Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

MODELO DE ASEGURAMIENTO PARA LA AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD BASADO EN ESTÁNDARES ABIERTOS

Línea de investigación:
Ingeniería de software, simulación y desarrollo de TICs

Tesis para Optar el Grado Académico de Doctor en Ingeniería de Sistemas

Autor

Saavedra Jiménez, Robert Roy

Asesor

Hilario Falcon, Francisco Manuel

ORCID: 0000-0003-3153-9343

Jurado

Coveñas Lalupu, Jose

Petrlik Azabache, Ivan Carlo

Ogosi Auqui, Jose Antonio

Lima - Perú

2026

MODELO DE ASEGURAMIENTO PARA LA AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD BASADO EN ESTÁNDARES ABIERTOS

INFORME DE ORIGINALIDAD

26%	16%	2%	22%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	19%
2	repositorio.unfv.edu.pe Fuente de Internet	2%
3	hdl.handle.net Fuente de Internet	1%
4	moam.info Fuente de Internet	1%
5	reunir.unir.net Fuente de Internet	1%
6	repositorio.autonoma.edu.pe Fuente de Internet	<1%
7	lifeartech.wordpress.com Fuente de Internet	<1%
8	www.coursehero.com Fuente de Internet	<1%
9	www.researchgate.net Fuente de Internet	<1%
10	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	<1%
11	David William Foster, Daniel Altamiranda, Carmen de Urioste. "Spanish Literature - From Origins to 1700", Routledge, 2000 Publicación	<1%
12	academy.itu.int Fuente de Internet	<1%
13	es.scribd.com Fuente de Internet	

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

MODELO DE ASEGURAMIENTO PARA LA AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD BASADO EN ESTÁNDARES ABIERTOS

Línea de Investigación:
Ingeniería de software, simulación y desarrollo de TICs

Tesis para Optar el Grado Académico de
Doctor en Ingeniería de Sistemas

Autor

Saavedra Jiménez, Robert Roy

Asesor

Hilario Falcon, Francisco Manuel

ORCID: 0000-0003-3153-9343

Jurado

Coveñas Lalupu, Jose
Petrlik Azabache, Ivan Carlo
Ogosi Auqui, Jose Antonio

Lima-Perú

2026

Título

Modelo de aseguramiento para la automatización de controles de seguridad basado en estándares abiertos

Autor

Mg. Saavedra Jiménez, Robert Roy

Asesor

Dr. Hilario Falcon, Francisco Manuel

Línea de investigación

Ingeniería de software, simulación y desarrollo de TICs.

Dedicatoria:

A Dios, por darme la fortaleza y la sabiduría para superar cada obstáculo en este camino académico.

A mis padres, por su amor incondicional, su apoyo y sacrificio. Gracias por ser mi mayor inspiración y por enseñarme que con esfuerzo y perseverancia todo es posible.

A mis hermanos y familiares, por su compañía, motivación y aliento en los momentos más difíciles.

A mis amigos y docentes, por su guía, enseñanzas y por compartir conmigo este viaje de aprendizaje.

A todos los que, de una u otra manera, han formado parte de este logro, mi más sincero agradecimiento.

Agradecimientos:

Expreso mi más sincero agradecimiento al doctor Hilario Aradiel Castañeda, quien con su experiencia, orientación y apoyo incondicional han sido fundamentales en el desarrollo de esta tesis. Su guía y conocimientos han sido una fuente invaluable de aprendizaje, y sus consejos me han impulsado a mejorar constantemente.

Agradezco también a todos los profesionales que, con su tiempo y dedicación, contribuyeron de alguna manera a la culminación de este trabajo. Su apoyo ha sido clave para alcanzar este logro.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Esta investigación plantea un modelo para llevar a cabo la implementación y aplicación de automatización enfocada a la verificación de controles de seguridad y remediación de vulnerabilidades sobre los sistemas operativos del tipo empresarial usados como base tecnológica para las aplicaciones de las empresas alineados a estándares internacionales como CIS y PCI. Se aplica un enfoque de procesos a la presente investigación, aunque se creara un nuevo modelo que aporta conocimiento como un marco de referencia, los objetivos planteados se enfocan a la mejora del proceso seleccionado a través de la mejora de sus indicadores, de igual manera las hipótesis planteadas están alineadas a los indicadores. Para demostrar la relevancia en la mejora del proceso, se desarrolló una prueba de concepto para que el modelo no solo sea teórico, sino genere datos de mejora los cuales serán validados a través de las pruebas de normalidad de datos y verificación de mejoras con dos muestras del tipo pre-prueba y post-prueba. Finalmente se describe una modelo de implementación con un diseño integral que comprende diferentes soluciones tecnológicas a través de capas que añaden valor al modelo planteado, el cual, es implementado de forma práctica generando datos para demostrar su relevancia además de permitir la mejora continua del mismo modelo y el proceso seleccionado.

***Palabras clave**:* automatización, seguridad de la información, CIS, PCI, estándares internacionales, mejora continua.

ABSTRACT

In this research, an automation implementation and application model is proposed focused on the verification of security controls and remediation of vulnerabilities on business-type operating systems used as a technological basis for company applications aligned with international standards such as CIS and PCI. A process approach is applied to this research, although a new model was created that provides knowledge as a framework of reference, the objectives set focus on the improvement of the selected process through the improvement of its indicators, in the same way the Hypotheses posed are aligned with the indicators. To demonstrate the relevance in process improvement, a proof of concept was developed so that the model is not only theoretical, but also generates improvement data which will be validated through data normality tests and verification of improvements with two samples. of the pre-test and post-test type. Finally, an implementation model is described with a comprehensive design that includes different technological solutions through layers that add value to the proposed model, which is implemented in a practical way, generating data to demonstrate its relevance in addition to allowing the continuous improvement of the same model. and the selected process..

***Keywords**:* automation, information security, CIS, PCI, international standards, continuous improvement.

I. INTRODUCCIÓN

Este análisis tiene como propósito potenciar el proceso de remediación de vulnerabilidades sobre sistemas operativos empresariales aplicando lineamientos de seguridad aceptados por la industria, para ello, se plantea un modelo para la implementación de plataformas automatizadas capaz de facilitar el proceso de revisión y ejecución de controles de seguridad y remediación de dichas vulnerabilidades encontradas, mejorando en los indicadores clave del proceso como el tiempo, costo, complejidad, cumplimiento e impacto.

Considerando la importancia de la seguridad de la información en las instituciones estatales y privadas del estado peruano, la presente investigación se alinea a marcos referenciales, legales y tecnológicos que permitan su correcta aplicación, siendo los principales referentes los estándares definidos por el CIS y PCI cuya aplicación está demostrada en instituciones referentes del Perú.

Debido a la enorme complejidad que supone aplicar un modelo de seguridad de la información en una compañía, la presente investigación facilita la implementación de la plataforma necesaria a través del modelo propuesto, así mismo, el modelo permite la ejecución de los controles seleccionados de forma eficiente obteniendo los objetivos de mejora planteados en la investigación demostrado en una prueba de concepto desarrollada en la UTP.

Como parte del proceso de análisis, la tesis doctoral comprende a nivel de prueba de concepto 2 fases, elaboración del modelo y aplicación del modelo, sin embargo, a nivel documental será estructurado en capítulos, cuyos contenidos son los siguientes:

El primer capítulo expone la problemática que enfrenta la UTP, en la que busca mejorar los indicadores clave identificados por el investigador con un enfoque de procesos, dicho proceso se describe en formato BPMN como estándar de la industria para facilitar el análisis

del mismo y así obtener la situación actual y plantear objetivos de mejora a través de la situación esperada.

En el segundo capítulo expone el proceso mediante el cual se construyen las bases teóricas del estudio, la redacción del estado del arte y los marcos esenciales para captar y delimitar la presente investigación.

En el tercer capítulo presenta el diseño del análisis el cual expone un enfoque de variables de investigación, donde se resalta el uso de la variable interviniente o modelo propuesto, además de la dependiente e independiente. Como parte del proceso de investigación alineado al método científico, se debe diseñar los experimentos necesarios para demostrar las hipótesis planteadas que permiten cumplir los objetivos definidos.

En el cuarto capítulo se revela el cronograma de actividades de la prueba de concepto con un enfoque ágil donde cada solución implementada agrega valor y es verificable de forma inmediata al proyecto. También se revelan los resultados de las pruebas de normalidad y contrastación de hipótesis para demostrar la relevación estadística del modelo aplicado.

En los capítulos finales se abordan las recomendaciones, conclusiones y discusiones, incluyendo además los anexos, donde se presenta el modelo expuesto ya efectuado en la prueba de concepto.

1.1 Planteamiento del problema

Las empresas públicas y privadas independientemente del tipo de negocio que ofrezcan, requieren soportar sus procesos críticos en tecnologías de la información, siendo los sistemas operativos empresariales la principal tecnología base más usada para sus aplicaciones, en este sentido, requieren plataformas aseguradas para cumplir con los lineamientos que la industria de tecnología recomiendan, por ello, el perfil de especialista en seguridad informática se debe encargar de cumplir con dichos lineamientos a través de la actualización de parches de

seguridad, remediación de configuraciones que pueden vulnerar los sistemas y aplicaciones, mejoras en los componentes de sistemas, entre otros. El proceso de remediación de vulnerabilidades se apoya en estándares internacionales que ofrecen la documentación necesaria para cumplirlos, sin embargo, estos estándares o marcos de referencias son complejos de diseñar, aplicar y mejorar, por ello, la presente investigación sugiere un modelo propuesto de implementación de una plataforma de automatización de operaciones con enfoque en el análisis de vulnerabilidades de los sistemas operativos para luego aplicar los procedimientos de remediación de vulnerabilidades detectadas a fin de cumplir con los estándares definidos por entidades especializadas en dichos lineamientos como el CIS, PCI o DSS.

