciones utilizan más de 6 herramienta para las pruebas de seguridad en las aplicaciones, aunque hay un pequeño porcentaje que desconoce el número de herramientas que se utilizan dentro de la organización. En su mayoría los encuestados conocen el enfoque de la organización hacia la seguridad de las aplicaciones.

Algunos de los criterios que las organizaciones toman más en cuenta para decir que pruebas de seguridad ejecutar son: sensibilidad de los datos, la información que contienen sus sistemas de información que en la mayor parte de las organizaciones es confidencial y delicada. Otro criterio son las mejores prácticas recomendados por terceros que son expertos en temas de seguridad.

La mayor parte de las pruebas se agregan automáticamente, aunque hay algunas que se agregan manualmente esto podría estar relacionado con el impacto que tienen las pruebas de seguridad de las aplicaciones en el tiempo de entrega y desarrollo de software. Con respecto a este

impacto la mayor parte de encuestados indica que las pruebas ralentizan entre modera y ligeramente las pruebas de seguridad.

Existe una clara relación entre los costos relacionados con la brecha de datos y el nivel de adopción de las organizaciones con respecto a DevSecOps donde se observa que el costo reduce considerablemente al tener un nivel alto de adopción.

4.2 INFORME DEL PROCESO DE RECOLECCIÓN DE DATOS

4.2.1 DESCRIPCIÓN DEL PROCESO

Antes de iniciar con la recolección de datos se definieron cuáles serían los criterios de selección para las fuentes, luego de tener los criterios se inició con la búsqueda en bases de datos académicas, sitios web de organizaciones relevantes y en bibliotecas digitales, se hizo una revisión de las fuentes encontradas para validar que cumpla con los criterios de selección definidos, se seleccionaron las fuentes más relevantes y adecuadas para la investigación.

Las fuentes seleccionadas pertenecen a reportes y encuestas realizadas en los años 2023 y 2024 por empresas relacionadas al desarrollo de software y se obtuvieron en las páginas web oficiales de cada una de las empresas se consideraron las 3 fuentes ya que se complementaban entre ellas para poder obtener una visión más clara de la implementación de DevSecOps.

4.2.2 PARTICIPANTES O FUENTES DE INFORMACIÓN

La población está formada por 3 reportes y encuestas que fueron seleccionados como fuentes secundarias. Durante la recolección de datos se seleccionaron estas 3 fuentes porque muestran información actualizada de los años 2023 y 2024, fueron realizadas por empresas relacionados al desarrollo de software y la seguridad en el SDLC.

Los participantes de las encuestas y reportes son personas que pertenecen a organizaciones de diferentes rubros como financiero, comercial, educativo, desarrollo de software, telecomunicaciones, entre otras, las personas desempeñas diferentes roles desde puestos de dirección, desarrolladores de software y personal funciones directamente relacionadas con el desarrollo de software.

Además, el contexto geográfico de las fuentes de información es global incluyendo encuestados de países como Estados Unidos, Canadá, Alemania, Japón, entre otros, esto permite tener una perspectiva global de la implementación de DevSecOps porque los datos también

incluyen empresas de diferentes tamaños desde empresas con menos de 100 empleados hasta empresas de más de 1000 empleados.

4.2.3 INSTRUMENTOS UTILIZADOS

Se utilizaron reportes y encuestas elaborados por empresas relacionados al desarrollo de software y la implementación de seguridad durante todo el ciclo de vida de desarrollo de software. Estos reportes y encuestas son de los años 2023 y 2024 y fueron realizadas a personas de diferentes países alrededor del mundo que pertenecen a empresas de diversos rubros.

Se realizó solo la selección de preguntas que estuvieran relacionadas directamente con las preguntas de investigación y ayudarán a cumplir los objetivos establecidos en la presente investigación

4.2.4 DIFICULTADES ENCONTRADAS

Dificultad de encontrar información en español, la mayor parte de la información sobre el tema de la implementación de DevSecOps en las empresas se encuentra en inglés lo que dificultó un poco la recolección y análisis de los datos encontrados.

Otra dificultad es que no se encontraron datos sobre implementación de DevSecOps en Honduras o países de Centroamérica los datos encontrados son de países como Estados Unidos, Francia, Alemania, India, Japón, Canadá, China, entre otros países, por lo que el análisis se realizó con datos globales.

4.2.5 CONSIDERACIONES ÉTICAS

La presente investigación utiliza únicamente fuentes secundarias, donde se incluye reportes y encuestas que se encontraron en los sitios web de las empresas que las realizaron, para acceder a algunas de ellos fue necesario registrarse para obtener el documento completo. Las fuentes secundarias utilizadas están debidamente citadas en todo el documento y en la bibliografía de la tesis.

En cada una de las fuentes no se mencionan datos personales de los encuestados ni datos de las empresas se mencionan solamente de manera general el rubro, tamaño de la organización, roles de los encuestas y países de origen.

4.3 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS

4.3.1 RESULTADOS CUANTITATIVOS

4.3.1.1 Presentación de datos

La siguiente figura detalla las Tasas de Adopción de diversas prácticas de DevSecOps por parte de los encuestados de los años 2021, 2022 y 2023, dónde se puede observar que las tres prácticas que más han adoptado los encuestados a los largo de estos 3 años son: la automatización de la compilación, la integración continua y las pruebas automatizadas y las que menos adopción han tenido son la ingeniería del caos, la retrospectiva sin culpa y el aprovisionamiento de infraestructura inmutable, lo que indica que estas últimas son las prácticas que menos utilizan los encuestados.

Además, se puede observar que en general las tasas de adopción de las prácticas de seguridad de DevSecOps aumentó más en el año 2022 en comparación con el año 2021 y 2023.

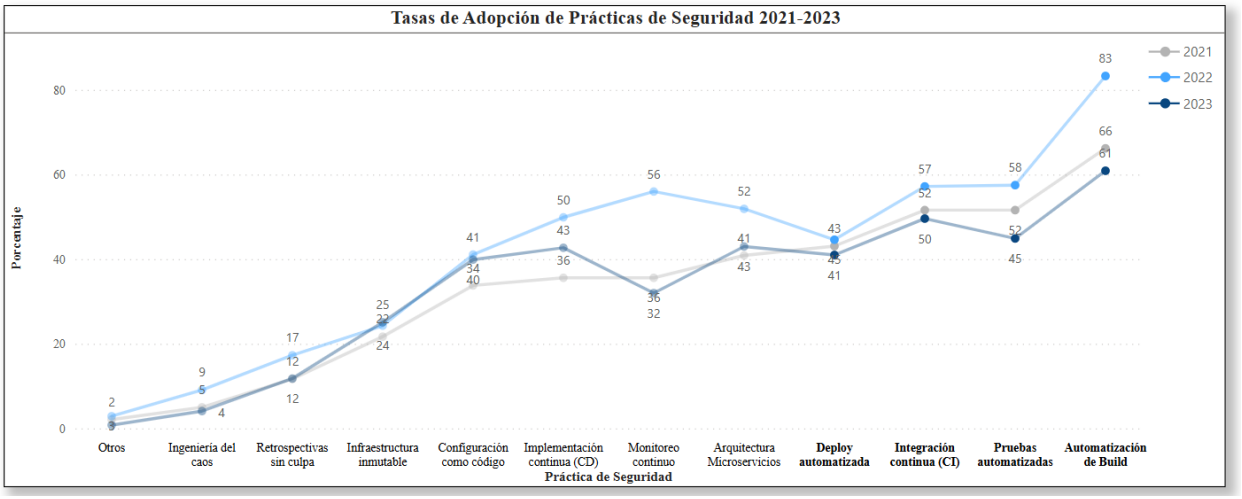


Figura 27. Tasas de adopción de prácticas de DevSecOps
Fuente: Elaboración Propia

La siguiente figura muestra los 10 principales desafíos a los que se han enfrentado las organizaciones cuando deciden implementar DevSecOps a lo largo de los años 2021 al 2023. Muchos de los desafíos están relacionados directamente con el personal como el desafío de los silos organizativos de las tres áreas que son necesarios para implementar DevSecOps, otros desafíos son por falta de personal o personal capacitado con las habilidades en seguridad de aplicaciones y seguridad en la nube.

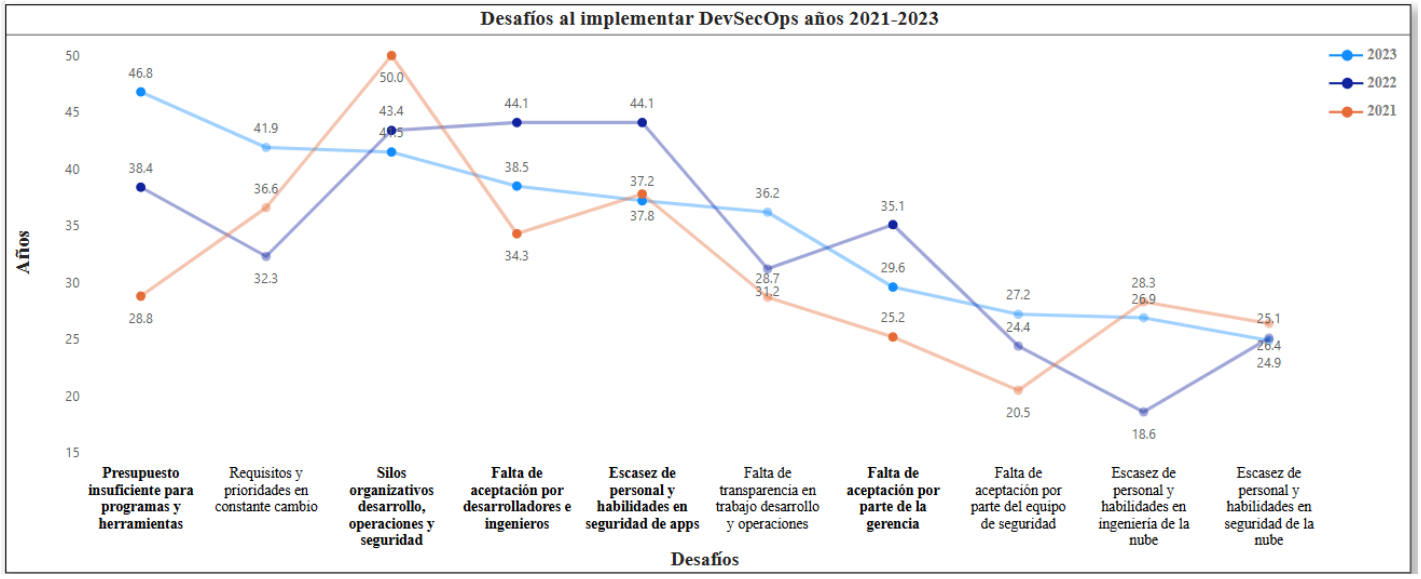


Figura 28. Desafíos al implementar DevSecOps

Fuente: Elaboración Propia

En esta figura también se muestra que algunos desafíos han ido incrementando con los años como el desafío del presupuesto insuficiente para invertir en programas y herramientas de seguridad y los requisitos y prioridades en constante cambio, en cambio otros como los silos organizativos entre las áreas involucradas y escasez de personal con las habilidades en seguridad de aplicaciones han disminuido con el paso de los años, lo que indica que a medida pasa el tiempo hay más personas capacitándose para obtener el conocimiento y habilidades necesarias para implementar efectivamente las prácticas de DevSecOps y con respecto a los silos ha tenido una disminución significativa desde el año 2021 que tenía un 50% al año 2023 donde tiene un 41.5% lo que puede significar que cada vez las áreas involucradas trabajan mejor de forma colaborativa para asegurar que las prácticas de DevSecOps se apliquen correctamente.

4.3.1.2 Descripción de los hallazgos

A lo largo de los años hay muchas prácticas de seguridad que las organizaciones han incrementado su adopción como ser la automatización tanto en la compilación de las aplicaciones como en las pruebas de seguridad que se aplican al software, lo que indica una clara tendencia hacia la automatización de los procesos para mejorar la productividad y eficiencia en el desarrollo de software.

La mayoría de los empleados de las organizaciones encuestadas conocen sobre la postura que se tiene en temas de seguridad de las aplicaciones, lo cual es una gran ventaja ya que conocen

bien el proceso que se debe seguir en todo el SDLC desde que se inicia y finaliza el desarrollo de software y las organizaciones a las que pertenecen las personas encuestadas utilizan en su mayoría más de 6 herramientas para realizar pruebas de seguridad.

En cuanto a temas de costos se observó que hay una clara reducción den las organizaciones que tienen un alto nivel de adopción de DevSecOps, lo que indica que se obtienen beneficios económicos al decidir adoptar DevSecOps. En temas de tiempo la mayoría de los encuestados indicaron que las pruebas ralentizan los tiempos de entrega y desarrollo de software, esto se puede deber a que hay muchas pruebas que se agregan todavía de manera manual.

Las organizaciones se enfrentan a muchos desafíos al implementar DevSecOps, alguno de ellos relacionados directamente con la falta de aceptación de los equipos de desarrollo y de la gerencia, aunque el mayor desafío es el presupuesto insuficiente para programas y herramientas de seguridad.

4.3.1.3 Relación con los objetivos

Con el primer objetivo el análisis de las tasas de adopción de las diferentes prácticas de seguridad a lo largo de los años permite conocer cuáles son las prácticas de DevSecOps son las que más han sido adoptadas y como han cambiado a lo largo de los años.

El segundo objetivo está relacionado con conocer el impacto de la implementación de DevSecOps en factores como el tiempo y el costo, en la pregunta 13 se puede observar la percepción de los encuestados sobre la relación que existe entre el tiempo de entrega del desarrollo de software y las pruebas de seguridad de aplicaciones que sería la implementación de DevSecOps en el SDLC. Además, en el análisis se pudo observar que existe una relación entre los costos y la adopción de prácticas de DevSecOps en las organizaciones donde las que presentan más altos niveles de adopción son las que tienen menos costos relacionados con la información y seguridad de las aplicaciones.

El tercer objetivo está relacionado con la percepción y adopción por parte de los equipos de desarrollo que están involucrados en la implementación de DevSecOps. Las tasas de adopción de las diversas prácticas de DevSecOps han variado con el paso de los años y de igual manera los desafíos a los que se enfrentan las organizaciones al implementar estas prácticas han cambiado con el paso de los años algunas han aumentado y otras han disminuido.

4.3.1.4 Análisis estadístico

En la siguiente tabla se observan las diferentes categorías que describen la relación entre las pruebas de seguridad y el tiempo de entrega y desarrollo de software, estos datos se utilizarán para realizar la prueba de hipótesis.

Para realizar la prueba se dividieron las categorías en 2 grupos, el grupo 1 está conformado por las categorías: las pruebas no ralentizan con 9.22% y no puedo evaluar la relación con precisión con 5.25% haciendo un total de 14.47%, y el grupo 2 por las categorías de ralentizan gravemente con un 18.04%, ralentizan moderadamente con un 42.81% y las pruebas ralentizan ligeramente con 24.68% haciendo un total de 85.53%. Estos 2 grupos representan el grupo 1 las pruebas no ralentizan el tiempo de desarrollo es decir no afecta el tiempo de desarrollo y entrega del software y el grupo 2 el tiempo si se ve afectado por las pruebas de seguridad.

Tabla 20. Resultado Pregunta sobre la relación entre las pruebas de seguridad y el desarrollo entrega de software

¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	
Categoria ▲	Porcentaje
Las pruebas ralentizan gravemente	18.04
Las pruebas no ralentizan	9.22
Las pruebas ralentizan ligeramente	24.68
Las pruebas ralentizan moderadamente	42.81
No puedo evaluar la relación con precisión	5.25
Total	**100.00**

Fuente: Elaboración Propia

Tabla 21. Prueba de hipótesis 1

Variable	Hipótesis Nula (H_0)	Hipótesis Alternativa (H_1)	Valor p	X^2	Conclusión
Tiempo de desarrollo	El tiempo de entrega del desarrollo **no disminuye al implementar DevSecOps a lo largo del SDLC**.	El tiempo de entrega del desarrollo **disminuye al implementar DevSecOps a lo largo del SDLC.**	1.0	0	No Se rechaza H_0.

Fuente: Elaboración Propia

Para realizar la prueba de la segunda hipótesis se utilizarán los datos de la tabla 19 que

indican los costos de filtración de datos que se obtuvieron en el año 2023 y la prueba t con un nivel de significancia de 0.05.

Tabla 22. Comparación de Costos por adopción de DevSecOps

Costos vs adopción de DevSecOps	
Categoría	**Costo en millones de USD**
Bajo nivel de adopción	5.22
Alto nivel de adopción	3.54

Fuente: Elaboración Propia

Tabla 23. Prueba de Hipótesis 2

Variable	Hipótesis Nula (H_0)	Hipótesis Alternativa (H_1)	Valor p	Conclusión
Costos de desarrollo	El costo relacionado con el desarrollo de software, al identificar y mitigar vulnerabilidades desde el inicio del desarrollo, **no disminuye cuando se implementa DevSecOps en el SDLC**	El costo relacionado con el desarrollo de software, al identificar y mitigar vulnerabilidades desde el inicio del desarrollo, **disminuye cuando se implementa DevSecOps en el SDLC**	0.0	Se rechaza H_0. El costo disminuye al adoptar prácticas de DevSecOps.

Fuente: Elaboración Propia

4.4 ANÁLISIS INFERENCIAL Y MODELOS APLICADOS

4.4.1 ANÁLISIS INFERENCIAL

Para realizar el análisis de los datos sobre las tasas de adopción de las diferentes prácticas de DevSecOps a lo largo de los años 2021 al 2023 se decidió utilizar el modelo de Clustering para identificar patrones entre la adopción de las diferentes prácticas y como estas se pueden agrupar.

En la siguiente figura se muestra el modelo aplicado a los datos sobre las tasas de adopción donde se crearon tres clústeres, el clúster 0 representa las prácticas que han tenido mayor variabilidad a lo largo de los años, el clúster 1 son las prácticas de seguridad que han tenido menor tasas de adopción y no han variado con el paso de los años y el clúster 2 representa la práctica de seguridad que tienen una mayor tasa de adopción y se ha mantenido este porcentaje a lo largo de los años.

	Práctica	2021	2022	2023	Cluster
0	Automatización de Build	60.9	83.3	66.2	2
1	Integración continua (CI)	49.6	57.2	51.6	0
2	Pruebas automatizadas	44.9	57.5	51.6	0
3	Arquitectura Microservicios	43.0	51.9	40.9	0
4	Implementación continua (CD)	42.7	49.9	35.6	0
5	Deploy automatizada	41.0	44.6	43.1	0
6	Configuración como código	39.9	41.1	33.8	0
7	Monitoreo continuo	32.0	56.0	35.6	0
8	Infraestructura inmutable	25.1	24.3	21.7	1
9	Retrospectivas sin culpa	11.8	17.3	11.7	1
10	Ingeniería del caos	4.1	9.1	5.0	1
11	Otros	0.8	2.9	2.1	1

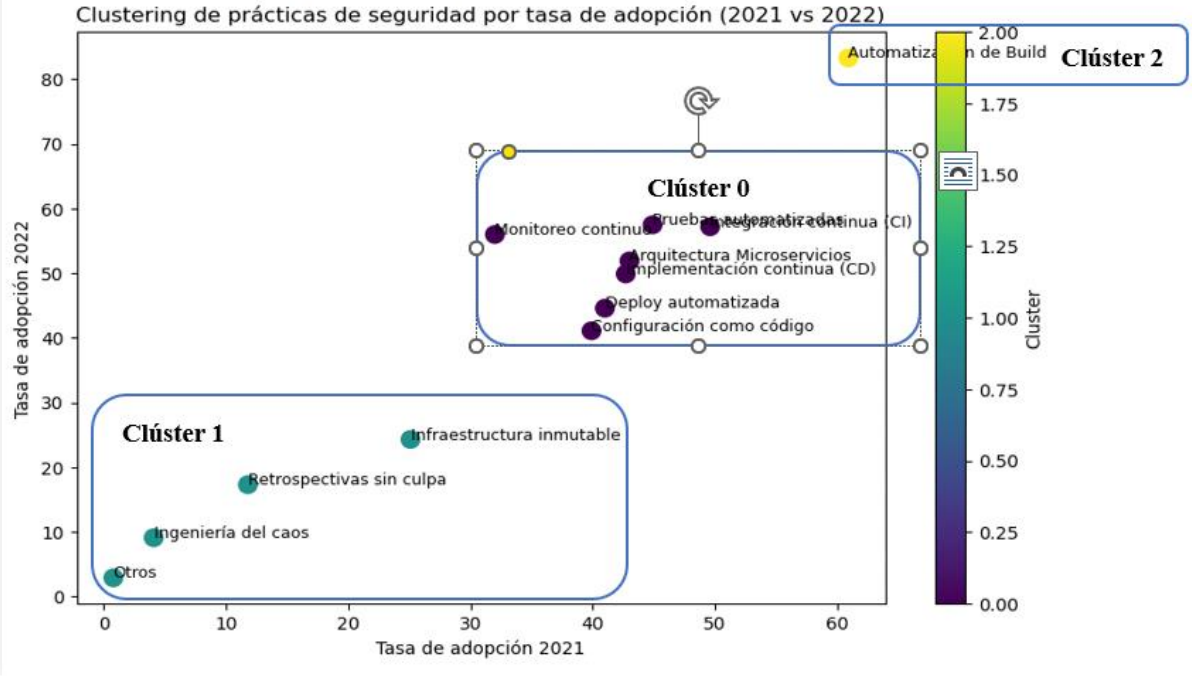


Figura 29. Clustering Tasas de Adopción de Prácticas de Seguridad 2021-2023
Fuente: Elaboración Propia

En la figura se muestra la comparación entre las tasas de adopción de los años 2021 y 2022 en el eje x representa el porcentaje de adopción de cada práctica en el año 2021 y el eje y representa el porcentaje de adopción del año 2022.

Para realizar el análisis de los desafíos también se decidió implementar el modelo de Clustering para agrupar los desafíos a lo largo de los años 2021 al 2023. En la siguiente figura se muestra los clústeres creados y el gráfico representativo de los datos.

Se crearon tres clústeres, el clúster 0 representa los desafíos que se han mantenido en los primeros puestos a lo largo de los años, el clúster 1 son los desafíos que han tenido mayor variabilidad a lo largo de los años y el clúster 2 son los desafíos que han tenido menor variabilidad y en los puestos más bajos.

```
Desafíos agrupados por clúster:
Cluster 0:
Presupuesto insuficiente para programas y herramientas
Requisitos y prioridades en constante cambio
Falta de transparencia en trabajo desarrollo y operaciones
Falta de aceptación por parte de la gerencia

Cluster 1:
Silos organizativos desarrollo, operaciones y seguridad
Falta de aceptación por desarrolladores e ingenieros
Escasez de personal y habilidades en seguridad de apps

Cluster 2:
Falta de aceptación por parte del equipo de seguridad
Escasez de personal y habilidades en ingeniería de la nube
Escasez de personal y habilidades en seguridad de la nube
```

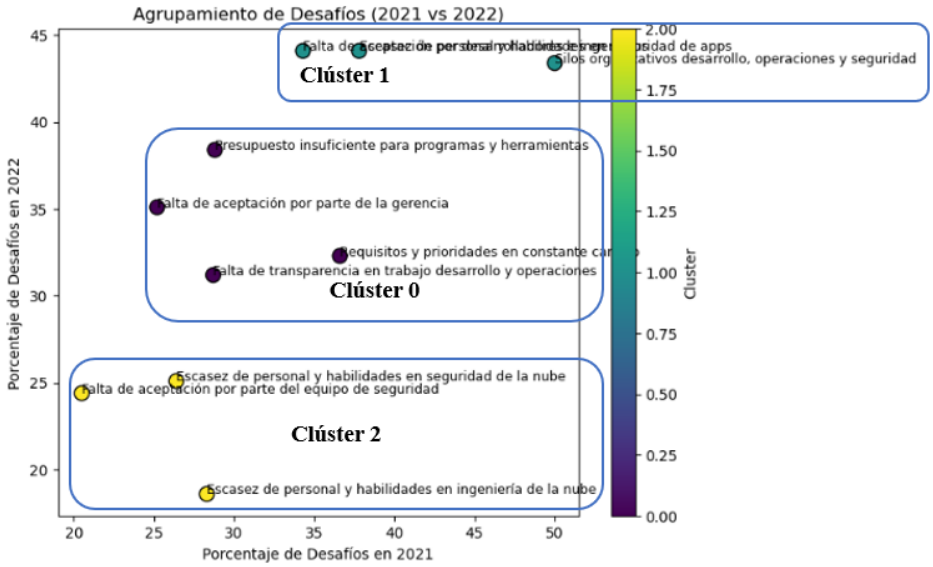


Figura 30. Clustering de Desafíos
Fuente: Elaboración Propia

Para el análisis de los costos y tiempos se decidió realizar modelos de regresión lineal.

En la siguiente figura se muestra la regresión lineal de la relación entre los tiempos de entrega y desarrollo de software y las pruebas de seguridad, donde se observa que el coeficiente es de 5.917

```
Resultados del modelo de percepción:
                                Categoria  Porcentaje  Categoria_encoded  \
0          Las pruebas ralentizan gravemente       18.04                  4
1       Las pruebas ralentizan moderadamente       42.81                  3
2         Las pruebas ralentizan ligeramente       24.68                  2
3                  Las pruebas no ralentizan        9.22                  1
4  No puedo evaluar la relación con precisión        5.25                  0

   Prediccion_Percepcion
0                 31.834
1                 25.917
2                 20.000
3                 14.083
4                  8.166

Coeficientes del modelo de percepción:
Coeficiente: [5.917]
Intercepto: 8.165999999999997
```

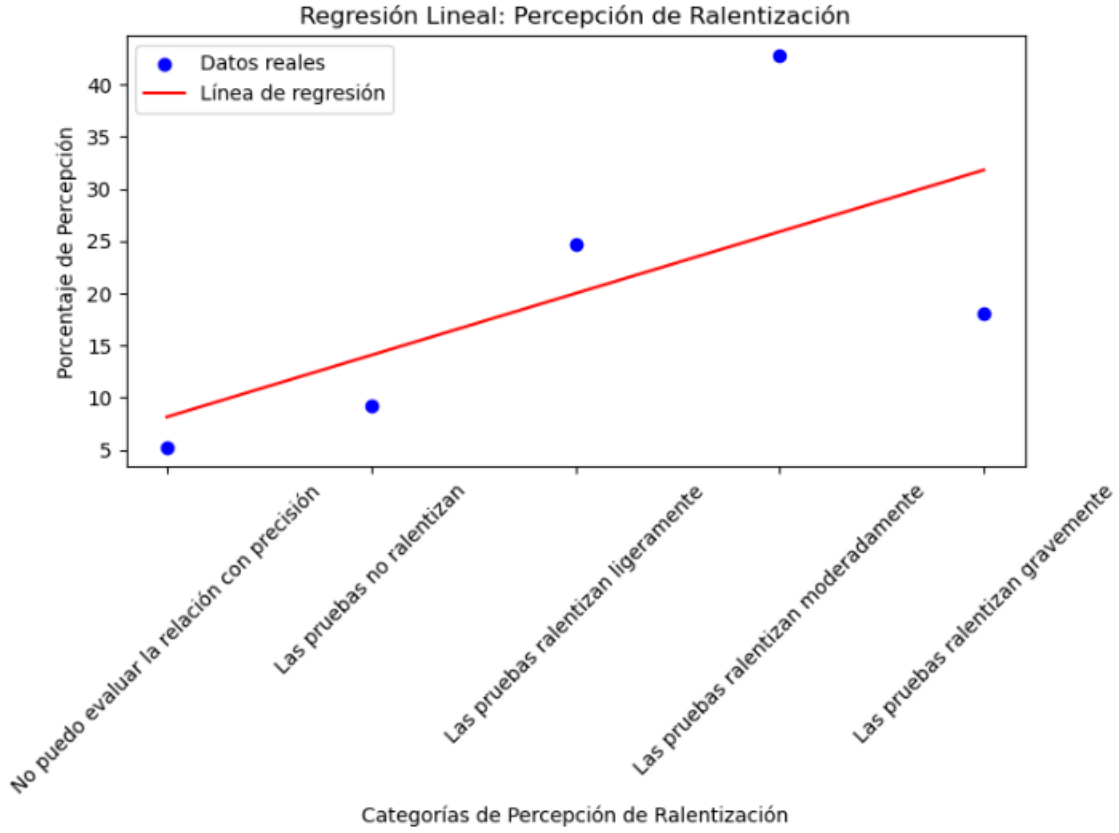


Figura 31. Regresión Lineal Relación tiempos y pruebas de seguridad
Fuente: Elaboración Propia