La presente investigación tiene como objetivo desarrollar y aplicar el modelo propuesto sobre una plataforma a modo de prueba de concepto para la Universidad Tecnológica del Perú sede Lima Norte. Para ello, se tomará una muestra de servidores con sistemas operativos empresariales independientemente de la aplicación primaria, pero que ofrezcan servicios hacia los usuarios externos e internos de la compañía.

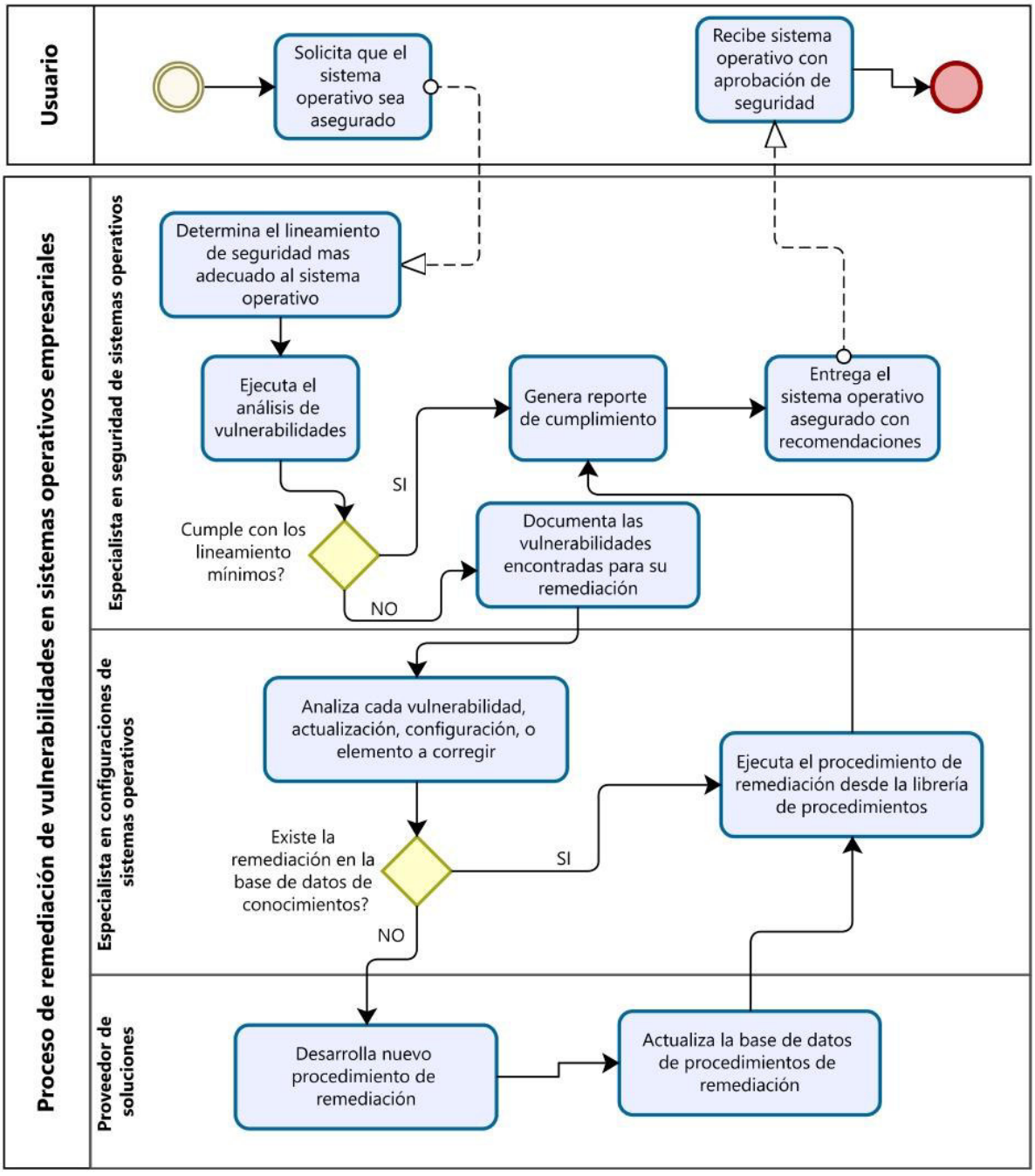
La presente investigación apoya el proceso de remediación de vulnerabilidades en sistemas operativos empresariales a través de tecnologías de software libre, pero con opción de soporte comercial, pero se aclara que los sistemas evaluados podrán ser sistemas comerciales libres o pagados como Red Hat Enterprise Linux, Microsoft Windows Server, Ubuntu Linux, CentOS Linux, entre otros.

1.2 Descripción del problema

Actualmente la fase de aseguramiento de sistemas operativos se efectúa como se revela en la Figura 1, donde dichos sistemas se aseguran y remedian a través de la ejecutan a través de controles definidos por la industria:

Figura 1

Proceso de remediación de vulnerabilidades AS-IS.



A parir del proceso descrito, se identifican los siguientes indicadores, los cuales se revelan en la tabla 1:

Tabla 1

Indicadores

Indicadores	Valores promedio
Tiempo	70
Costo	3500
Complejidad	60
Cumplimiento	30
Impacto	80

Los valores presentados en la Tabla 1 se expresan en unidades derivadas del calculo basado en otros valores establecidos durante la operacionalización de los indicadores.

A fin de progresar los indicadores de la fase seleccionada por el investigador, se deberá reformular el proceso de la Figura 1 para que pueda usar la tecnología de automatización y que además de integrar las diferentes tecnologías usadas para las prueba, podría simplificar el proceso ya que reducen muchas operaciones manuales por el motor de automatización propuesto en el modelo de implementación, de tal manera que los indicadores de la Tabla 1 podrán ser mejorados como se muestra en la Tabla2:.

Tabla 2

Situación actual/Situación esperada

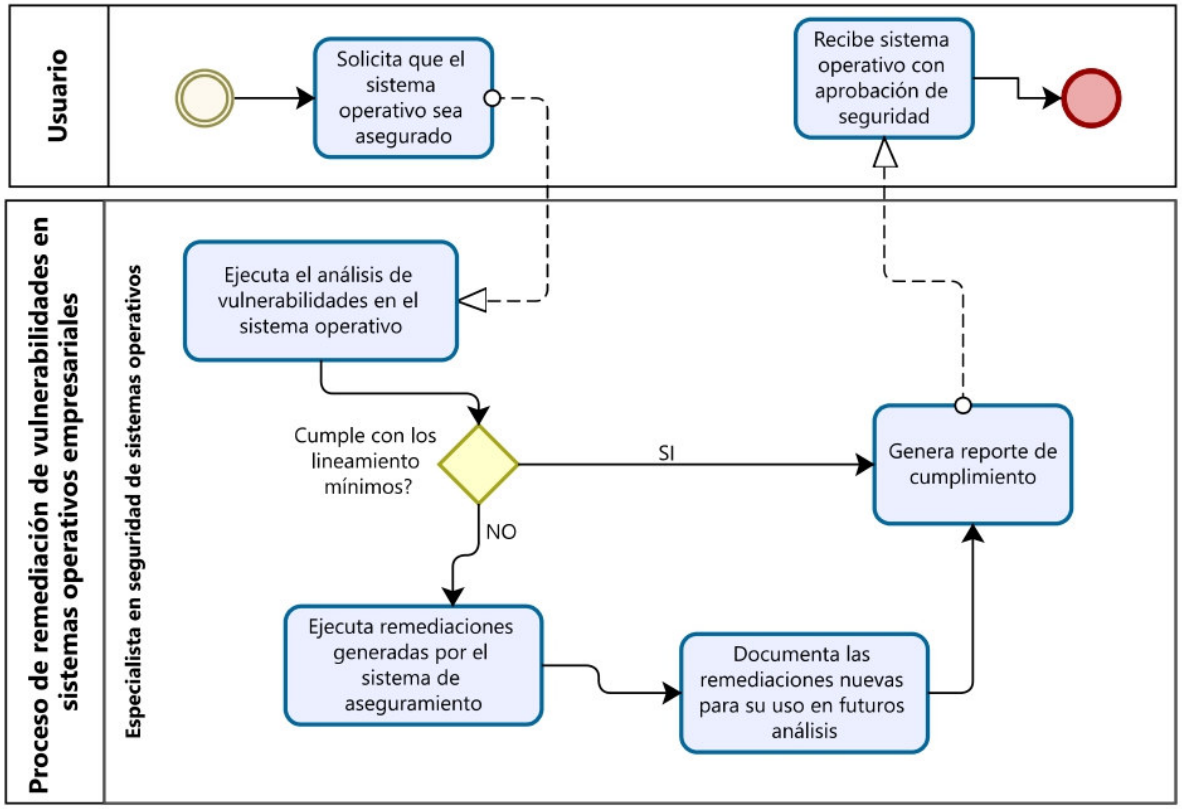
Situación Actual(AS-IS)	Situación Propuesta (TO-BE)
Tiempo – 70	Tiempo – 60
Costo – 3500	Costo – 2500
Complejidad - 60	Complejidad - 48
Cumplimiento – 30	Cumplimiento – 40

Impacto – 80 Impacto – 60

Para lograr este progreso, es indispensable reformularlo, tal como se ilustra en la Figura 2:

Figura 2

Proceso de remediación de vulnerabilidades TO-BE.



1.3 Formulación del problema

1.3.1 Problema general

¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales?

1.3.2 Problemas específicos

a) ¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?
b) ¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?
c) ¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?
d) ¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?
e) ¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?

1.4 Antecedentes

Para Atalaya (2023) en su tesis doctoral titulada “Modelo de ciberseguridad en universidades privadas en el Perú” se plantea un modelo de ciberseguridad orientado a universidades privadas, aunque su enfoque está delimitado al rubro educación, las aplicaciones y sistemas operativos son los mismos a los que se usan en empresas de diferentes rubros, por ello, la tesis de doctoral de Atalaya es un punto de partida para plantear un modelo en la presente investigación que use los mismo controles, normas, lineamiento, buenas prácticas de cara al aseguramiento de los sistemas operativos empresariales y las aplicaciones críticas del negocio.

Para Chávez (2023) en su tesis doctoral titulada “Catalizadores cobit 5 (control para tecnologías de información o relacionadas) y seguridad de la información en la empresa datco S&H, Huaraz, 2020” se estable la relación de los catalizadores de COBIT5 con la seguridad de la información, es decir, Chávez plantea alinear los controles de COBIT5 para cumplir con los requisitos de seguridad que las empresas desean implementar por exigencia de entidades supervisores, en este punto, la tesis de Chávez permite reutilizar un marco referencial muy aceptado por la industria como COBIT5 y estable una línea base para el modelo propuesto en la presente investigación.

Para Hernández (2023) en su tesis doctoral titulada “Investigación policial de la ciberdelincuencia y capacidad de respuesta de la policía nacional en materia de formación y capacitación a través del proyecto c1b3rwall” se aclara que cada vez los entornos digitales son más complejos y globalizados, por eso, se requieren modelos o métodos que garanticen la seguridad y hacer frente a amenazas que afecten o vulneren los sistemas operativos y aplicaciones críticas. En este punto, la tesis doctoral de Hernández aporta los marcos referenciales para aplicar lineamientos que puedan ser actualizados constantemente de cara a un entorno que también es cambiante, facilitando el aseguramiento por parte de los especialistas en tecnologías de la información, aportando al modelo propuesto en la presente investigación la base para aplicar los controles de seguridad que la industria requiere.

1.5 Justificación e importancia de la investigación

1.5.1 Justificación de la investigación

La presente investigación se justifica a través del aporte entregado, ya que el modelo propuesto aún no existe y será desarrollado en la investigación a través de la consolidación de buenas prácticas, estándares internacionales, modelos de automatización de sistemas, entre

otros elementos que serán integrados en un solo modelo de conceso a través de la experiencia del investigador.

La presente investigación es muy importante ya que implementara estándares abiertos a través del uso de software libre como plataforma base, sin embargo, su aplicación será en sistemas operativos sean libre o no, por lo que su desarrollo y aplicación fomenta el uso de tecnologías libres que pueden ser mejoradas en futuras investigaciones sin restricciones de patentes o derechos de autor siempre y cuando se referencie al investigador original.

Finalmente, la investigación apoyara a la mejora del proceso seleccionado al reducir la complejidad de la implementación de una plataforma que originalmente por separado deben diseñarse, instalarse, actualizarse y mejorar de forma continua a través de un modelo con pasos sugeridos y generando la documentación más importante para llevar el proyecto con una metodología de gestión como Scrum aplicada a infraestructura de TI.

1.5.2 Importancia de la investigación

El presente análisis es importante porque a través de la creación de un nuevo modelo se genera conocimiento en el dominio tecnológico de seguridad de la información, la documentación situada en el modelo permite identificar fases, actividades, roles y entregables necesarios para la adopción de la tecnología de automatización enfocada al proceso de remediación de vulnerabilidades.

El modelo propuesto adquiere importancia al ser aplicado y demostrado con una prueba de concepto desarrollada en la empresa seleccionada, obteniendo datos de mejora sobre sistemas operativos empresariales, generando información relevante para aplicar la mejora continua de procesos, permitiendo un modelo que puede ser mejorado en investigaciones futuras.

1.6 Limitaciones de la investigación

1.6.1 Limitaciones tecnológicas

Este análisis estará limitado por las tecnologías utilizadas, siendo la principal tecnología usada la automatización Ansible que ofrecerá la plataforma base de gestión de ejecución de tareas remotas en diferentes sistemas operativos empresariales.

Los sistemas operativos donde se realizará los análisis y remediaciones serán de uso empresarial, aunque estos podrán ser de uso no empresarial, la investigación se limitará solo a los empresariales ya que se requerirá en ciertos casos el apoyo bridando por un soporte empresarial.

Los análisis de realizaran a través de la solución openSCAP que permite el escaneo de sistemas y realizar evaluaciones alineadas al CIS, PCI o DSS, además de apoyarse de estas para la generación de programas de remediación, los cuales serán alojados en repositorios de código basados en GIT, teniendo las limitaciones técnicas de estas soluciones, aunque al ser soluciones de código libre tiene un alto nivel de integración con otras plataformas, lo que garantiza que dichas limitaciones podrán superarse a través de la programación de módulos en futuras investigaciones.

1.6.2 Limitaciones espaciales

Esta investigación se llevara a cabo como una provea de concepto en la Universidad Tecnológica del Perú, ubicado en Lima; sin embargo, su aplicación es extensible a cualquier empresa que implemente sistemas operativos empresariales para sus aplicaciones..

1.6.3 Limitaciones temporales

Esta investigación se efectuará en 2024, considerando las limitaciones tecnológicas vigentes en ese periodo, donde se indica que las tecnologías de remediación de controles de seguridad y automatización de operaciones, con un ciclo de vigencia temporal no mayor a 3

años, siendo necesario actualizar las plataformas tecnológicas para extender este tiempo de vigencia.

1.7 Objetivos de la investigación

1.7.1 Objetivo general

Mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad.

1.7.2 Objetivos específicos

a) Reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad.
b) Disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad.
c) Reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad.
d) Aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad.
e) Mitigar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad.

1.8 Hipótesis

1.8.1 Hipótesis general

La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

1.8.2 Hipótesis especificas

a) La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.
b) La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.
c) La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.
d) La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.
e) La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

II. MARCO TEÓRICO

2.1 Teorías que fundamentan la investigación

2.1.1 Teorías generales

Automatización

El portal de RedHat (2023) define la automatización de operaciones como un medio para alcanzar el progreso de los indicadores de las fases que normalmente se ejecutar de forma manual o con un nivel de automatización que no involucra la integración de diversas plataformas, ya que permite obtener resultados más rápido con la menor intervención de operadores minimizando el porcentaje de incidencias.

Sistemas Operativos Linux

Según Lenovo (2024) se define Linux como un sistema operativo de código abierto, el cual está compuesto por un software que permite administrar de forma directa los componentes de hardware de un sistema y sus recursos. Está situado entre las aplicaciones y el hardware, el cual nos permite establecer las diferentes conexiones entre todos los recursos físicos y sistemas de software que ejecutan las funciones.

2.1.2 Teorías especializadas

Ansible

La tecnología de Ansible (2023) es una plataforma de automatización de operaciones de propósito múltiple que se adecua a cualquier proceso de negocio que se soporte sobre soluciones de TI. Ansible permite la gestión de tareas remotas en sistemas operativos o aplicaciones, las cuales pueden realizarse de forma centralizada y creando excepciones que le dan un alto nivel de respuesta ante posibles eventualidades durante las fases de pruebas.

Protocolo de automatización de contenido de seguridad (SCAP)

El proyecto opensource de Openscap (2024) define a SCAP como un método que nos permite utilizar estándares específicos que apoya a las distintas organizaciones a lograr la automatización de la gestión de vulnerabilidades y la evaluación del cumplimiento de políticas. SCAP está compuesto por numerosos estándares abiertos de seguridad que son utilizados por aplicaciones que usan estos estándares para verificar vulnerabilidades en los sistemas y configuraciones incorrectas. OpenScap al ser un marco de referencia abierto, puede ser customizado para aplicarse en cualquier empresa por lo que requiere guías que faciliten su aplicación en sistemas operativos empresariales o libres como indica Atef (2025).

Centro de Seguridad en Internet

Para Amazon Web Services (AWS, 2024) los benchmarks del Centro de Seguridad en Internet (CIS) son prácticas ampliamente aceptadas y reconocidas a nivel internacional, creadas con el propósito de asistir a los expertos en el manejo y la instalación de sistemas de ciberseguridad. Estas recomendaciones elaboradas por varios especialistas a nivel internacional, como indica Edwards (2024) permiten a las organizaciones defenderse proactivamente contra el surgimiento de nuevas amenazas.