En la siguiente figura se muestra la regresión lineal de la relación entre los costos y el nivel de adopción de DevSecOps, donde se observa que el coeficiente es de -1.68 lo que indica que hay una relación donde si el nivel de adopción aumenta los costos disminuyen algo que es muy claro porque las organizaciones con un alto nivel lograron ahorrar y reducir considerablemente los costos relacionados con la brecha de datos en comparación con las organizaciones que tienen un

bajo nivel de adopc

```
Resultados del modelo de costo:
  Categoria  Costo  Categoria_encoded  Prediccion_Costo
0      Bajo   5.22                  0              5.22
1      Alto   3.54                  1              3.54

Coeficientes del modelo de costo:
Coeficiente: [-1.68]
Intercepto: 5.219999999999999
```

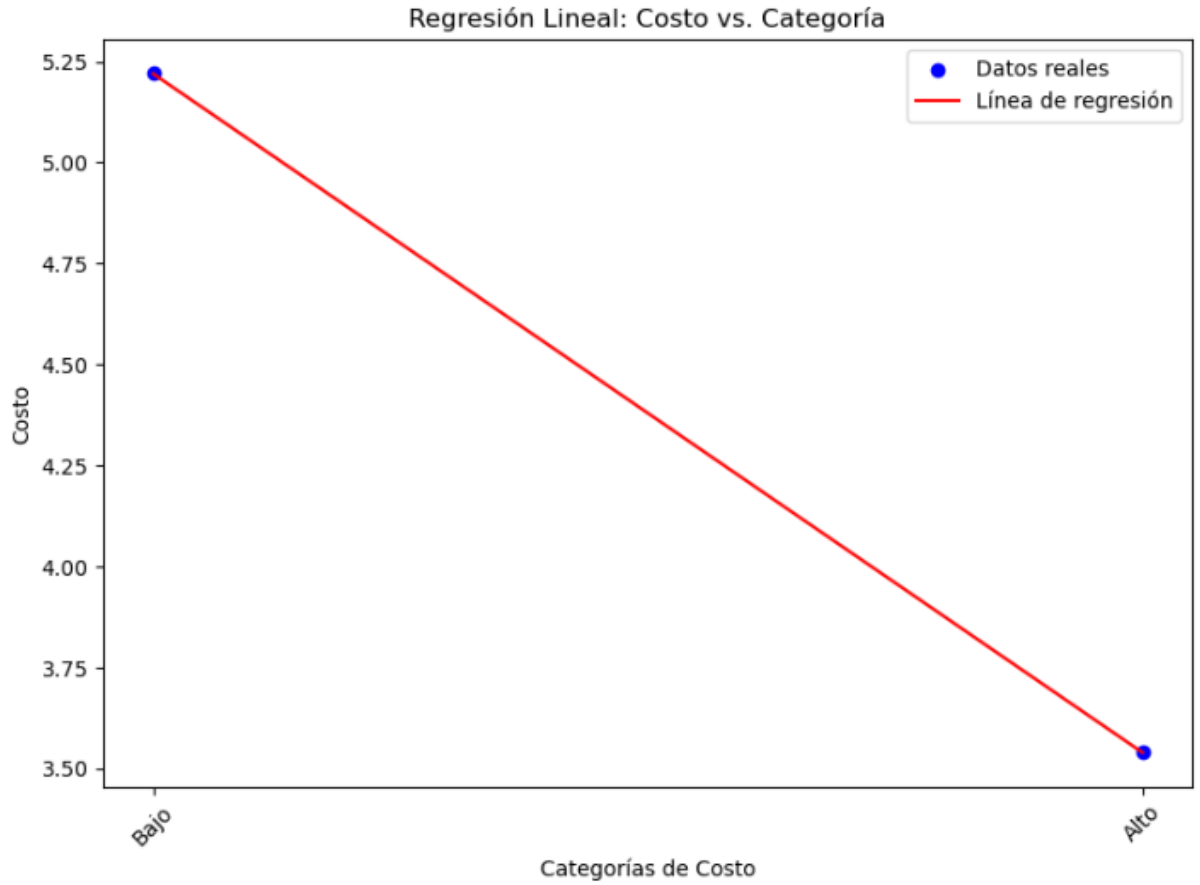


Figura 32. Regresión lineal Costos vs Nivel de adopción DevSecOps
Fuente: Elaboración Propia

4.4.2 DISCUSIÓN DE HALLAZGOS

Se identificó una clara relación entre las pruebas de seguridad y el proceso de entrega y desarrollo de software. La mayoría de los encuestados concuerdan que las pruebas de seguridad tienen un impacto importante, ralentizando el proceso en una medida que varía entre ligera y moderada, además que según los encuestados hay muchas pruebas que son realizadas de manera manual lo que puede ocasionar que el tiempo de entrega y desarrollo de software se ralentice

considerablemente.

En 2023, se observó una disminución considerable en los costos relacionados con la filtración de datos y otros incidentes de seguridad al adoptar prácticas de DevSecOps, ya que al implementar prácticas de seguridad en cada fase del ciclo de vida de desarrollo de software, las organizaciones pueden detectar y resolver vulnerabilidades mucho antes de que lleguen a producción, lo que reduce considerablemente la posibilidades de ataques cibernéticos, robos y filtraciones de datos, de igual manera minimiza los daños financieros y reputacionales derivados de posibles incidentes.

4.4.3 LIMITACIONES

Una de las limitaciones encontradas en este análisis fue la forma en que se presentaron las respuestas a las preguntas. En particular, solo se tuvo acceso a datos categóricos que reflejan porcentajes de respuestas, esto significa que, aunque se dispone de información sobre las respuestas en estas categorías, no se cuenta con un acceso completo a todos los datos relevantes. En particular, no se tiene información sobre la relación entre las diferentes preguntas, lo que limita la capacidad de realizar un análisis más profundo y exhaustivo.

Para realizar el análisis de los datos se decidió utilizar toda la población como muestra y seleccionar las preguntas que más se adaptaban y ayudaban a cumplir con los objetivos planteados de la presente investigación.

Otra de las limitaciones es que no se encontró información de la implementación de DevSecOps en Honduras ni la región Latinoamericana por lo que se decidió trabajar con los datos de reportes y encuestas donde participaron organizaciones de diferentes países a nivel mundial.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

1.1 CONCLUSIONES

1. Entre las prácticas de seguridad que más han adoptado las organizaciones a lo largo de los años 2021 al 2023 son relacionadas con las pruebas automatizadas lo que indica una tendencia hacia la automatización para mejorar la eficiencia de las pruebas de seguridad y hacia un enfoque más preventivo y proactivo.

   Las organizaciones han adoptado menos prácticas como la ingeniería del caos y la perspectiva sin culpa, aunque estas últimas podrían fortalecer la resiliencia y la capacidad de recuperación ante fallos. Más del 60% de las organizaciones utilizan entre 6 y 15 herramientas para realizar pruebas de seguridad, lo que refleja el esfuerzo por asegurar la protección a través de diversas soluciones tecnológicas.

   Las organizaciones seleccionan que pruebas de seguridad ejecutar en las aplicaciones basados en diferentes criterios entre los que más toman en cuenta son: la sensibilidad de la información, las mejores prácticas recomendados por organizaciones de terceros que son expertos en temas de seguridad y la facilidad en la configuración y ejecución de las pruebas.

2. .Las organizaciones con un alto nivel de adopción de DevSecOps han experimentado una disminución de más del 30 % en los costos, con un valor promedio de 3.54 millones de dólares, en comparación con aquellas con adopción baja, que reportaron un promedio de 5.22 millones de dólares. Esta diferencia fue estadísticamente significativa al realizar una prueba t de diferencia de medias, lo que permitió concluir que el nivel de adopción alto está asociado a menores costos operativos relacionados con la brecha de datos.

   La relación entre las pruebas de seguridad y el tiempo de entrega es un punto clave: muchos encuestados mencionan que las pruebas de seguridad ralentizan moderadamente el desarrollo, mientras que un porcentaje importante considera que estas pruebas ralentizan gravemente el proceso. Esto puede ser resultado de pruebas manuales que aún se realizan en algunas organizaciones. Mediante una prueba de chi-cuadrado se concluyó que el tiempo no disminuye al implementar pruebas de

seguridad por lo que las pruebas tienen un grado de impacto en los tiempos de entrega de desarrollo. En particular, las pruebas manuales tienden a estar asociadas con mayores retrasos en el ciclo de desarrollo.

A pesar de estos desafíos, se observa una oportunidad importante: la adopción de herramientas automatizadas puede reducir estos tiempos, permitiendo mantener altos estándares de seguridad sin comprometer la agilidad del proceso. Esto refuerza el valor estratégico de implementar DevSecOps de forma integral y automatizada.

3. En su mayoría, los encuestados conocen el enfoque de su organización en cuanto al tema de seguridad de las organizaciones, lo que indica que las organizaciones se interesan que su personal este informado sobre la seguridad que se utiliza en las aplicaciones. A lo largo de los años han existido cambios en la adopción de las diferentes prácticas de seguridad de DevSecOps siendo el año 2022 donde hubo un aumento en la adopción de prácticas de seguridad como monitoreo e implementación continuos, en cambio en el año 2023 las tasas de adopción de algunas prácticas de seguridad se han mantenido y otras han disminuido.

   Algunos de los desafíos que las organizaciones han encontrado al adoptar DevSecOps y que involucran al personal son presupuesto insuficiente para programas y herramientas de seguridad, silos organizativos de las diferentes áreas que deben estar involucradas como son el área de desarrollo, operaciones y seguridad, lo cual es un obstáculo sino se aborda a tiempo para la implementación eficaz de DevSecOps, otro desafío importante es la falta de aceptación por parte de desarrolladores e ingenieros de software e incluso por parte de la gerencia y un desafío que se puede mejorar mediante la capacitación y mejora continua es la escasez de personal con habilidades necesarios para implementar seguridad en las aplicaciones.

1.2 RECOMENDACIONES

1. Las organizaciones deben priorizar la inversión en la automatización de pruebas de seguridad, especialmente en áreas que en la actualidad dependen de procesos manuales. Esto puede incluir la implementación de herramientas de automatización de pruebas en todas las fases del ciclo de vida del software, para ello es necesario

implementar herramientas que faciliten la automatización como por ejemplo SonarQube una herramienta open source que permite el análisis de código estático de aplicaciones en busca de vulnerabilidades y es capaz de realizar inspecciones automáticas.

Se recomienda crear procesos iterativos de evaluación y ajuste de las herramientas de automatización y de seguridad de las aplicaciones, buscando siempre mejorar su cobertura y eficacia a medida que evoluciona la infraestructura tecnológica de la organización.

2. Las organizaciones deben acelerar la adopción de prácticas de DevSecOps desde las primeras etapas del desarrollo, ya que, al integrar la seguridad desde el inicio del ciclo de vida del software, las organizaciones pueden reducir significativamente los costos asociados con las brechas de datos y evitar correcciones costosas en etapas posteriores del desarrollo.

   Es recomendable que se establezcan métricas para medir la velocidad de entrega del desarrollo de software al implementar prácticas de DevSecOps y realizar un seguimiento continuo de los costos relacionados con las brechas de datos y el tiempo de entrega del desarrollo, evaluando periódicamente la efectividad de las herramientas y prácticas implementadas y si es necesario ajustar las herramientas automatizadas de acuerdo con los resultados ayudará a reducir los retrasos en el proceso de desarrollo.

   Se recomienda realizar un seguimiento continuo de los costos relacionados con las brechas de datos y el tiempo de entrega del desarrollo, evaluando periódicamente la efectividad de las herramientas y prácticas implementadas. Ajustar las herramientas automatizadas de acuerdo con los resultados ayudará a reducir los retrasos en el proceso de desarrollo.

3. Para superar barreras como la falta de aceptación, la escasez de personal capacitado y los silos organizativos, las organizaciones deben crear programas de capacitación y concientización específicos para desarrolladores, operaciones y equipos de seguridad y promover una mayor colaboración interdepartamental mediante

herramientas que integren los equipos de manera más efectiva. Los programas de capacitación deben ser relacionados con temas de seguridad en las aplicaciones y deben tener como objetivo fomentar una cultura de seguridad y colaboración entre los equipos que harán uso de la metodología de DevSecOps.

Además, establecer métricas claras para medir la efectividad de la capacitación y colaboración interdepartamental, y revisar periódicamente las necesidades de recursos y habilidades a medida que la tecnología y las amenazas evolucionan.