2.2 Marco conceptual

Marco conceptual de la variable interviniente – Modelo propuesto

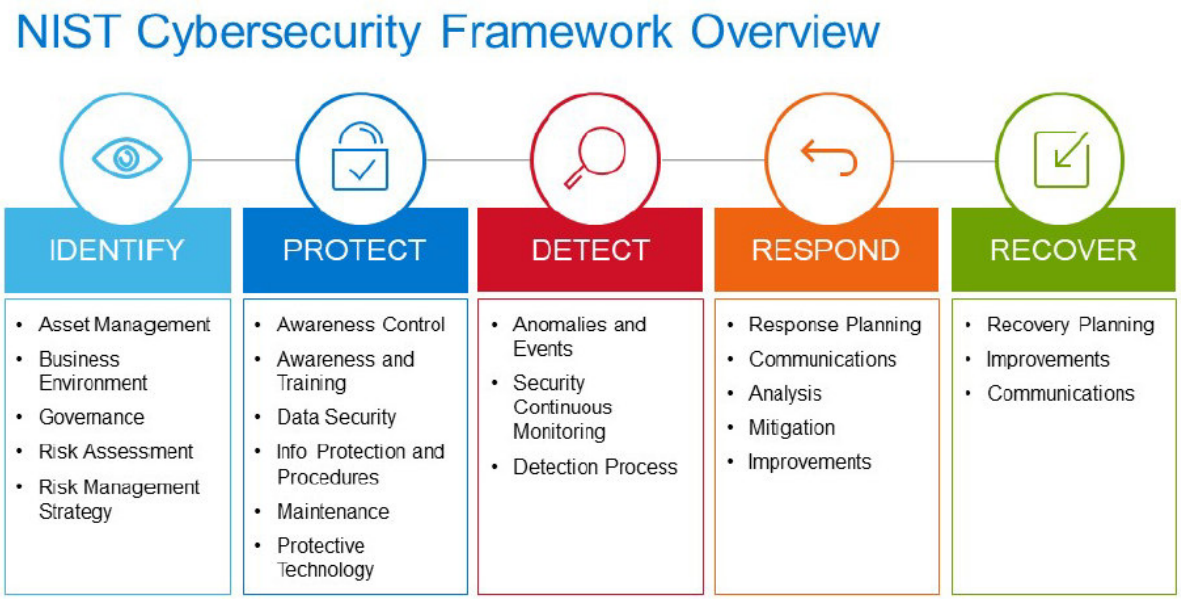
La variable interviniente no está claramente documentada en la bibliografía, por lo que se recurrió a literatura que presenta modelos similares al propuesto.

Para el Instituto Nacional de Estándares y Tecnología (NIST, 2024), el marco de trabajo de ciberseguridad es uno de los modelos con mayor prestigio y por lo tanto de los más

utilizados en la industria. El modelo otorgará una taxonomía de elevado nivel y una metodología para evaluar y gestionar los hallazgos de ciberseguridad. Renales (2024) en su investigación indica cinco funciones principales: identificar, proteger, detectar, responder y recuperar, tal como se revela en la Figura 3

Figura 3

Framework NIST. (NIST, 2024)



Otro modelo que proporciona información a la presente investigación es el estándar de la Organización Internacional de Normalización (ISO, 2024), donde se define el ISO/IEC 27001 como un patrón que brinda a diferentes empresas indistintamente del sector de actividad, la orientación necesaria para fijar, efectuar, mantener y potenciar de forma constante un sistema de gestión de seguridad de la información, permitiéndoles gestionar los riesgos relacionados con la seguridad de los datos pautando las mejores prácticas y principios en lo que a sistemas respecta como se muestra en la Figura 4.

Figura 4

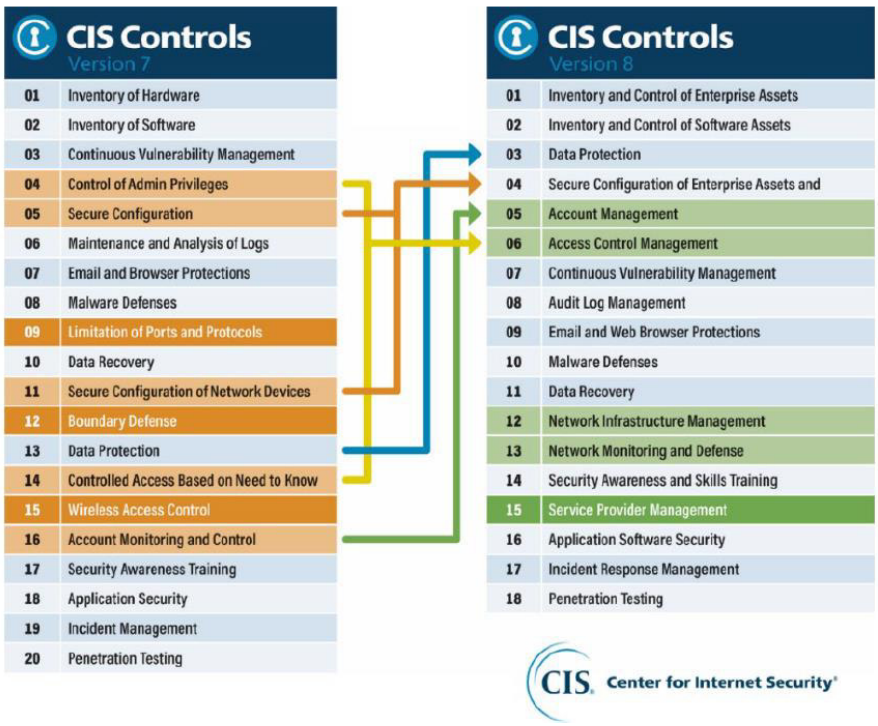
Estándar ISO 27001. (ISO, 2024)

La norma ISO aunque se sugiere que sea aplicado a empresas de alto volumen de información, procesos o empleados, puede aplicarse a empresas medianas y pequeñas como indica Alvarez y Gomez (2024) donde aplica perfectamente la norma en la Pymes.

Finalmente Centro para la Seguridad en Internet (CIS, 2024) define a Los controles críticos de seguridad del CIS como un conjunto de acciones recomendadas para la ciberdefensa que prioriza y simplifica las mejores prácticas para fortalecer la postura de la ciberseguridad. Permitiendo cumplir diferentes regulaciones de la industria como PCI DSS, HIPPA, GDPR, NIST, FISMA, ISO/IEC 27001, entre otros controles que indica Castro (2012) Dicho modelo agrupa los controles en perfiles que aseguran sistemas y aplicaciones siguiendo un orden como se revela en la Figura 5

Figura 5

Controles del CIS. (CIS, 2023)

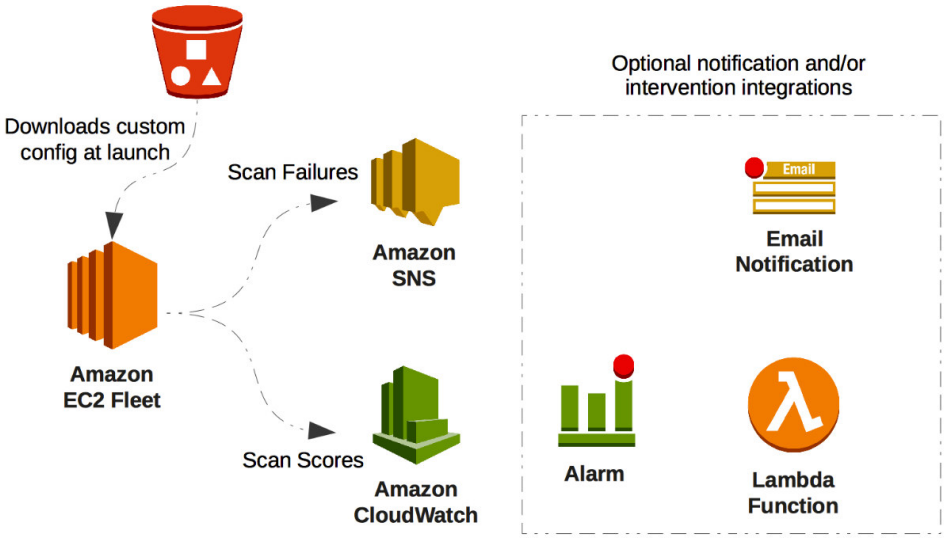


Marco conceptual de la variable independiente – Automatización de controles de seguridad

Para Amazon Web Services (AWS, 2024) se utiliza la arquitectura de openscap para realizar el proceso de análisis y remediación de vulnerabilidades, aunque openscap ofrece la posibilidad de ejecutar el escaneo de sistemas operativos, es necesario seleccionar los lineamientos más adecuados para cada sistema operativo y de ser necesario las aplicaciones críticas, por lo tanto, se muestra en la Figura 6 la arquitectura de AWS usa con OpenScap y se replicara en parte para el modelo propuesto

Figura 6

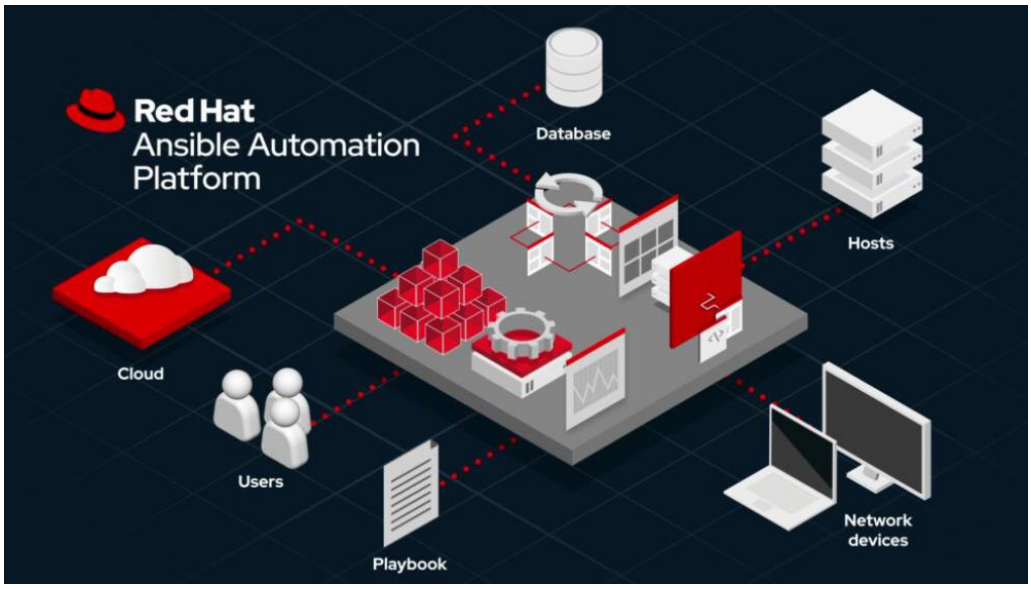
Arquitectura de openScap. (AWS, 2023)



El fabricante Redhat (2023) comercializa una plataforma empresarial basada en Ansible llamada Red Hat Automation Platform el cual proporcionara el componentes base de automatización del modelo propuesto, implementada a través de una arquitectura redundante cuya funciona principal es la ejecución de las tareas relacionadas con los controles de seguridad proporcionados por openscap en la arquitectura que Meijer-Hochstein et at. (2017) indica y se distribuyen bajo el modelo de suscripción como se revela en la Figura 7, para automatizar operaciones, despliegues, códigos, scripts o cualquier requerimiento de infraestructura o aplicaciones.

Figura 7

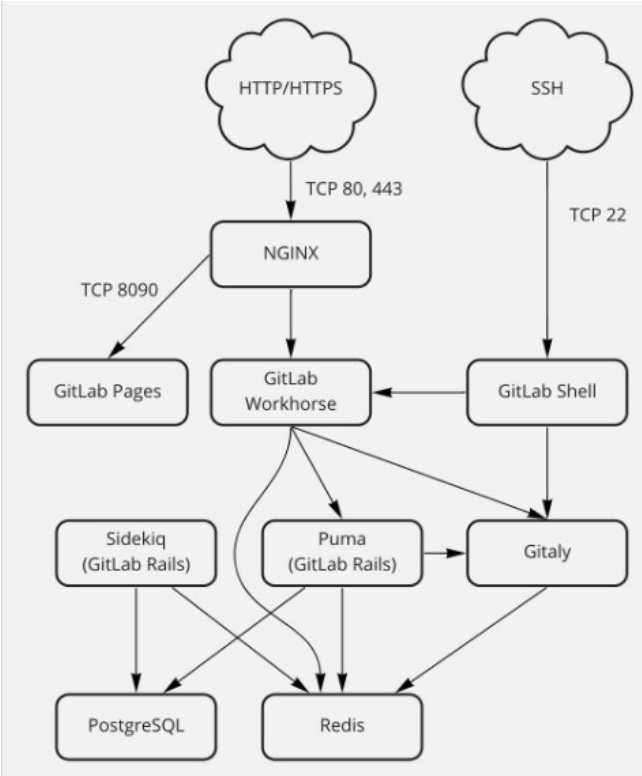
Arquitectura de Red Hat Automation Platform. (RedHat, 2023)



La presente investigación buscará combinar las arquitecturas de RedHat (2023) y de Gitlab (2023) basado en estándares abiertos. GitLab cumplirá el rol de repositorio de código de programas de automatización scripts en YAML como indica Telang (2020) y los controles de seguridad definidos en XML necesarios para la implementación del modelo expuesto apoyándose en las practicas descritas en Smith (2024) y como se revela en la Figura 8 para almacenar todos los programas e instrucciones complejas de la infraestructura, esto facilitará el restablecimiento de la plataforma en caso de caídas o perdida de infraestructura.

Figura 8

Arquitectura de GitLab-CE. (GitLab, 2023)



Marco conceptual de la variable dependiente – Proceso de remediación de vulnerabilidades en sistemas operativos empresariales

Para Goldman (2024) el proceso de remediación de vulnerabilidades son todos aquellos pasos que deben tomar las organizaciones para lograr proteger sus aplicaciones críticas y de esta manera cumplir los requisitos normativos y de seguridad internos. Lo cual involucra la creación e implementación de procedimientos y controles descritos por Gomez (2011) que permitan garantizar el cumplimiento de los requisitos de seguridad siguiendo de esta forma las mejores prácticas para proteger y salvaguardar sistemas, datos y operaciones.

Los controles de seguridad según Goldman (2024), son cruciales para poder proteger la información confidencial, prevenir ataques cibernéticos y cumplir regulaciones, ya que nos permiten definir medidas y mecanismos para lograr la ejecución de los propósitos de ciberseguridad.

Algunas mejores prácticas para el cumplimiento de la seguridad son:

- Crear un programa de cumplimiento de seguridad.
- Establecer controles de seguridad y automatizarlos
- Desarrollar un plan de administración de riesgos en las infraestructuras de TI
- Garantizar un monitoreo continuo

En el portal de Fortra (2022), se destaca que un programa eficaz en la gestión de vulnerabilidades necesita contar con un sistema de análisis que detecte debilidades. Esta herramienta de reducción automatizada escanea a fondo redes, sistemas y software en búsqueda de brechas de seguridad como las que describe Kennedy-Aharoni et at. (2025) que puedan ser utilizadas por accesos no autorizados para fines dañinos, por lo cual, las fases se dividen en cuatro:

- Tratamiento de vulnerabilidades
- Identificación de vulnerabilidades
- Informe de vulnerabilidades
- Evaluación de vulnerabilidades

Dicho proceso no repetitivo, ya que la gestión de vulnerabilidades es una actividad de mejora continua.

2.3 Marco legal

Aunque el alcance de la presente investigación a través de su prueba de concepto está limitada a una universidad privada, su aplicación puede extenderse tanto como al sector privado como al público, siendo en el caso puntual de las contrataciones estatales la ley de contracciones publicas descrita en Alvarez (2026) sin embargo, el marco legal que norma la presente investigación, se puede citar a los siguientes lineamientos del estado peruano:

- NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos
- NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1a Edición
- NTP-ISO/IEC 27003:2019 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Orientación. 2ª Edición
- NTP-ISO/IEC 27004:2018 Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación. 2ª Edición
- NTP-ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. 2ª Edición

Así mismo, en caso la información del negocio se considere de carácter confidencial relacionada con el sector financiero, banca o seguros como explica Ortega (2025), se citan los siguientes lineamientos como marco legal:

- Resolución S.B.S. Nº 504-2021 Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad

2.4 Marco filosófico

Para Lloredo (2012) el El paradigma positivista es una corriente filosófica y epistemológica que indica que el conocimiento científico debe fundamentarse en hechos observables, medibles y verificables, por ello, este de utilizar métodos objetivos para descubrir leyes que expliquen y permitan predecir los fenómenos de la realidad. Considerando esta descripción del paradigma positivista como también lo describe Comte (2012), la seguridad de la información debe estudiarse como un conjunto de hechos observables y medibles. Los riesgos, vulnerabilidades, actualizaciones, bufix, erratas, amenazas e incidentes de seguridad

se analizan mediante datos objetivos que permiten identificar patrones, formular hipótesis y diseñar controles efectivos. La presente investigación propone un modelo de seguridad que se alinea a la corriente filosófica de forma muy similar a la descrita por Burnashev (2024).

El paradigma positivista se destaca por el elevado interés por la verificación del conocimiento por medio de predicciones. La presente investigación se alinea a dicha corriente filosófica, ya que el proceso seleccionado que se busca mejorar es en esencia la aplicación y verificación de controles de seguridad que son lineamientos establecidos por la industria a través de estándares internacionales, los cuales deberán pasar por la verificación de conocimiento que ya cuentan con las buenas prácticas que son aceptado por las empresas de tecnología de información.

La Agenda 2030 en el sector educativo, liderada por el Ministerio de Educación del Perú a través de la (Comisión Económica para América Latina y el Caribe (CEPAL, 2023) , garantiza una educación inclusiva, equitativa y de calidad para 2030. Sus objetivos incluyen la enseñanza primaria y secundaria gratuita, igualdad de género, y el desarrollo de competencias para el trabajo y la sostenibilidad. En este sentido, la presente investigación presenta un modelo que fomenta estos objetivos a través de las tecnologías de la información y estándares abiertos, ya que no solo se trata de la implementación de tecnología en las universidades, sino de concientizar en la seguridad de la información en todos los componentes tecnológicos de las plataformas educativas.

El Plan Estratégico Institucional 2025-2030 de la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU, 2025) define sus objetivos con la Agenda 2030 y el sector educativo, enfocándose en la calidad y pertinencia de la educación superior y técnico-productiva. En este punto, la presente investigación enfoca el modelo de implementación de plataformas seguras, escalables, altamente disponibles, y otros factores de

calidad normados en los estándares ISO de cara a las tecnologías de la información como indica los objetivos que Rivera y Cervantes (2014) plantea para el año 2030.

2.5 Estado del arte

Comenzando con el diagnóstico del estado del arte en vínculo con el análisis enfocado a potenciar procesos efectuando tecnologías de la información en la educación a distancia, se ha preparado una recopilación de los estudios y sus primordiales contribuciones, señalando cómo estos estudios son relevantes para el desarrollo de este proyecto de investigación:

En la tesis de maestría de Banchof (2019) titulada “Infraestructura como Cóodigo Caso de estudio: Cientópolis” se resalta la complejidad que implica desplegar plataformas tecnológicas, siendo necesario apoyarse en metodologías capaces de simplificar y agilizar este proceso, en este sentido, el crecimiento de las metodologías agiles representa una mejora significativa, sin embargo, esta debe alinearse al dominio de despliegue de plataformas tecnológicas. Banchoff plantea que los sistemas informáticos deben apoyarse en repositorios especializados que faciliten el almacenamiento, versionamiento, corrección, etc., del código necesario para el despliegue, generando el concepto de infraestructura como código, donde los componentes tecnológicos son gestionados en procesos automatizados que consumen dicho código para facilitar la entrega, actualización, aseguramiento y mantenimiento de los sistemas. Sobre la investigación de Banchoff se aprovechará el diseño arquitectónico basado en modulo, sobre todo el repositorio de código que servirá para versionar los controles de seguridad.