CAPÍTULO VI. APLICABILIDAD

El sector financiero ha mostrado una creciente digitalización de sus productos y servicios lo cual ha promovido la creación de nuevas aplicaciones o mejora de las herramientas estos a su vez impulsa la necesidad de fortalecer la seguridad en el desarrollo de software, dado que las amenazas cibernéticas y los requisitos regulatorios son cada vez más exigentes. La implementación de DevSecOps en el área de desarrollo de una empresa del sector financiero representa un enfoque innovador que permite integrar la seguridad desde las primeras fases del ciclo de vida del software, garantizando aplicaciones confiables, resistentes a vulnerabilidades y alineadas con normativas como PCI-DSS e ISO 27001.

Este capítulo aborda la aplicabilidad de la propuesta de implementación de DevSecOps en el área de desarrollo del sector financiero, proporcionando un marco detallado para su ejecución. En primer lugar, se presenta la justificación de la propuesta, destacando la necesidad de adoptar este enfoque para fortalecer la seguridad de las aplicaciones financieras, se define el alcance de la propuesta, estableciendo objetivos y áreas específicas dentro de la empresa que serán impactadas por la implementación de DevSecOps. Posteriormente, se detallan la descripción y desarrollo de la propuesta, donde se describen las herramientas y procesos que serán implementados.

Además, en este capítulo se describen las medidas de control para supervisar y evaluar la efectividad de la implementación, se presenta un cronograma de implementación y presupuesto y finalmente se analiza la concordancia de los segmentos de la tesis con la propuesta.

6.1 IMPLEMENTACIÓN DE DEVSECOPS EN EL ÁREA DE DESARROLLO DE UNA EMPRESA DEL SECTOR FINANCIERO

La presente propuesta resalta la importancia de integrar DevSecOps en el área de desarrollo de una empresa del sector financiero. La combinación de Dev (Development - Desarrollo), Sec (Security - Seguridad) y Ops (Operations - Operaciones) es fundamental para garantizar que la seguridad se incorpore desde el inicio en cada fase del ciclo de vida del software y que las aplicaciones sean más eficientes, resilientes y estén alineadas a los estándares regulatorios del sector financiero, Este enfoque no solo fortalece la protección contra amenazas cibernéticas sino que también permite optimizar los procesos de desarrollo, pruebas y despliegue de software, asegurando la entrega de software confiable y seguro.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La creciente amenaza de ciberataques y la necesidad de garantizar la seguridad en las aplicaciones desarrolladas en el sector financiero hacen imprescindible la implementación de un enfoque robusto que integra la seguridad en todas las fases del ciclo de vida de desarrollo de software.

La falta de medidas de seguridad adecuadas puede derivar en incidentes de gran magnitud, desde brechas de datos hasta daños a la reputación de la empresa. Según el informe Cost of a Data Breach 2023 de IBM, el costo promedio de una brecha de datos es de 4.45 millones de dólares. (IBM Security, 2023)

La implementación de DevSecOps en el área de desarrollo de una empresa del sector financiero es fundamental para garantizar la seguridad, la eficiencia y la agilidad en el ciclo de vida de desarrollo de software. En un sector donde la protección de datos sensibles, y la conformidad con regulaciones son críticas, integrar prácticas de seguridad desde las primeras etapas del desarrollo permite:

Protección de datos sensibles: En el sector financiero se manejan muchos datos sensibles sobre números de cuenta, historial de transacciones, datos personales, la cuál es extremadamente valiosa y debe ser protegida adecuadamente. DevSecOps permite implementar prácticas de seguridad en el ciclo de vida de desarrollo de software, asegurando que se realicen pruebas de seguridad adecuadas para proteger estos datos sensibles. Un estudio de SANS Institute indica que el 70% de las organizaciones que realizan pruebas de seguridad en el ciclo de vida de desarrollo de software reportan menor vulnerabilidades. (SANS Institute, 2024)

También, la sensibilidad de los datos es el criterio que se encuentra en la 1ra posición de la lista de los criterios que toman en cuenta las organizaciones para determinar que pruebas de seguridad ejecutar. (Allen et al., 2023)

Mitigar riesgos: Al incorporar seguridad en cada fase de desarrollo implementado DevSecOps, se pueden reducir las vulnerabilidades y se minimizan los riesgos de brechas de seguridad. Según el informe de Cybersecurity & Infrastructure Security Agency (CISA), las empresas que adoptan un enfoque proactivo en ciberseguridad pueden reducir el riesgo de ataques en un 70%. (CISA, 2024)

Cumplimiento Normativo: Las empresas financieras están sujetas a estrictas regulaciones y normativas. DevSecOps ayuda a asegurar que las aplicaciones cumplan con los estándares de seguridad y privacidad. Esto ayuda a minimizar el riesgo de sanciones y a mejorar la reputación de la empresa al demostrar compromiso con la seguridad. Además, este criterio, según los datos de la investigación, se encuentra en 4to lugar en la lista de criterios que toman en cuenta las organizaciones para determinar que pruebas de seguridad ejecutar.

Mejora de la colaboración: DevSecOps fomentar una cultura de colaboración entre los equipos de desarrollo, seguridad y operaciones, lo que puede resultar en un mayor eficiencia y respuesta más rápida ante las amenazas.

Ahorro de costos: Según datos utilizados en la investigación implementar DevSecOps es uno de los aspectos que genera mayor ahorro de costos relacionados con la brecha de datos, las organizaciones que poseen un alto nivel de adopción generan menos costos en comparación con las empresas que tienen un bajo nivel de adopción o no tienen implementado DevSecOps.

Según los datos utilizados en esta investigación las empresas que tienen un alto nivel de adopción de DevSecOps lograron un ahorro considerable en los costos por brechas de datos. Según el informe Cost of a Data Breach 2023 de IBM las empresas que adoptaron DevSecOps lograron ahorrar más de 30% en los costos relacionados con la brecha de datos.

6.3 ALCANCE DE LA PROPUESTA

Esta propuesta incluye diversos aspectos que buscan mejorar la seguridad en el desarrollo de software, centrándose en áreas claves como capacitación sobre la seguridad de las aplicaciones, reducción costos derivados de posibles brechas de datos y fomentar una cultura organizaciones centrada en la seguridad.

Objetivos

- Mejorar la seguridad en las aplicaciones y garantizar que cumplan con las normativas y regulaciones de seguridad del sector financiero, al integrar de manera temprana y continua herramientas y prácticas de DevSecOps en el ciclo de vida de desarrollo de software, asegurando que la seguridad se convierta en una pieza fundamental desde el inicio permitiendo un desarrollo de software más seguro y

confiable.

- Ahorrar costos relacionados con la brecha de datos, incluyendo los costos operativos por la brecha de datos, costos por daño a la reputación y los costos asociados al incumplimiento de las normativas, al integrar DevSecOps se podrán identificar de manera temprana las vulnerabilidades lo que reducirá el riesgo de consecuencias económicas.
- Optimizar la identificación y mitigación de vulnerabilidades mediante la automatización de pruebas de seguridad y el análisis continuo de código, esto permitirá responder de manera rápida y eficiente ante cualquier amenaza, garantizando la protección de datos sensibles y reduciendo los tiempos de reacción antes incidentes de seguridad.
- Promover programas de capacitación para brindar conocimientos sobre uso de herramientas de seguridad y mejores prácticas, programas que promuevan la adopción de una cultura de seguridad, colaboración entre áreas claves para implementar DevSecOps y eliminar silos organizativos.

6.4 DESCRIPCIÓN Y DESARROLLO

6.4.1 DESCRIPCIÓN

La implementación de DevSecOps en el área de desarrollo de una empresa financiera requiere una transformación cultural y tecnológica entre los equipos de Desarrollo, Seguridad y Operaciones para garantizar que el software cumpla con los estándares de protección y normativas regulatorias. Al implementar DevSecOps se busca tener un modelo preventivo que permita detectar y mitigar vulnerabilidades desde el inicio del desarrollo.

Esta propuesta incluye realizar una evaluación del estado actual, planificar la ruta a seguir para la adopción de DevSecOps, implementar programación de capacitación que fomenten la cultura de seguridad, la colaboración entre los equipos y brinden conocimientos sobre las prácticas y herramientas de seguridad que se aplicará al software, la integración de prácticas de seguridad, realizar pruebas de seguridad y validación del software antes y durante su despliegue a producción.

Además, que se realicen monitoreos, pruebas y escaneos constantes para identificar y mitigar vulnerabilidades que podrían provocar incidentes o posibles ciberataques que pongan en

riesgo la seguridad de los datos sensibles que se almacenan en las aplicaciones.

6.4.2 DESARROLLO

Para garantizar una implementación efectiva de DevSecOps, es necesario desarrollar alguno elementos clave que son fundamentales durante el proceso de adopción de DevSecOps, dónde se requiere de un enfoque estructurado que abarque desde la evaluación inicial hasta el monitoreo continuo de las aplicaciones en producción.

El desarrollo de esta propuesta se basa en una serie de actividades estratégicas que permitirán fortalecer la seguridad en cada fase del ciclo de vida del software. A continuación, se detallan las actividades claves que se llevarán a cabo:

Evaluación y diagnóstico en temas de seguridad del software

Antes de implementar DevSecOps, es fundamental realizar un análisis del estado actual de las prácticas de seguridad en el desarrollo de software dentro de la organización. Esta evaluación incluirá:

- Análisis de riesgos específicos del sector financiero como protección de datos sensibles, cumplimiento normativo (PCI-DSS, ISO 27001) y amenazas internas y externas.
- Identificación de herramientas de seguridad existentes y su integración con DevSecOps.
- Evaluar el nivel de madurez que tienen los procesos de desarrollo y seguridad para determinar si las practicas actuales cumplen con los estándares requeridos.

Esta evaluación y diagnóstico permitirá diseñar una estrategia alineada con las necesidades y regulaciones del sector financiero y de esta manera asegurar una implementación efectiva de DevSecOps.

Entregable clave para esta actividad:

- Informe de resultados de la evaluación de riesgos y seguridad del software.

Planificación

En base a los resultados del diagnóstico y evaluación se desarrollará un plan de acción para

la adopción gradual de DevSecOps en el área de desarrollo. Esta planificación incluirá los siguientes aspectos:

- Priorización de la adopción de herramientas de seguridad en función de los riesgos más críticos identificados.
- Definición de objetivos, tiempos de entrega y responsables claros para cada fase del proceso.
- Integración de DevSecOps en el ciclo de vida de desarrollo de software (SDLC), asegurando que la seguridad esté presente desde la planificación hasta la producción.
- Estrategia de cumplimiento regulatorio para garantizar que la implementación de DevSecOps cumpla con las normativas financieras aplicables.

  Entregables claves:

  - Plan de implementación de DevSecOps
  - Informe de estrategia para cumplimiento normativo
  - Cronograma y presupuesto de la implementación

Programas de Capacitación del Personal

Los programas de capacitación al personal son clave para la implementación de DevSecOps en la organización. Se implementarán programación de capacitación enfocados en:

- Uso de las herramientas de seguridad de las aplicaciones para asegurar que el personal cuente con los conocimientos necesarios para integrar correctamente las nuevas prácticas de seguridad de DevSecOps.
- Colaboración entre los equipos de Desarrollo, Seguridad, lo cual es fundamental para una implementación efectiva de DevSecOps. Durante las capacitaciones se llevarán a cabo actividades diseñadas para romper los silos organizacionales, que es uno de los desafíos durante la implementación de DevSecOps, y promover la comunicación efectiva entre estas 3 áreas.
- Promover la cultura de seguridad dentro de la organización. Se tratarán temas como

la importancia de la seguridad en las aplicaciones con el objetivo que la seguridad no se perciba como un tema aislado sino como una responsabilidad compartida que impulse la eficiencia y la innovación.

Los programas de capacitación continua deben adaptarse para estar preparados antes los desafíos que se pueden presentar al implementar DevSecOps y para que los equipos estén preparados para enfrentar amenazas y garantizar la protección del software.

Entregables claves:

- Planificación de capacitaciones junto con materiales necesarios.
- Formatos para evaluaciones de conocimientos.

Integrar las herramientas y prácticas de DevSecOps

Para garantizar la seguridad en cada fase del desarrollo de software se deben integrar herramientas y metodologías específicas para el sector financiero, algunas de ellas son:

- Análisis de código estático y dinámico para detectar vulnerabilidades en las aplicaciones
- Gestión segura de las dependencias y librerías de terceros, para evitar el uso de componentes desactualizados, obsoletos o con vulnerabilidades conocidas.
- Automatización de pruebas de seguridad, para asegurar que cada nueva versión del software cumpla con los estándares de seguridad entes de su despliegue a producción.
- Implementación de mecanismos de autenticación seguros en las aplicaciones, para garantizar que solo las personas indicades pueden acceder al software.
- Implementación de métodos de cifrados seguros para protegerlos datos sensibles de los clientes.

Entregables claves:

- Documentación de mejores prácticas de DevSecOps.
- Configuración de herramientas de seguridad.

- Reportes de integración de prácticas de seguridad.

Pruebas y Validación

Es necesario que para una implementación efectiva de DevSecOps se lleven a cabo rigurosas pruebas al software para garantizar la seguridad y la estabilidad de las aplicaciones desarrolladas. Estas pruebas incluirán:

- Pruebas de penetración específicas para las aplicaciones, en especial las que estén expuestas a clientes internos.
- Validación del cumplimiento normativo, para asegurar que las aplicaciones cumplen con todos los estándares y normas requeridos.
- Pruebas de estrés y carga, estas pruebas son necesarias para evaluar la estabilidad del software en especial ante ataques de denegación de servicio.

La finalidad de realizar las pruebas es poder identificar y mitigar las vulnerabilidades antes de que ocurra un incidente y se comprometa la seguridad de las aplicaciones.