En la tesis de grado de Caiza (2019) titulada “Diseño de un proceso de Hardening de servidores para una institución financiera del sector público” se indica el requerimiento de impulsar la seguridad de los sistemas operativos, ya que estos sistemas alojan las aplicaciones que soportan el negocio de las empresas, se requiere marcos de referencia de seguridad como

los que recomienda CIS que apoyan el cumplimiento de controles que reducen la probabilidad de vulneraciones de los sistemas y las aplicaciones.

La investigación de Caiza se enfoca a sistemas operativos empresariales ya que estos son respaldados por una garantía comercial que le permiten a los proveedores de sistemas de seguridad trabajar en conjunto con los proveedores de sistemas operativos para adecuar los controles sin comprometer dicha garantía, en este sentido, la investigación de Caiza permite efectuar con los requerimientos de las normas de seguridad y estándares internacionales reconocidos por la industria.

La presente investigación se relaciona mucho con la investigación de Caiza ya que ambas proponen el aseguramiento de sistemas operativos empresariales, por lo tanto, gran parte de la investigación de Caiza se reutilizará, enfocándose en los controles de seguridad definidos en el modelo propuesto.

En el tesis de maestría de Fandiño (2019) titulado “Cumplimiento del Esquema Nacional de Seguridad en servidores CentOS 7 con OpenSCAP” se presenta la solución openscap como la base tecnológica para el análisis y remediación de la seguridad en servidores Linux, considerando que openscap está basado en estándares abiertos, este se puede aplicar a diferentes sistemas, sean o no sistemas basados en Linux ya que su nivel de integración es muy alto y podrá alinearse a cualquier plataforma que logre complementar el modelo de Fandiño.

La investigación de Fandiño se relaciona con la presente investigación ya que ambas se basan en estándares libres, sin embargo, Fandiño no define componentes especializados de automatización para openscap, sobre este punto, la presente investigación añadirá capas de funcionalidades entregadas por soluciones complementarias para el modelo propuesto.

En la tesis de maestría de Gabarrin (2019) titulada “Integración y automatización de seguridad en procesos de desarrollo de metodologías ágiles” se resalta el uso cada vez más frecuente de metodologías tomando como base su capacidad interactiva e incremental, ofreciendo una serie de beneficios para la entrega de servicios de TI, sin embargo, Gabarrín indica que la seguridad no puede ser comprometida solo por entregar una plataforma de forma rápida, por ello, sugiere un modelo de entrega de servicios con enfoque de seguridad, alineándose a DevSecOps como parte del cambio cultural sugerido por la industria. En este punto la investigación de Gabarrín servirá como línea base de la presente investigación, ya que ambas se basarán en el manifiesto ágil, donde los componentes tecnológicos serán implementados como sprints, cada uno de ellos entregara valor al modelo, siendo la investigación de Gabarrín el marco metodológico necesario para implementar los controles de seguridad propuestos en el modelo propuesto.

En la tesis de grado de Ramírez (2019) titulada “Implementación de lineamientos base de seguridad en bases de datos Oracle y SQL Server en una entidad bancaria” se toma como caso de estudios las bases de SQL Oracle, Server, siendo las bases de datos críticas para la empresa seleccionada, su nivel de criticidad es muy alto y en caso de ser vulneradas tendrían gran impacto en los procesos de negocio, por ello, se requiere asegurar dichas bases y los sistemas operativos que las alojan a traves de lineamientos de seguridad capaces de establecer una línea base segura para el servicio. Por lo cual, el análisis de Ramírez se vincula con el presente análisis, ya que ambas ofrecen el uso de los lineamientos presentes en el CIS y en PCI para analizar y remediar las vulnerabilidades de los sistemas seleccionados. Aunque la investigación de Ramírez (2019) se enfoca solo a las bases de datos, su aplicación puede ampliarse a cualquier aplicación y sistema operativo siempre y cuando sus controles de seguridad estén incluidos en el CIS y PCI, y en caso no estén incluidos se trabajara en un programa de remediación a medida como parte de la presente investigación.

En el artículo de Mera-Aguilar et at. (2020) titulado “Herramienta de Software para la automatización de la construcción del catálogo de servicios de tecnologías de la información” se muestra la necesidad de simplificar la entrega de servicios a través de catálogos que proporcionen plataformas, sin embargo, se ha descuidado el dominio de seguridad en la entrega de dichos servicios. Por ello, en el artículo se propone un modelo de automatización de operaciones que permita facilitar el proceso de gestión de la configuración de las plataformas, en este punto, la investigación se relaciona con la presente investigación, ya que ambas se apoyan en la solución de automatización para analizar y remediar las vulnerabilidades encontradas, como parte del modelo propuesto, se busca una mejora continua de sistemas de información por medio de la ejecución del modelo.

En la tesis de grado de Ardila y Daza (2020) titulada “Verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado” se muestra la necesidad de asegurar las aplicaciones críticas del negocio, siendo una plataforma muy importante el directorio activo de la empresa, ya que esta entrega no solo la autenticación centralizada, además ofrece la data de contacto de cada empleado de la compañía, en este sentido, la exposición de la información a usuarios fuera del dominio corporativo supone una vulneración a la seguridad definida a nivel institucional, en este punto, la presente investigación coindice con la investigación de Ardila y Daza al aplicar los estándares CIS y NIST para proteger a las aplicaciones críticas ante posibles intrusiones al establecer una línea base segura en el tiempo, además de ello, se propone el uso del ciclo de mejora continua para actualizar constantemente la línea base de seguridad requerida por la empresa.

En la tesis de maestría de Castro (2020) titulado “DevSecOps: Implementación de seguridad en DevOps a través de herramientas open source” se justifica como la industria de tecnología ha evolucionado a un método de despliegue ágil de sistemas basado en

componentes más ligeros, los cuales llevan a la cultura de DevOps, sin embargo, la agilidad esperada tiende a descuidar aspectos de seguridad, ya que los controles de seguridad tienden a retrasar los procesos de despliegues en caso no se cuente con modelos de referencia enfocados a estas metodologías agiles, en este punto, la investigación de Castro propone controles de seguridad alineado a DevOps cambiando el enfoque a DevSecOps lo cual cumple con los requerimientos esperados por la empresa sin descuidar los aspectos de seguridad. La presente investigación es muy similar a la investigación de Castroya que ambas sugieren la adopción de tecnologías de opensource para alcanzar los objetivos planteados, siendo importante entregar plataformas tecnológicas capaces de integrarse de forma transparente a los procesos existentes a través de interfaces de conexión desarrollado en estándares abiertos. La presente investigación propone un modelo que tomara muchos componentes de código abierto del modelo de Castro cambiando el alcance a sistemas operativos empresariales.

En el artículo de Khumaidi (2021) titulado “Implementation of devops method for automation of server management using Ansible” se sustenta como la cultura de DevOps apoya a los programadores a tener plataformas tecnológicas de forma rápida reduciendo la complejidad en las operaciones de despliegue, aunque el programador tradicionalmente tiene poco conocimientos de infraestructura, redes, alta disponibilidad, entre otros, DevOps simplifica las operaciones para contar con plataformas tecnológicas, por ello, Khumaidi que es necesario descargar todo el conocimiento que los programadores requieren en soluciones de automatización, en este punto, el estudio de Khumaidi se relaciona con el presente análisis ya que ambos usan a Ansible como plataforma base de automatización. La investigación de Khumaidi también indica que las prácticas de aseguramiento tienden a ser obviadas por los especialistas, por ello, el modelo propuesto tendrá un enfoque claro de aseguramiento de sistemas que pueda mejorar el enfoque de DevOps indicado por Khumaidi.

En el artículo de Likitha (2022) titulado “Automation of Server Configuration Using Ansible” se presenta un modelo de automatización de operaciones muy similar al modelo expuesto en el presente análisis, el modelo de Likitha busca la integración de diferentes soluciones de automatización basadas en estándares abiertos, los cuales crean capas de añaden funcionalidad a la plataforma final. Likitha resalta la complejidad que implica desplegar una plataforma tecnológica, sobre todo por la cantidad de configuraciones que deben realizarse, en caso de no cumplir correctamente las configuraciones sugeridas en lineamientos de tecnología, se podría exponer el sistema a ataques internos o externos, por ello, Likitha resalta la importancia de aplicar dichas configuraciones de forma simplificada, en este punto, la presente investigación tomara como línea base el modelo de Likitha para implementar un nuevo modelo propuesto.

En el artículo de Payá-Cotarelo et at. (2022) titulado “Automated security configuration deployment systems with early error detection” se resalta la importancia de aplicar controle de seguridad a las plataformas, este proceso debe realizarse de forma continua para lograr que las aplicaciones y sistemas operativos alojados en ellas cumplan con una línea base de seguridad que permite disminuir la probabilidad de caer en intrusiones que comprometan la uniformidad de los servicios de las compañías. Para ello los investigadores implementan un modelo de automatización que realice la tarea de escaneo o análisis de seguridad para luego facilitar el proceso de remediación de las vulnerabilidades encontradas, sobre esta forma de trabajo la propuesta del artículo se puede considerar a la mejora continua como base metodológica del estudio, siendo una metodología de trabajo muy similar al presente análisis, por lo tanto, la investigación será reutilizada como base para los procesos sugeridos en el análisis.

En el artículo de Sasidharan (2022) titulado “A Case Study to Implement Windows System Hardening using CIS Controls” se presenta un caso de estudio donde los servidores

Windows Server son avaluados a través del estándar CIS entregado por el Centro de Seguridad de Internet. En el caso de estudio Sasidharan se determinó que sistemas que no logran aprobar los controles de seguridad indicados por el CIS, son vulnerables a ataques que vulneran la seguridad del sistema, siendo muy probable la denegación del servicio instalado en el servidor.

El estudio de Sasidharan se vincula con el presente análisis en el alcance de las soluciones tecnológicas aplicadas, siendo su objetivo el aseguramiento de sistemas operativos empresariales, en el caso de Sasidharan se aplicará en sistemas Windows, sin embargo, CIS proporciona los controles para múltiples plataformas, por este motivo, la investigación de Sasidharan proporcionará una parte del modelo propuesto por el investigador.

En la tesis de grado de Rodríguez y Cedeño (2022) titulada “Marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación, comercialización y exportación de muebles” se muestra la aplicación del CIS en una empresa de fabricación, comercialización y exportación de bienes, la cual soporta sus procesos en aplicaciones instaladas sobre sistemas operativos empresariales, ya que la empresa requiere el soporte comercial del proveedor de sistemas. En el caso de Rodríguez y Cedeño los sistemas operativos requieren asegurar su plataforma, configuraciones, accesos remotos entre otros componentes que ofrecen servicios críticos a la empresa.

La investigación de Rodríguez y Cedeño se relaciona con la presente investigación en muchos componentes, empezado por los sistemas operativos que son parte del alcance de la investigación, los servicios alojados en dichos sistemas operativos y las configuraciones requeridas en los sistemas los cuales deben cumplir con los controles de seguridad del CIS para pasar de ambientes de prueba a ambientes de producción, en este sentido, la investigación de Rodríguez y Cedeñoutiliza la misma base del modelo propuesto en el análisis.

En la tesis de maestría de Giraldo (2022) titulada “Herramienta de Ciberseguridad para la auditoría de una línea base de buenas prácticas de seguridad informática en Pymes a través de un prototipo funcional de Chatbot que ofrezca recomendaciones para la mitigación de vulnerabilidades en servidores Windows” se resalta que las compañías sean medianas, grandes o pequeñas, sufren igualmente del impacto generado por la vulneración de sus servicios, en este sentido, Giraldo indica que se requieren marcos de referencia que ayuden a aplicar la metodología de análisis y mitigación de vulnerabilidad a través del cumplimiento de controles de seguridad, los cuales son elaborados por empresas especializadas con todo el conocimiento necesario para configurar los sistemas operativos a fin de asegurar en gran medida dichas plataformas. La metodología mencionada por Giraldo concientiza sobre la necesidad de la aplicación de las buenas prácticas en ciberseguridad sin sumar el tamaño de la empresa, por ello dicha investigación se relaciona en gran medida con la presente investigación, ya que ambas proponen la aplicación de los controles de seguridad en sistemas operativos Windows y Linux Empresarial que vendrían a ser los sistemas con mayor aplicación comercial en la industria.

En la tesis de maestría de Torchio (2022) titulada “Security assessment and threat response through SCAP” se expone las funcionalidades de OpenScap, siendo una herramienta capaz de gestionar los controles de seguridad sugeridos por diferentes proveedores de lineamientos de seguridad, openscap trabaja como herramienta basada en software libre, por lo tanto, es libre de usarse en cualquier sistema operativo ya sea libre o propietario. Para Torchio el uso de openscap le permite importar los lineamientos del CIS, PCI o de cualquier otro proveedor, para realizar el análisis de vulnerabilidades en un parque informático, a fin de recomendar remediaciones de seguridad para ser aplicadas y corregir dichas configuraciones, parches, actualizaciones, etc. En este punto, la investigación de Torchio aportará el modelo propuesto la tecnología más relevante para la ejecución de sus objetivos de investigación

deseados, donde el procederá a la mejora del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

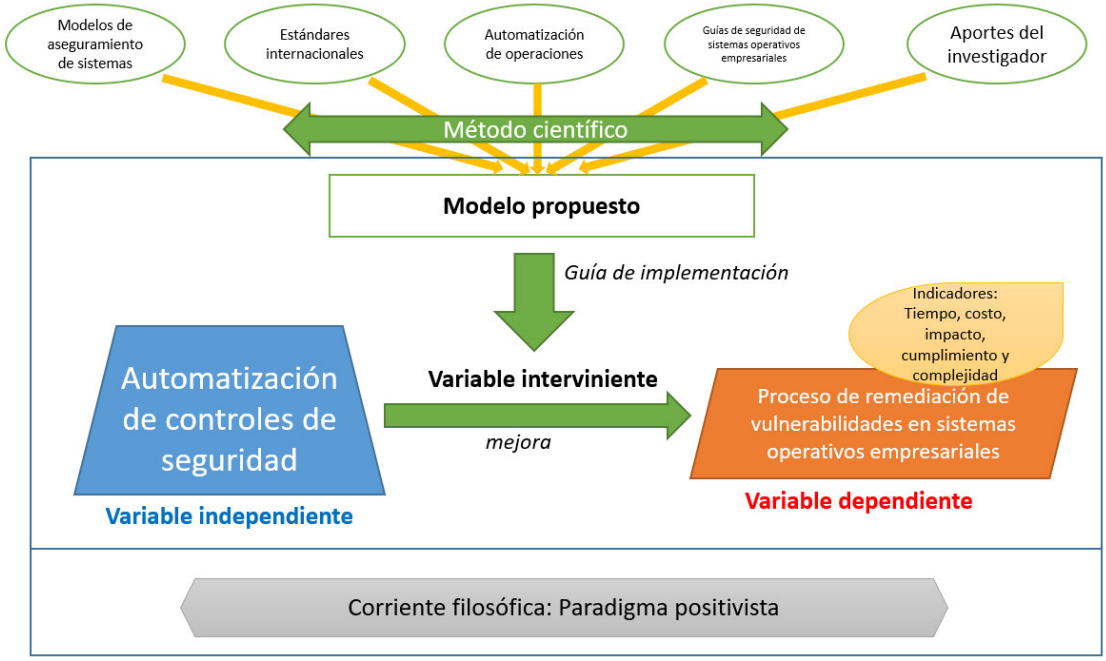
En la tesis de grado de Yaqui (2023) titulado “Implementación de hardening en sistemas operativos de servidor: implememementación de hardening en sistemas operativos de servidor linux de base debian” se muestra un proceso de hardenización o aseguramiento de la plataforma Debían o Ubuntu, siendo un proceso que no existe en la empresa y necesita ser documentado con un enfoque de aplicación de controles de seguridad, donde Yanqui propone al CIS como base para la remediación de vulnerabilidades. La investigación de Yanqui se relaciona con la presente investigacion en la selección de controles, ya que estos se aplicarán a Linux empresariales, siendo los servidores Linux un grupo de servidores donde el nivel de aseguramiento es muy customizable y la complejidad en el aseguramiento es alta, en esta complejidad el aporte de la presente investigación se aprovecha bastante a través del modelo propuesto.

III. MÉTODO

Para agilizar el progreso del proceso de análisis, se presenta el diseño que guiara la realización del análisis.

Figura 9

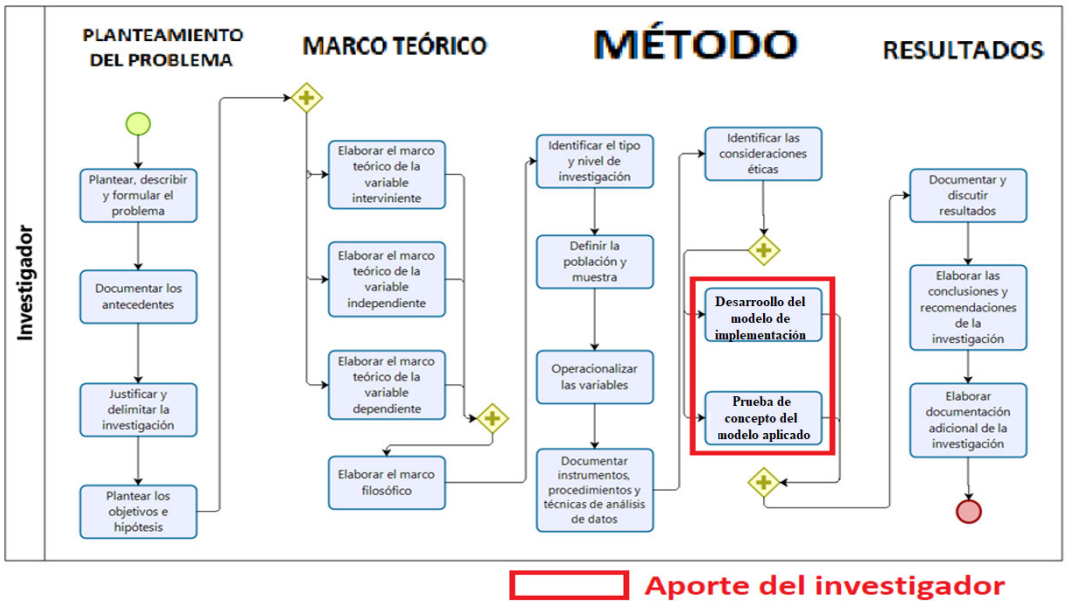
Diseño de la investigación propuesta.



Asimismo, se representa gráficamente la fase de análisis mediante un modelo BPM, destacando las funciones primordiales que constituyen el aporte de este estudio.

Figura 10

Metodología de investigación propuesta.



3.1 Tipo de investigación

En esta investigación identificamos el tipo:

Tipo básico: se contribuirá con conocimiento mediante el progreso de un modelo que no ha sido documentado previamente en la revisión del estado del arte, siendo un modelo que facilita la implementación de la tecnología de automatización de cara a aplicar controles de seguridad en sistemas operativos empresariales. El modelo luego será aplicado para demostrar estadísticamente su relevancia en el proceso seleccionado por el investigador.