Entregables claves:

- Documentación de las pruebas de seguridad y vulnerabilidades detectadas
- Certificación del cumplimiento normativo
- Informes de resultados de las pruebas de estrés y rendimiento de las aplicaciones.

Despliegues de las aplicaciones con DevSecOps

La implementación de DevSecOps abarca todas las etapas del ciclo de vida de desarrollo de software incluyendo el despliegue a producción. Para garantizar despliegues seguros se deben implementar estrategias en los procesos de entrega de software tales como:

- Validaciones de seguridad automatizadas antes de cada despliegue.
- Despliegues progresivos y pruebas en entornos controlados, permitiendo detectar posibles fallos del software antes de una implementación en producción.
- Mecanismos para realizar rollback o retornos automáticos, para poder revertir adecuadamente los cambios o nuevas funcionalidades del software en caso de

identificar vulnerabilidades críticas después de la puesta en producción.

Entregables claves:

- Informe de procedimiento de despliegue seguro
- Reporte de validaciones de seguridad en el despliegue.
- Plan de rollback documentado.

Monitoreo y evaluación continua

La seguridad en DevSecOps no finaliza en la etapa del despliegue, sino que requiere que se realicen monitores constantes para poder prevenir y responder de manera rápida y efectiva ante posibles amenazas. Para ellos se deben implementar:

- Sistemas de monitoreo en tiempo real, para identificar actividades sospechosas y posibles ciberataques.
- Análisis de logs y auditorías de seguridad continuas, tanto de las aplicaciones cómo de la infraestructura donde se encuentra instalado el software.
- Pruebas de seguridad recurrentes, para garantizar la protección de las aplicaciones a lo largo del tiempo y asegurarse que cumplan con los estándares y normativas vigentes.
- Retroalimentación continua y optimización de procesos, para buscar la mejora constante de las herramientas, prácticas y estrategias de seguridad.

Entregable Claves

- Dashboard para monitoreo en tiempo real
- Informes de auditorías y análisis de logs de servidores y aplicaciones.
- Plan de mejora continua en seguridad.

6.5 MEDIDAS DE CONTROL

La implementación de DevSecOps en el área de desarrollo de una empresa del sector financiero implica un enfoque integrado de los equipos de desarrollo, seguridad y operaciones que debe garantizar la protección de datos y la conformidad con las regulaciones del sector financiero,

Para asegurar que esta implementación sea efectiva, es necesario, establecer medidas de control que permitan monitorear y evaluar continuamente el progreso del proceso de adopción de DevSecOps.

6.5.1 INDICADORES

A continuación, se detalla los indicadores claves que se establecerán para medir la efectividad de la propuesta:

Métricas de seguridad: medir la identificación, priorización y mitigación efectiva de las vulnerabilidades.

- Revisión de código, implementando herramientas para el análisis de código que permita identificar vulnerabilidades de seguridad antes que el código sea desplegado en producción, se puede medir con el número de vulnerabilidades de seguridad que logran ser identificadas en el código. KPI: Aumentar a un 95% la revisión de código fuente en cada ciclo de desarrollo.
- Establecer un proceso continuo para identificar y priorizar vulnerabilidades encontradas en el software y la mitigación de riesgos de seguridad de manera efectiva, se puede medir con el tiempo promedio desde la identificación hasta la mitigación de vulnerabilidades críticas en el software. KPI: Mitigar el 90% de las vulnerabilidades críticas dentro de un plazo de 15 días después de su identificación.
- Realizar auditorías de seguridad internas y externas de manera periódica para verificar la eficacia de las medidas de seguridad implementadas, se puede medir por el número de auditorías completadas al año y el porcentaje de auditorías con resultados satisfactorios que no cuenten con incidentes graves de seguridad. KPI: Realizar al menos 1 auditoría de seguridad mensual.
- Realizar evaluaciones periódicas de riesgos para identificar nuevas amenazas y brechas de seguridad, se pude medir con el número de evaluaciones de riesgos realizadas y el porcentaje de riesgos mitigados de acuerdo a la priorización de los mismos. KPI: Reducir un 50% el número de vulnerabilidades encontradas en las auditorías.

Métricas de cumplimiento regulatorio: evaluar el cumplimiento de las normativas y las

regulaciones del sector financiero.

- Asegurar que las aplicaciones y procesos de desarrollo cumplan con las regulaciones del sector financiero, el indicador de esta medida sería el porcentaje de cumplimiento de las auditorías de seguridad y regulaciones externas. KPIs Alcanzar al menos el 95% de cumplimiento normativo en 2 años. Reducir en un 50% el número de sanciones y multas por incumplimiento en un año.

Métricas de desempeño organizacional y colaboración: evaluar que los empleados estén adecuadamente capacitados y que los equipos trabajen juntos.

- Implementar programas de capacitación en DevSecOps y seguridad para todo el personal involucrado de las áreas claves, el indicador de esta medida sería el número de empleados capacitados y porcentaje de empleados que completan las capacitaciones con éxito. KPI: Asegurar que cada empleado reciba al menos 16 horas de capacitación en seguridad y cumplimiento normativo anualmente.
- Fomentar la colaboración entre los equipos de desarrollo, seguridad y operaciones para garantizar una implementación exitosa de DevSecOps y eliminar los silos organizativos, se puede medir por el nivel de satisfacción del equipo en relación con la colaboración entre los diferentes departamentos a través de la realización de entrevistas o encuestas internas. KPI: Lograr una tasa de satisfacción de al menos 85% medido mediante encuestas de colaboración entre equipos. Realizar al menos una reunión mensual entre los equipos para discutir el desarrollo de los proyectos y la efectividad de la colaboración entre los equipos.

6.5.2 PLAN DE SEGUIMIENTO

El plan de seguimiento se enfocará en la implementación y evaluación continua de los indicadores clave de las métricas de seguridad, métricas de cumplimiento regulatorio y métricas de desempeño organizacional y colaboración.

Para las métricas de seguridad se utilizarán herramientas de análisis estático para garantizar la revisión del código antes de su despliegue a producción, asegurando que se logre una revisión exhaustiva en cada ciclo de desarrollo, el seguimiento se debe realizar mensualmente midiendo el porcentaje de código revisado y el número de vulnerabilidades corregidas antes del despliegue.

Además, se establecerá un proceso continuo para la identificación, priorización y mitigación de vulnerabilidades, con un seguimiento regular del tiempo promedio desde la identificación hasta la resolución de vulnerabilidades críticas. En cuanto a las auditorías de seguridad, se programarán auditorías internas y externas de manera periódica para verificar la efectividad de las medidas de seguridad implementadas. El seguimiento se realizará mensualmente, evaluando el número de auditorías realizadas y los resultados obtenidos. Las evaluaciones periódicas de riesgos se llevarán a cabo trimestralmente para identificar nuevas amenazas y brechas de seguridad, registrando las vulnerabilidades encontradas y el progreso en su mitigación.

Respecto al cumplimiento normativo, se monitoreará anualmente el porcentaje de cumplimiento de las normativas aplicables y las auditorías externa para asegurar la reducción de las sanciones y multas por incumplimiento. La revisión continua será realizada de manera trimestral para poder adaptarse adecuadamente a las normativas del sector financiero ya que estas suelen cambiar con frecuencia. Con la implementación de DevSecOps se debe asegurar que en cada etapa del SDLC se adapte y cumpla todas las normativas de seguridad y privacidad vigentes.

El seguimiento de la capacitación en seguridad se realizará de manera anual realizando calendarización de capacitaciones para los empleados y cada capacitación deberá incluir un sistema para evaluar la efectividad de los temas brindados. Además, se deberá mantener un registro detallado de todas las horas de capacitación brindadas a cada uno de los empleados y los resultados de las evaluaciones con el objetivo de identificar áreas de mejorar y necesidades de formación adicionales. Para la colaboración interdepartamental se realizará seguimiento trimestral a través de encuestas para medir la satisfacción con la colaboración entre los equipos de desarrollo, seguridad y operaciones, organizar reuniones regulares mensuales o trimestrales para revisar el progreso de los proyectos de desarrollo de software y discutir posibles mejoras en los procesos de colaboración.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

Para realizar el cronograma de implementación y presupuesto se utilizó la Estimación por Tres Valores PERT, en la siguiente tabla se detalla la comparación entre las diferentes estimaciones basándose en criterios como la disponibilidad de datos históricos, la precisión, la complejidad, el tipo de estimación, el propósito y la visión del proyecto.

Tabla 24. Comparación entre estimaciones

Criterio	Estimación PERT	Estimación Análoga	Estimación Paramétrica
Datos Históricos	No requiere datos históricos	Requiere datos históricos de proyectos similares	Requiere datos históricos precisos para crear una fórmula matemática
Precisión	Es más útil para estimaciones inciertas ya que utiliza una distribución probabilística	Menos precisa, ya que se basa en promedios de proyectos pasados	Alta precisión si los datos históricos son precisos, pero menos fiable si no lo son
Complejidad	Moderada	Baja	Alta
Tipo de estimación	Utiliza estimaciones basadas en el juicio (optimista, más probable y pesimista)	Basada en el análisis de los proyectos previos	Basada en fórmulas matemáticas derivadas de datos pasados
Propósito	Estimar la duración de proyectos con incertidumbre	Estimar de forma rápida y comparativa	Estimar de manera precisa con base en cálculos y patrones históricos
Visión del proyecto	Proporciona una visión más flexible y detallada, teniendo en cuenta múltiples escenarios	Proporciona una visión basada en comparaciones anteriores, pero no tan detallada.	Proporciona una visión precisa, pero con una alta dependencia de los datos históricos

Fuente: Elaboración Propia

Se decidió utilizar la estimación PERT porque no se contaban con datos históricos sobre la implementación de DevSecOps en una empresa el rubro financiero y además no se cuenta con los datos exactos de la organización para realizar una estimación paramétrica

6.6.1 CRONOGRAMA DE IMPLEMENTACIÓN EN MESES

Tabla 25. Cronograma de Implementación

Actividad	Optimista (O)	Más Probable (MP)	Pesimista (P)	Triangular	Beta	Descripción detallada	Dependencias
Evaluación y diagnóstico en temas de seguridad de software	2	4	6	4	4	Análisis de vulnerabilidades, estado actual de seguridad	Ninguna
Planificación	2	3	6	4	3	Definición de KPIs, alcance, y estrategia de implementación	Evaluación y diagnóstico
Revisión y aprobación del plan	2	3	5	3	3	Validación del plan por stakeholders clave	Planificación
Capacitación del Personal	2	3	6	4	3	Módulo 1. Programa de formación en seguridad de software y DevSecOps, dirigido a los equipos de desarrollo, seguridad y operaciones. Se incluyen: Módulo 1: Principios de DevSecOps y seguridad en el ciclo de vida del software Contenido: Introducción a DevSecOps, gestión de riesgos, y principios de integración de seguridad. Duración: 2 semanas Participantes: Equipos de desarrollo, seguridad, DevOps y QA. Módulo 2: Uso de herramientas SAST, DAST y SCA en CI/CD (1 mes). Contenido: Implementación y uso práctico de herramientas de seguridad automatizadas. Duración: 2 semanas Participantes: Equipos de desarrollo y DevOps.	Revisión y aprobación del plan

						Módulo 3: Respuesta a incidentes de seguridad y gestión de vulnerabilidades Contenido: Técnicas de respuesta ante incidentes y cómo gestionar vulnerabilidades. Duración: 2 semanas Participantes: Equipos de seguridad, operaciones y QA. Módulo 4: Prácticas seguras de codificación y revisión de código (1 mes). Contenido: Mejores prácticas de codificación y técnicas de revisión de código. Duración: 2 semanas Participantes: Equipos de desarrollo y QA.	
Integración de Herramientas	4	6	9	6	6	Plataforma de Análisis de Código Estático (Ej.: SonarQube Developer Edition) Herramienta de Análisis Dinámico de Seguridad (Ej.: Acunetix) Sistema de Gestión de Vulnerabilidades (Ej.: Tenable Nessus Professional) Monitoreo de Seguridad en Tiempo Real (Ej.: Splunk Enterprise Security)	Capacitación del personal
Pruebas y validación del software	2	4	7	4	4	Después de la integración de las herramientas realizar las pruebas y validar su efectividad en la detección de vulnerabilidades.	Integración de herramientas
Despliegue de las aplicaciones	1	3	4	3	3	Realizar despliegues controlados a producción.	Pruebas y validaciones del software
Monitoreo y evaluación	6	8	12	9	8	Fomentar un monitoreo continuo de las aplicaciones y evaluaciones que permiten garantizar la seguridad en las aplicaciones que ya se encuentran desplegadas en producción.	Despliegue de las aplicaciones
Reserva de contingencias para actividades				4	3		

Reserva de Contingencia	6	5		
Línea Base de Costos (BAC)	47	43		
Reserva de Gestión	5	4		
Total del Proyecto	52	47		

Fuente: Elaboración Propia

6.6.2 PRESUPUESTO

Tabla 26. Presupuesto

Actividad	Optimista (O)	Más Probable (MP)	Pesimista (P)	Triangular	Beta
Adquisición de Herramientas de Seguridad y Automatización	L500,000	L750,000	L1,000,000	L750,000	L750,000
- Proveedores y Servicios Relacionados	L200,000	L300,000	L400,000	L300,000	L300,000
Licencias de Software / Desglose de Herramientas					
- Licencia Anual para plataforma de Análisis de Código Estático (Ej.: SonarQube Developer Edition)	L80,000	L120,000	L160,000	L120,000	L120,000
- Licencia Anual Empresarial para herramienta de Análisis Dinámico de Seguridad (Ej.: Acunetix)	L90,000	L135,000	L180,000	L135,000	L135,000
- Licencia Anual para Sistema de Gestión de Vulnerabilidades (Ej.: Tenable Nessus Professional)	L70,000	L105,000	L140,000	L105,000	L105,000
- Monitoreo de Seguridad en Tiempo Real (Ej.: Splunk Enterprise Security)	L60,000	L90,000	L120,000	L90,000	L90,000
Capacitación en Seguridad y Cultura DevSecOps Se incluyen costos para talleres presenciales, materiales, capacitadores certificados y licencias de plataformas educativas como Udemy Business.	L250,000	L500,000	L750,000	L500,000	L500,000
Consultoría Especializada El costo incluye consultores seniors especializados en implementación de DevSecOps. (125 horas)	L375,000	L625,000	L875,000	L625,000	L625,000
Horas Adicionales de Consultoría (15 horas)	L50,000	L75,000	L100,000	L75,000	L75,000
Mantenimiento y Actualización de Herramientas Incluye costos asociados a la renovación de licencias, soporte técnico, actualizaciones periódicas de software de seguridad y ajustes de compatibilidad entre las herramientas.	L100,000	L150,000	L200,000	L150,000	L150,000

Cumplimiento Normativo (Auditorías y Certificaciones) Costos necesarios para asegurar que un proyecto cumpla con los estándares y normativas vigentes, incluyendo evaluaciones y procesos de certificación.	L150,000	L250,000	L350,000	L250,000	L250,000
Auditorías Externas Costos relacionados con las revisiones realizadas por entidades independientes para verificar la implementación efectiva de controles de seguridad y buenas prácticas de DevSecOps.	L50,000	L100,000	L150,000	L100,000	L100,000
Costos Administrativos Se incluyen gastos operativos indirectos relacionados con la gestión del proyecto, como insumos, servicios de apoyo, logística, documentación y actividades para el desarrollo y monitoreo del proyecto.	L100,000	L120,000	L150,000	L123,333	L121,667
Reserva de Contingencias para Actividades				L120,000	L100,000
Línea Base de Costos (BAC)				L2,693,333	L2,671,667
Reserva de Gestión				L50,000	L30,000
Total del Proyecto				L2,743,333	L2,701,667

Fuente: Elaboración Propia

6.7 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Capítulo I			**Capitulo II**	**Capítulo III**			**Capítulo V**	**Capítulo VI**	
Título Investigación	Objetivo General	Objetivos Específicos	Teorías / Metodologías de Sustento	Variables	Poblaciones	Técnicas	Conclusiones	Nombre de la propuesta	Objetivos Propuesta
Impacto al integrar DevSecOps durante el ciclo de vida del desarrollo de software en las organizaciones a nivel mundial 2023-2024	Analizar el impacto en las organizaciones al integrar DevSecOps durante el ciclo de vida de desarrollo de software y conocer como los equipos de desarrollo adoptan la integración de estas prácticas.	•Identificar que prácticas de DevSecOps se pueden integrar en el desarrollo de software que ayuden a identificar vulnerabilidades y mitigar amenazas que se pueden presentar cuando el software se encuentre en producción. •Analizar si la implementación de DevSecOps permite ahorrar en costos de desarrollo asociados a la identificación y mitigación	Gestión del desarrollo de software Gestión de Riesgos Gestión de Incidentes Gestión de la Seguridad de la información Ciberseguridad	Implementación de DevSecOps en el SDLC Tiempo de entrega de desarrollo Costos de desarrollo asociados a identificación y mitigación de vulnerabilidades	2024 Global DevSecOps Report 5,315 (GitLab, 2024) SANS 2023 DevSecOps Survey 363 (Allen et al., 2023) Global State of DevSecOps 2024 100 (Blackduck, 2024) Total 6,618 encuestados	En esta investigación se trabajará con toda la población por lo que no se utilizarán técnicas de muestreo	1.Las organizaciones seleccionan que pruebas de seguridad ejecutar en las aplicaciones basados en diferentes criterios entre los que más toman en cuenta son: la sensibilidad de la información, las mejores prácticas recomendados por organizaciones de terceros que son expertos en temas de seguridad y la facilidad en la configuración y ejecución de las pruebas. Entre las prácticas de seguridad que más han adoptado las organizaciones	Implementación de DevSecOps en el área de desarrollo de una empresa del sector financiero	•Mejorar la seguridad en las aplicaciones y garantizar que cumplan con las normativas y regulaciones de seguridad del sector financiero, al integrar de manera temprana y continua herramientas y prácticas de DevSecOps en el ciclo de vida de desarrollo de software, asegurando que la seguridad se

		vulnerabilidades en el software desde el inicio de desarrollo y verificar si el tiempo de entrega del desarrollo de software disminuye al implementar DevSecOps •Conocer cuál es la percepción y adopción de DevSecOps por parte del equipo de desarrollo de la organización.					son la automatización de la compilación, la integración continua y las pruebas automatizadas y las que menos han adoptado las organizaciones son: la ingeniería del caos y la perspectiva sin culpa. Más del 60% las organizaciones que participaron en la encuesta utilizan entre 6 y 15 herramientas para realizar pruebas de seguridad en las aplicaciones. 2.Las personas y organizaciones encuestadas afirmaron que la relación entre el tiempo de entrega y desarrollo de software y la implementación de pruebas de seguridad en las aplicaciones se puede describir		convierta en una pieza fundamental desde el inicio permitiendo un desarrollo de software más seguro y confiable. •Ahorrar costos relacionados con la brecha de datos, incluyendo los costos operativos por la brecha de datos, costos por daño a la reputación y los costos asociados al incumplimiento de las normativas, al integrar DevSecOps se podrán identificar de manera temprana

							como que las pruebas ralentizan entre moderada y ligeramente el desarrollo de software, aunque hay un porcentaje considerable de encuestados que consideran que las pruebas de seguridad ralentizan gravemente el desarrollo y entrega de software, esto puede ser también porque hay pruebas que se agregan manualmente. El costo de la brecha de datos se ve afectado al tener un alto nivel de adopción de prácticas de DevSecOps según los resultados del reporte el costo disminuye en más de un 30% en comparación con las organizaciones		las vulnerabilidades lo que reducirá el riesgo de consecuencias económicas. •Optimizar la identificación y mitigación de vulnerabilidades mediante la automatización de pruebas de seguridad y el análisis continuo de código, esto permitirá responder de manera rápida y eficiente ante cualquier amenaza, garantizando la protección de datos sensibles y

							que tienen un bajo nivel de adopción. 3.En su mayoría, los encuestados conocen el enfoque de su organización en cuanto al tema de seguridad de las organizaciones, lo que indica que las organizaciones se interesan que su personal este informado sobre la seguridad que se utiliza en las aplicaciones. A lo largo de los años las organizaciones siguen aumentando la adopción de las diferentes prácticas de seguridad de DevSecOps. Algunos de los desafíos que las organizaciones han encontrado al adoptar DevSecOps y que involucran al personal son presupuesto		reduciendo los tiempos de reacción antes incidentes de seguridad. •Promover programas de capacitación para brindar conocimientos sobre uso de herramientas de seguridad y mejores prácticas, programas que promuevan la adopción de una cultura de seguridad, colaboración entre áreas claves para implementar DevSecOps y eliminar silos organizativos.

							insuficiente para programas y herramientas de seguridad, silos organizativos de las diferentes áreas que deben estar involucradas como son el área de desarrollo, operaciones y seguridad, la falta de aceptación por parte de desarrolladores e ingenieros de software y escasez de personal con habilidades necesarios para implementar seguridad en las aplicaciones.		

Fuente: Elaboración Propia

REFERENCIAS BIBLIOGRÁFICAS

Allen, B., Edmundson, C., &. (2023). *SANS 2023 DevSecOps Survey*.

Amazon Web Services, Inc. (2024). *¿Qué es el SDLC? - Explicación del ciclo de vida del desarrollo de software - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/sdlc/

Atlassian. (2024). *¿Qué es DevOps?* Atlassian. https://www.atlassian.com/es/devops

AXELOS. (2019a). *ITIL foundation: ITIL 4 edition* (First edition). TSO (The Stationery Office).

AXELOS. (2019b). *ITIL foundation: ITIL 4 edition* (First edition). TSO (The Stationery Office).

Blackduck. (2024). *Global DevSecOps Report*. https://go.blackduck.com/rs/846-ESG-342/images/Global-DevSecOps-Report_nb_fhb.pdf?version=0&mkt_tok=ODQ2LUVTRy0zNDIAAAGXBwoY89LItra26TtP_R48poE_wIOfIRjVu19oDiFnWAkvQZB2Cl7xrRAgs2TNgORKyK7W5aZB0DFyJ7Pfk_wGA49nQM5n9WIKJYD68F0ltmU

Bocconi, M. (2025, enero 21). *Los ciberincidentes en Latinoamérica aumentaron 25% cada año en la última década*. https://www.welivesecurity.com/es/cibercrimen/ciberincidentes-america-latina-aumentaron/

Camana, R. G. (2016). Potenciales Aplicaciones de la Minería de Datos en Ecuador. *Revista Tecnológica - ESPOL*, *29*(1), Article 1. https://rte.espol.edu.ec/index.php/tecnologica/article/view/464

Central, R. (2024, febrero 5). *HACKEO A CLARO PONE EN RIESGO INFORMACIÓN DE MILES DE CLIENTES - EL LIBERTADOR*. https://ellibertador.hn/2024/02/05/hackeo-a-claro-pone-en-riesgo-informacion-de-miles-de-clientes/, https://ellibertador.hn/2024/02/05/hackeo-a-claro-pone-en-riesgo-informacion-de-miles-de-clientes/

Check Point Software. (2024). *¿Qué es SDLC seguro? - Software Check Point*. Check Point Software. https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-secure-sdlc/

Checkpoint. (2025). *THE STATE OF CYBER SECURITY 2025*. Checkpoint.

CISA. (2024). *Informe CISA*. https://www.cisa.gov/

CodeSpaceAcademy. (2023, junio 26). *Cómo utilizar Python para el Análisis de Datos*. https://codespaceacademy.com/como-utilizar-python-para-el-analisis-de-datos/

Content.pdf. (s. f.). Recuperado 20 de noviembre de 2024, de https://repository.unimilitar.edu.co/server/api/core/bitstreams/afe74bdd-3b7d-46da-a118-f52f7fa16b62/content

CrowdStrike. (2024). *CrowdStrike 2024 Global Threat Report*. https://go.crowdstrike.com/global-threat-report-2024.html?utm_campaign=cao&utm_content=crwd-cao-amer-nola-en-psp-x-wht-gtr-tct-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=cyber%20safety%20and%20security&cq_cmp=21555316786&cq_plac=&gad_source=1&gclid=CjwKCAiAmfq6BhAsEiwAX1jsZ4CQdcGiPMcam0lGRrm_TcTPZubplCyswFti0slF30RFDsOCE5LkPRoCKCgQAvD_BwE

Data Bridge Market Research. (2025, enero). *Tamaño Del Mercado De Devsecops Y Estadísticas De Crecimiento De La Industria Para 2029*. https://www.databridgemarketresearch.com/es/reports/global-devsecops-market

Dell. (2024). *Global Data Protection Index Report | Dell USA*. Dell. https://www.dell.com/en-us/lp/dt/data-protection-gdpi

Dragon Jar. (2003, octubre 15). *Pentesting continuo en Honduras—DragonJAR*. https://www.dragonjar.org/pentesting-continuo-en-honduras.xhtml

Everett, G. D., McLeod, R., &. (2007). *Software testing: Testing across the entire software development life cycle*. IEEE Press, Wiley-Interscience, a John Wiley & Sons, Inc., Publication. https://doi.org/10.1002/9780470146354

García, A. E. M. (2024). *Ciberseguridad. Curso Práctico*. Ra-Ma Editorial.

Gartner. (2024). *Definition of DevOps—Gartner Information Technology Glossary*. Gartner. https://www.gartner.com/en/information-technology/glossary/devops

GitLab. (2024). *GitLab 2024 Global DevSecOps Report*. GitLab. https://learn.gitlab.com/devsecops-

survey-2024

Gitlab. (2025). *Lockheed Martin ahorra tiempo, dinero y recursos tecnológicos con GitLab*. https://about.gitlab.com/es/customers/lockheed-martin

Gobierno de Honduras. (2023, junio 15). *PLAN NACIONAL DE GOBIERNO DIGITAL 2023-2026 | Dirección de Gestión por Resultados (DIGER)*. https://www.diger.gob.hn/index.php/node/137

GoLegal. (2024). Protección de Datos Personales Costa Rica—Abogados Derecho Digital. *GoLegal - Firma legal en Derecho Digital / Derecho Informático en Costa Rica*. https://golegalcr.com/proteccion-de-datos-personales-asesoria-legal-costa-rica/

Grupo Kapa 7. (2024). Ciberataques en Honduras. *Grupo Kapa 7*. https://www.kapa7.com/threats/

Gutierrez, N. (2024, mayo 13). *30 Estadísticas sobre Seguridad Informática*. https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Hernández-Sampieri, R., Mendoza Torres, C. P., &. (2018). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA*.

Hincapie, J. (2024, noviembre 22). *Ciberseguridad en Honduras*. Ethical Hacking Latam. https://www.ethicalhackinglatam.com/ciberseguridad-en-honduras/

IBM Security. (2023). *Cost of a Data Breach Report*.

International, D. (2017a). *DAMA-DMBOK: Data Management Body of Knowledge (2nd Edition)*. Technics Publications, LLC.

International, D. (2017b). *DAMA-DMBOK: Guía Del Conocimiento Para La Gestión De Datos (Spanish Edition)*. Technics Publications.

IT Digital Security. (2022, septiembre 7). *Solo el 22% de las organizaciones tienen una estrategia formal de DevSecOps | Actualidad | IT Digital Security*. https://www.itdigitalsecurity.es/actualidad/2022/09/solo-el-22-de-las-organizaciones-tienen-una-estrategia-formal-de-devsecops

ITU. (2020). *Global Cybersecurity Index 2020*.

ITU. (2024a). *Global Cybersecurity Index 2024*.

ITU. (2024b). *Global Cybersecurity Index 2024*.

Juan Carlos Rivera. (2023, diciembre 4). *Ataques cibernéticos causan pérdidas millonarias en 2023*. La Prensa. https://www.laprensa.hn/honduras/honduras-ataques-ciberneticos-causan-perdidas-millonarias-2023-NK16498702

La Tribuna. (2024, julio 4). *Servicios de ciberseguridad crecen en Honduras en 16%*. Diario La Tribuna. https://archivos.latribuna.hn/2024/07/04/servicios-de-ciberseguridad-crecen-en-honduras-en-16/

Magazine, C. (2018, febrero 21). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

ManageEngine. (2024). *El estado de Ciberseguridad en América Latina 2024*. https://www.manageengine.com/latam/encuesta/estado-de-la-ciberseguridad-2024

MANUEL, O. C., JOSÉ. (2021). *Ciberseguridad. Manual práctico*. Ediciones Paraninfo, S.A.

manzanelli. (2023a, enero 16). *Norma ISO 29119: Estándares de pruebas de software - Lo que debes saber*. NormasISO.org. https://normasiso.org/norma-iso-29119/

manzanelli. (2023b, mayo 23). *Guía ISO 27034: Seguridad de la Información en Aplicaciones*. NormasISO.org. https://normasiso.org/norma-iso-27034/

manzanelli. (2023c, septiembre 19). *Norma ISO 27001: Garantiza la seguridad de la información*. NormasISO.org. https://normasiso.org/norma-iso-27001/

Marqués, M. P. (2015). *Minería de datos: A través de ejemplos*. Alpha Editorial.

MICITT. (2024). *MICITT | Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones*. https://www.micitt.go.cr/

Microsoft. (2024). *¿Qué es DevSecOps? Definición y procedimientos recomendados | Seguridad de Microsoft*. https://www.microsoft.com/es-mx/security/business/security-101/what-is-devsecops

Mordor Intelligence. (2023). *Análisis del tamaño del mercado de ciberseguridad en América Latina y el*

análisis de acciones—Informe de investigación de la industria—Tendencias de crecimiento. https://www.mordorintelligence.com/es/industry-reports/latin-america-cyber-security-market

Nist, G. M. (2024). *Spanish Translation of the NIST Cybersecurity Framework 2.0* (NIST CSWP 29 spa; p. NIST CSWP 29 spa). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.spa

Oficina del Director Nacional Cibernético | La Casa Blanca. (2023). *Oficina del Director Nacional Cibernético | La Casa Blanca*. https://www.whitehouse.gov/es/oncd/

OpenWebinars. (2024, diciembre 2). *DevSecOps: Seguridad integrada para DevOps moderno | OpenWebinars*. OpenWebinars.net. https://openwebinars.net/blog/devsecops-seguridad-integrada-para-devops-moderno/

Osborne, C. (2025, mayo 19). *Most companies take over six months to detect data breaches | ZDNET*. https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

owasp. (2024). *OWASP DevSecOps Guideline | OWASP Foundation*. https://owasp.org/www-project-devsecops-guideline/

Poder Legislativo Honduras. (2019, mayo 10). *Https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf*. https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

Polanco, I. Y., & Betancourt, J. F. (2022). *Análisis de datos con power bi, r-rstudio y knime: Curso práctico*. Ediciones de la U.

Prey. (2021). *Shift: Status of The Remote Work and Cybersecurity Landscape*. https://preyproject.com/resources/shift

Ramirez, O. (2025, febrero 14). DevSecOps en LATAM: La estrategia para frenar los ciberataques. *Bambu Mobile*. https://bambu-mobile.com/devsecops-la-estrategia-clave-para-frenar-el-crecimiento-de-ciberdelitos-en-latam/

Redhat. (2022, mayo 10). *El concepto de DevOps*. https://www.redhat.com/es/topics/devops

Redondo, A. M. F., Cárdenas, F. de J. N., &. (2022a). DevOps: Un vistazo rápido. *Ciencia Huasteca Boletín*

Científico de la Escuela Superior de Huejutla, *10*(19), Article 19. https://doi.org/10.29057/esh.v10i19.8121

Redondo, A. M. F., Cárdenas, F. de J. N., &. (2022b). DevOps: Un vistazo rápido. *Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla*, *10*(19), Article 19. https://doi.org/10.29057/esh.v10i19.8121

Reglamento general de protección de datos, 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/spa

Remache Típan, M. L. (2022). *Marcos de gestión de tecnologías de información: Análisis del marco de gestión ITIL v4*. [bachelorThesis, Quito : EPN, 2022.]. http://bibdigital.epn.edu.ec/handle/15000/22414

Rep_IUPB_Ing_Sof_Diseño_Prototipo.pdf. (s. f.). Recuperado 20 de noviembre de 2024, de https://repositorio.pascualbravo.edu.co/bitstream/pascualbravo/2377/1/Rep_IUPB_Ing_Sof_Dise%c3%b1o_Prototipo.pdf

Romero, M. Á. M., Tiza, D. R. H., Murillo, J. P. M., Cervantez, D. O. O., & Ordóñez, G. I. (2023). Método mixto de investigación: Cuantitativo y cualitativo. En *Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú*. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.105

SANS Institute. (2024). *SEC540: Cloud Security DevSecOps Training | Cloud Application Security Course | SANS Institute*. https://www.sans.org/cyber-security-courses/cloud-security-devsecops-automation/

Spoclearn. (2025). *DevSecOps Foundation Honduras | DevSecOps Foundation Training | DevSecOps Foundation Course | Spoclearn*. https://www.spoclearn.com/hn/courses/devops/devsecops-foundation-training/

Synopsis. (2023). *Awesome-annual-security-reports/Annual Security Reports/2023/Synopsys-Global-State-of-DevSecOps-2023.pdf at main · jacobdjwilson/awesome-annual-security-reports*. GitHub. https://github.com/jacobdjwilson/awesome-annual-security-

reports/blob/main/Annual%20Security%20Reports/2023/Synopsys-Global-State-of-DevSecOps-2023.pdf

Union Europea. (2024). *Ley de Ciberresiliencia de la UE | Configurar el futuro digital de Europa*. https://digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act

Valencia Duque, F. J., Orozco Alzate, M., &. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *22*, 73-88. https://doi.org/10.17013/risti.22.73-88

Vergara Cobos, E. (2024). *ECONOMÍA DE LA CIBERSEGURIDAD PARA LOS MERCADOS EMERGENTES*. https://openknowledge.worldbank.org/server/api/core/bitstreams/9ebee657-5ead-40e7-9d13-1836c6d4cd48/content

Villamarín, A. É., Sánchez-Montañés, J. L., &. (2023). *Introducción a DevSecOps para la mejora de los procesos de desarrollo de software con herramientas Open Source*.

WEforum. (2023). *Global Risks Report 2023*. World Economic Forum. https://www.weforum.org/publications/global-risks-report-2023/

Zapata, D. (2024, 08). *Ataques cibernéticos en Honduras van en aumentó cada año*. https://www.elheraldo.hn/honduras/instituciones-estado-vulnerables-ciberataques-honduras-HL20818492

ANEXOS

```python
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt

# Crear DataFrame de los datos
data = {
    'Costos': [3.54,5.22],
    'Nivel de adopción': ['Alto', 'Bajo']
}

df = pd.DataFrame(data)
df['Nivel de adopción'] = df['Nivel de adopción'].map({'Alto': 1, 'Bajo': 0})
print(df)
# Calcular la matriz de correlación
correlation_matrix = df.corr()

# Crear un gráfico de calor (heatmap) para visualizar la correlación
plt.figure(figsize=(10, 6))
sns.heatmap(correlation_matrix, annot=True, cmap='coolwarm', fmt=".2f", square=True, cbar_kws={"shrink": .8})
plt.title('Matriz de Correlación')
plt.show()
```

```
   Costos  Nivel de adopción
0    3.54                  1
1    5.22                  0
```

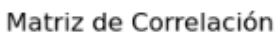


Figura 33. Código de Python para matriz de correlación
Fuente: Elaboración Propia

```python
import pandas as pd
import scipy.stats as stats

# Crear un DataFrame con los datos observados
observed_data = [
    [14.47, 85.53],  # Grupo 1 no ralentiza, Grupo 2 ralentiza
]
df = pd.DataFrame(observed_data, columns=["Grupo 1", "Grupo 2"])

# Realizar el test chi-cuadrado
chi2, p, dof, expected = stats.chi2_contingency(df)

# Imprimir los resultados
print(f'Chi-cuadrado: {chi2}')
print(f'Valor p: {p}')

# Tomando una decisión con un nivel de significancia de 0.05
alpha = 0.05
if p < alpha:
    print("Rechazamos la hipótesis nula.")
else:
    print("No rechazamos la hipótesis nula.")
```

```
Chi-cuadrado: 0.0
Valor p: 1.0
No rechazamos la hipótesis nula.
```

Figura 34. . Código de Python Prueba de Hipótesis 1
Fuente: Elaboración Propia

```python
from scipy import stats
import numpy as np

# Datos de costo para cada grupo
alto_adopcion = np.full(553,3.54)  # 553 encuestados, costos de 3.54 millones de dolares
bajo_adopcion = np.full(553,5.22)  # 553 encuestados, costos de 5.22 millones de dolares

# Prueba t de Student para comparar las medias
t_stat, p_value = stats.ttest_ind(bajo_adopcion, alto_adopcion)

print(f'Estadístico t: {t_stat}')
print(f'Valor p: {p_value}')

# Tomando una decisión con un nivel de significancia de 0.05
if p_value < 0.05:
    print("Rechazamos la hipótesis nula: hay una diferencia significativa en los costos.")
else:
    print("No rechazamos la hipótesis nula: no hay diferencia significativa en los costos.")
```

Figura 35. Código de Python Prueba de Hipótesis 2
Fuente: Elaboración Propia

```python
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
from sklearn.cluster import KMeans
from sklearn.preprocessing import StandardScaler

# Datos de adopción de las prácticas a lo largo de los años (2021, 2022, 2023)
data = {
    'Práctica': ['Automatización de Build', 'Integración continua (CI)', 'Pruebas automatizadas',
                 'Arquitectura Microservicios', 'Implementación continua (CD)', 'Deploy automatizada',
                 'Configuración como código', 'Monitoreo continuo', 'Infraestructura inmutable',
                 'Retrospectivas sin culpa', 'Ingeniería del caos', 'Otros'],
    '2021': [60.90, 49.60, 44.90, 43.00, 42.70, 41.00, 39.90, 32.00, 25.10, 11.80, 4.10, 0.80],
    '2022': [83.30, 57.20, 57.50, 51.90, 49.90, 44.60, 41.10, 56.00, 24.30, 17.30, 9.10, 2.90],
    '2023': [66.20, 51.60, 51.60, 40.90, 35.60, 43.10, 33.80, 35.60, 21.70, 11.70, 5.00, 2.10]
}
# Convertir los datos en un DataFrame
df = pd.DataFrame(data)
# Seleccionar solo los valores de adopción
X = df.drop(columns=['Práctica'])
# Normalización de los datos
scaler = StandardScaler()
X_scaled = scaler.fit_transform(X)
# Aplicar el algoritmo KMeans para clustering
kmeans = KMeans(n_clusters=3, random_state=42)  # Usamos 3 clusters
df['Cluster'] = kmeans.fit_predict(X_scaled)

# Ver los resultados con los clusters asignados
print("Resultados con Clusters Asignados:")
print(df)

# Visualización de los clusters
plt.figure(figsize=(10, 6))
plt.scatter(df['2021'], df['2022'], c=df['Cluster'], cmap='viridis', s=100)
plt.title('Clustering de prácticas de seguridad por tasa de adopción (2021 vs 2022)')
plt.xlabel('Tasa de adopción 2021')
plt.ylabel('Tasa de adopción 2022')
plt.colorbar(label='Cluster')
for i in range(len(df)):
    plt.text(df['2021'][i], df['2022'][i], df['Práctica'][i], fontsize=9)
plt.show()
```

Figura 36. Código de Python para Clustering para prácticas de seguridad

Fuente: Elaboración Propia

```python
import pandas as pd
import matplotlib.pyplot as plt
from sklearn.cluster import KMeans
from sklearn.preprocessing import StandardScaler

# Crear el DataFrame con los datos proporcionados
data = {
    "Desafíos": [
        "Presupuesto insuficiente para programas y herramientas",
        "Requisitos y prioridades en constante cambio",
        "Silos organizativos desarrollo, operaciones y seguridad",
        "Falta de aceptación por desarrolladores e ingenieros",
        "Escasez de personal y habilidades en seguridad de apps",
        "Falta de transparencia en trabajo desarrollo y operaciones",
        "Falta de aceptación por parte de la gerencia",
        "Falta de aceptación por parte del equipo de seguridad",
        "Escasez de personal y habilidades en ingeniería de la nube",
        "Escasez de personal y habilidades en seguridad de la nube"
    ],
    "2023": [46.8, 41.9, 41.5, 38.5, 37.2, 36.2, 29.6, 27.2, 26.9, 24.9],
    "2022": [38.4, 32.3, 43.4, 44.1, 44.1, 31.2, 35.1, 24.4, 18.6, 25.1],
    "2021": [28.8, 36.6, 50, 34.3, 37.8, 28.7, 25.2, 20.5, 28.3, 26.4]
}

# Crear DataFrame con los datos
df = pd.DataFrame(data)
# Seleccionar las columnas con los datos de los años
X = df.drop(columns=['Desafíos'])
# Normalización de los datos
scaler = StandardScaler()
X_scaled = scaler.fit_transform(X)

# Aplicar K-means para encontrar 3 clusters
kmeans = KMeans(n_clusters=3, random_state=0)
clusters = kmeans.fit_predict(X_scaled)
df['Cluster'] = clusters

# Visualizar los resultados de clustering
plt.figure(figsize=(8, 6))
plt.scatter(df['2021'], df['2022'], c=df['Cluster'], cmap='viridis', s=100, edgecolors='black')
plt.xlabel('Porcentaje de Desafíos en 2021')
plt.ylabel('Porcentaje de Desafíos en 2022')
plt.title('Agrupamiento de Desafíos (2021 vs 2022)')
plt.colorbar(label='Cluster')
plt.show()

# Mostrar los desafíos agrupados por clúster
grouped_by_cluster = df.groupby('Cluster')['Desafíos'].apply(lambda x: "\n".join(x)).reset_index()

# Mostrar los desafíos agrupados en líneas separadas
print("Desafíos agrupados por clúster:")
for _, row in grouped_by_cluster.iterrows():
    print(f"Cluster {row['Cluster']}:\n{row['Desafíos']}\n")
```

Figura 37. Código de Python para Clustering para Desafíos

Fuente: Elaboración Propia

```python
import pandas as pd
import matplotlib.pyplot as plt
from sklearn.linear_model import LinearRegression
from sklearn.preprocessing import LabelEncoder

# Datos para percepción de ralentización
data_percepcion = {
    'Categoria': ['Las pruebas ralentizan gravemente', 'Las pruebas ralentizan moderadamente',
                  'Las pruebas ralentizan ligeramente', 'Las pruebas no ralentizan',
                  'No puedo evaluar la relación con precisión'],
    'Porcentaje': [18.04, 42.81, 24.68, 9.22, 5.25]
}
# Crear DataFrame para percepción
df_percepcion = pd.DataFrame(data_percepcion)
# Convertir las categorías en números usando LabelEncoder
label_encoder = LabelEncoder()
# Definir el orden deseado para las categorías (de 4 a 0)
categoria_orden = {
    'Las pruebas ralentizan gravemente': 4,
    'Las pruebas ralentizan moderadamente': 3,
    'Las pruebas ralentizan ligeramente': 2,
    'Las pruebas no ralentizan': 1,
    'No puedo evaluar la relación con precisión': 0
}
# Codificar las categorías según el orden específico
df_percepcion['Categoria_encoded'] = df_percepcion['Categoria'].map(categoria_orden)
# Usar el porcentaje como la variable dependiente
X_percepcion = df_percepcion[['Categoria_encoded']]  # Variables independientes
y_percepcion = df_percepcion['Porcentaje']  # Variable dependiente
# Crear el modelo de regresión
model_percepcion = LinearRegression()
# Ajustar el modelo
model_percepcion.fit(X_percepcion, y_percepcion)
# Predicción
df_percepcion['Prediccion_Percepcion'] = model_percepcion.predict(X_percepcion)
# Mostrar resultados
print("Resultados del modelo de percepción:")
print(df_percepcion)
# Coeficientes del modelo de
print("\nCoeficientes del modelo de percepción:")
print(f"Coeficiente: {model_percepcion.coef_}")
print(f"Intercepto: {model_percepcion.intercept_}")
# Visualización de los resultados
plt.figure(figsize=(8,6))
# Gráfico de dispersión
plt.scatter(df_percepcion['Categoria_encoded'], df_percepcion['Porcentaje'], color='blue', label='Datos reales')
# Línea de regresión
plt.plot(df_percepcion['Categoria_encoded'], df_percepcion['Prediccion_Percepcion'], color='red', label='Línea de regresión')
# Etiquetas y título
plt.xlabel('Categorías de Percepción de Ralentización')
plt.ylabel('Porcentaje de Percepción')
plt.title('Regresión Lineal: Percepción de Ralentización')
plt.xticks(df_percepcion['Categoria_encoded'], df_percepcion['Categoria'], rotation=45)
plt.legend()
# Mostrar el gráfico
plt.tight_layout()
plt.show()
```

Figura 38. Código de Python para regresión Lineal Tiempos y Prácticas de seguridad

Fuente: Elaboración Propia

```python
# Datos para el costo
data_costo = {
    'Categoria': ['Bajo', 'Alto'],
    'Costo': [5.22,3.54]
}
# Crear DataFrame para costo
df_costo = pd.DataFrame(data_costo)
# Convertir las categorías en números usando LabelEncoder
df_costo['Categoria_encoded'] = df_costo['Categoria'].map({'Bajo': 0, 'Alto': 1})
# Variables para el modelo de costo
X_costo = df_costo[['Categoria_encoded']]  # Variables independientes (categorías codificadas)
y_costo = df_costo['Costo']  # Variable dependiente (Costo)
# Crear el modelo de regresión para costo
model_costo = LinearRegression()
# Entrenar el modelo
model_costo.fit(X_costo, y_costo)
# Predicción de costo
df_costo['Prediccion_Costo'] = model_costo.predict(X_costo)
# Mostrar resultados del modelo de costo
print("\nResultados del modelo de costo:")
print(df_costo)
# Coeficientes del modelo de costo
print("\nCoeficientes del modelo de costo:"
print(f"Coeficiente: {model_costo.coef_}")
print(f"Intercepto: {model_costo.intercept_}")
# Visualización de los resultados para costo
plt.figure(figsize=(8,6))
# Gráfico de dispersión para costo
plt.scatter(df_costo['Categoria_encoded'], df_costo['Costo'], color='blue', label='Datos reales')
# Línea de regresresión para costo
plt.plot(df_costo['Categoria_encoded'], df_costo['Prediccion_Costo'], color='red', label='Línea de regresión')
# Etiquetas y título
plt.xlabel('Categorías de Costo')
plt.ylabel('Costo')
plt.title('Regresión Lineal: Costo vs. Categoría')
plt.xticks(df_costo['Categoria_encoded'], df_costo['Categoria'], rotation=45)
plt.legend()
# Mostrar el gráfico
plt.tight_layout()
plt.show()
```

Figura 39. Código de Python para regresión Lineal Costos y Nivel de Adopción

Fuente: Elaboración Propia

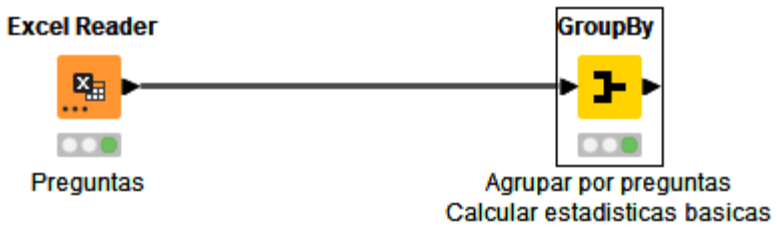


Figura 40. Nodos de Knime
Fuente: Elaboración Propia

Dialog - 3:78 - Excel Reader (Preguntas)

File

File and Sheet | Data Area | Advanced | Transformation | Flow Variables | Job Manager Selection | Memory Policy

Input Location

Read from: Local File System

Mode: File / Files in folder

File: C:\Users\Usuario\Documents\Clases Maestria\Trabajo Final Graduacion\Tesis\Pregunta 13.xlsx — Browse...

Select Sheet

First with data *(Pregunta 1)*

By name: Todas Preguntas

By position: 0 *(Position starts with 0.)*

Preview | File Content

Preview with current settings

The suggested column types are based on the first 10000 rows only. See 'Advanced Settings' tab.

Row ID	Pregunta	Categoria	Porcent...
Row0	¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	Las pruebas ralentizan gravemente	18.04
Row1	¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	Las pruebas ralentizan moderada...	42.81
Row2	¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	Las pruebas ralentizan ligeramente	24.68
Row3	¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	Las pruebas no ralentizan	9.22
Row4	¿Qué afirmación describe mejor la relación entre las pruebas de seguridad de aplicaciones y el desarrollo/entrega de software?	No puedo evaluar la relación con ...	5.25
Row5	¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	1 - 5	9.32
Row6	¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	6 - 10	33.5
Row7	¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	11 - 15	33.3
Row8	¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	16 - 20	14.57
Row9	¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	21+	3.86
Row10	¿Aproximadamente cuántas herramientas de prueba de seguridad de aplicaciones utiliza su organización?	No puedo estimar la cantidad	5.45
Row11	Costo de la brecha de datos	Alto nivel de adopción	3.54
Row12	Costo de la brecha de datos	Bajo nivel de adopción	5.22
Row13	¿Está seguro del enfoque de su organización hacia la seguridad de las aplicaciones?	No	13
Row14	¿Está seguro del enfoque de su organización hacia la seguridad de las aplicaciones?	Neutral	21
Row15	¿Está seguro del enfoque de su organización hacia la seguridad de las aplicaciones?	Si	60
Row16	¿Está seguro del enfoque de su organización hacia la seguridad de las aplicaciones?	No se	6

Figura 41. Nodo Excel Reader
Fuente: Elaboración Propia

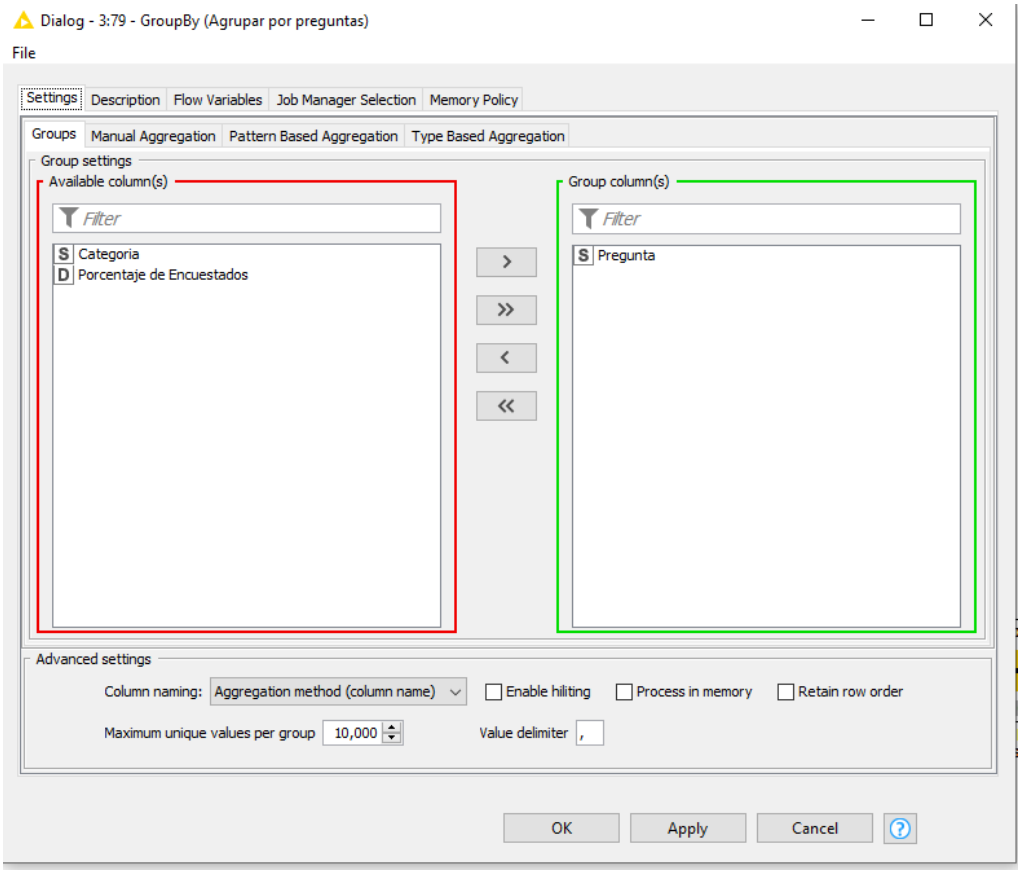


Figura 42. Nodo Group By

Fuente: Elaboración Propia

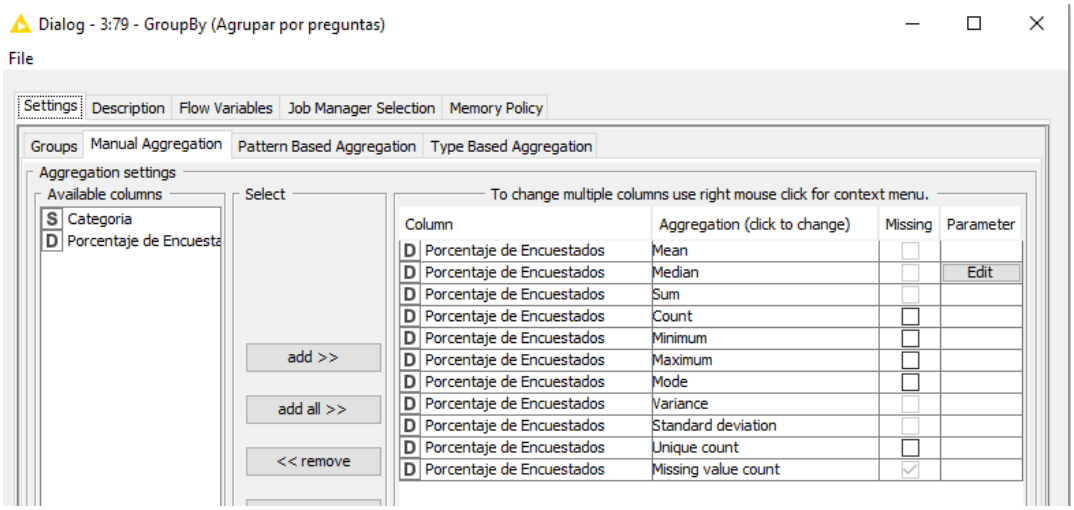


Figura 43. Configuración Nodo Group By

Fuente: Elaboración Propia