También identificamos el nivel:

Nivel explicativo: se explicará y revelará el existente vínculo entre la tecnología de automatización y el proceso de aseguramiento de sistemas operativos empresariales, con el fin de determinar el impacto en la mejora del proceso. Además, se incluyen acciones respecto a otros niveles, aunque con inferior relevancia en comparación con el nivel sobresaliente que es el explicativo.

3.2 Población y muestra

Para lograr los objetivos fijados en esta investigación, señalados en la sección 1.6.1, se determina como unidad de análisis los indicadores presentados en la Tabla 1.

La cantidad de veces que se ejecutan los controles de seguridad para remediar vulnerabilidades en los sistemas operativo son repetitivas y continuas sobre todo en los primeros días de descubrimiento de la vulnerabilidad, siendo un proceso muy variable que no se puede determinar con exactitud, por lo cual, se define a la población como:

N= Indeterminado

Con una población indeterminada, podemos utilizar un método de muestreo intencionado basado en la suposición de teoremas previos validados en investigaciones similares, que se basa en el razonamiento estadístico, como el Hogg (1978) donde podemos establecer una muestra intencionada de al menos 30 observaciones donde la desviación estándar de la población es desconocida, definiendo así la muestra como:

n= 30 mediciones de los indicadores planteados - Muestreo intencionado

Diseño de Experimentos

Se revela el siguiente tipo de experimento a ser efectuado en la contratación de la hipótesis

Tabla 3

Experimento

GE	**O1**	**X**	**O2**

Grupo Experimental = Ge = Procesos tecnológicos de educación remota.

Observación Nr01 = O1 = Cálculo de los Indicadores del proceso sin efectuar la del modelo expuesto.

Estimulo = X = Modelo propuesto.

Observación Nr02 = O2 = Cálculo de los Indicadores del proceso después de efectuar el modelo expuesto.

3.3 Operacionalización de variables

Variable independiente: Automatización de controles de seguridad.

Variable interviniente: Modelo propuesto.

Variable dependiente: Proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

Tabla 4

Variables y sus indicadores

Variables	Dimensión	Indicadores (
Independiente: Automatización de controles de seguridad	Tecnológica	Presencia_Ausencia
Dependiente: Proceso de remediación de vulnerabilidades en sistemas operativos empresariales	Proceso	Tiempo Costo Complejidad
	Seguridad	Cumplimiento

Impacto

Tabla 5

Conceptualización de indicadores

Variable independiente: Automatización de controles de seguridad	
Presencia_Ausencia	Se define como la presencia o ausencia de la tecnología de automatización de controles de seguridad en la investigación
Variable dependiente: Proceso de remediación de vulnerabilidades en sistemas operativos empresariales	
Tiempo	El indicador tiempo se refiere al cálculo del tiempo desde que se requiere el análisis de un sistema operativo empresarial y la remediación de las vulnerabilidades del mismo sistema operativo hasta llegar a una línea base considerada segura por los especialistas.
Costo	El indicador costo se refiere a la sumatoria de todos los costos asumidos por el proceso de análisis y remediación de vulnerabilidades del sistema operativo empresarial, se considera el costo de infraestructura, licencias, software de escaneo, software de remediación, entre otros costos.
Complejidad	El indicador complejidad es la ponderación del esfuerzo y la dificultad del trabajo realizados por proveedores especializados en desarrollar programas de remediación a

	medida en lenguaje yaml siendo criterios de evaluación las líneas de código, interacción con sistemas externos, uso de módulos de trabajo o colecciones de roles que fueron desarrollados por terceros, entre otros componentes que sirven para desarrollar programas de remediación.
Cumplimiento	El indicador cumplimiento se refiere al porcentaje de aprobación de los lineamientos establecidos en la línea base del estándar de evaluación, siendo necesario referenciar estándares de seguridad que ponderan los lineamientos según su importancia definidos por especialistas en seguridad como CIS, PCI o DDS.
Impacto	El indicador impacto se refiere a las consecuencias negativas de no mitigar las vulnerabilidades identificadas en los sistemas operativos, siendo necesario considerar el impacto en el proceso, en las aplicaciones y en negocio y ponderarlos en un valor numérico,

Tabla 6

Operacionalización de indicadores

Variable	**Indicador()**	**Índice**	**Unidad de Medida**	**Unidad de Observación**
Independiente	Presencia_Ausencia	[No..Si]	-	-

Dependiente	Tiempo	[1..200]	horas	Planes de remediación
	Costo	[1..10000]	Soles	Presupuestos del área de seguridad informática
	Complejidad	[1..100]	unidades	Reporte de proveedores
	Cumplimiento	[1..100]	unidades	Análisis de vulnerabilidades
	Impacto	[1..100]	unidades	Matriz de riesgos

3.4 Instrumentos

Tabla 7

Instrumentos de recolección de datos

Técnicas	Instrumentos
Entrevista	Cuestionario y encuestas
Observación	Guía de observación

3.5 Procedimientos

Para analizar los datos recogidos mediante los instrumentos expuestos, se ejecutan la siguiente fase con el objetivo de contrastar cada una de las hipótesis fijadas; este procedimiento se aplica de forma individual a cada una.

Paso 1: Planteamos el problema por medio de la hipótesis especifica nula.

Paso 2: Efectuamos la prueba de normalidad para corroborar que la data lograda cuenta con normalidad tanto en PrePrueba como en PostPrueba.

Paso 3: Efectuaremos la prueba estadística con 2 muestras (PrePrueba y PostPrueba) con el software estadístico.

Paso 4: Conseguimos el p-value a fin de efectuar el análisis de resultados.

Paso 5: Aprobamos o negamos la hipótesis especifica nula.

3.6 Análisis de datos

Tabla 8

Procesamiento y análisis de datos

Instrumentos de recolección	Instrumentos de análisis
Cuestionario	Software estadístico
Guía de observación	Simuladores

3.7 Consideraciones éticas

El investigador de este análisis se compromete a adherirse a las pautas éticas mínimas ilustradas en evitar conflicto de intereses, ser honesto, objetivo y respetar la propiedad intelectual

El responsable de esta investigación se compromete a cumplir con los principios éticos fundamentales, tales como la objetividad, la honestidad y el respeto por los derechos de autor y respeto por las investigaciones revisadas previamente, así como un análisis crítico para eludir consecuencias perjudiciales o cualquier riesgo para las empresas que apoyan la investigación.

Toda tesis, documento, publicación, etc. de autoría de terceros será citado con la norma APA 7ma edición para evitar el plagio.

De acuerdo con los principios de consentimiento y confidencialidad informativo, toda la data utilizada en la prueba de concepto virtual se basará provenientes de sistemas operativos existentes. En caso de requerirse data sensible, esta no será divulgada con el propósito de resguardar los intereses de quienes colaboran con el análisis.

IV. RESULTADOS

4.1 Cronograma de actividades

Se revela el cronograma de actividades con el enfoque de la metodología Scrum donde se plantean los Sprints necesarios para concretar la aplicación del modelo propuesto:

Tabla 9:

Cronograma

	Actividad	Duración(días)	Inicio	Fin	Dependencia
Modelo de aseguramiento para la automatización de controles de seguridad basado en estándares abiertos		60	01/09/2024	30/10/2024	
1	Sprint 01 - Desarrollo del modelo propuesto	5	01/09/2024	05/09/2024	
2	Análisis de requerimientos y controles de seguridad	1	01/09/2024	01/09/2024	
3	Selección de plataformas tecnológicas	1	02/09/2024	02/09/2024	2
4	Documentación de las fases y actividades del modelo	2	03/09/2024	04/09/2024	3
5	Elaboración de plantillas y formatos de entregables	1	05/09/2024	05/07/2024	4

6	Sprint 02 - Implementación de la arquitectura propuesta	4	06/09/2024	09/09/2024	1
7	Diseño de la solución de automatización de controles de seguridad	1	06/09/2024	06/09/2024	1
8	Diseño de los componentes de interoperabilidad e integración	1	07/09/2024	07/09/2024	7
9	Elaboración del plan de despliegue e implementación	1	08/09/2024	08/09/2024	8
10	Documentación de la arquitectura general de la solución integral	1	09/09/2024	09/09/2024	9
11	Sprint 03 - Implementación de la solución de automatización Ansible	12	10/09/2024	21/09/2024	6
12	Preparación de los sistemas operativos y componentes para Ansible	1	10/09/2024	10/09/2024	6
13	Instalación de la plataforma de automatización Ansible en modo cluster	3	11/09/2024	13/09/2024	12
14	Programación y adecuación de contenidos de automatización en yaml	5	14/09/2024	18/09/2024	13
15	Despliegue de los programas de ejecución de controles de seguridad	2	19/09/2024	20/09/2024	14
16	Documentación de la plataforma Ansible implementada	1	21/09/2024	21/09/2024	15
17	Sprint 04 - Implementación de la solución de contenidos y código	3	22/09/2024	24/09/2024	11
18	Preparación del sistema operativo compatible con GitLab	1	22/09/2024	22/09/2024	11
19	Instalación de la plataforma GitLab	1	23/09/2024	23/09/2024	18
20	Documentación de la plataforma GitLab implementada	1	24/09/2024	24/09/2024	19
21	Sprint 05 - Implementación de la solución de OpenSCAP	8	25/09/2024	01/10/2024	11

22	Preparación de los sistemas virtuales para OpenSCAP	1	25/09/2024	25/09/2024	11
23	Instalación de la solución OpenSCAP	2	26/09/2024	27/09/2024	22
24	Configuración de los perfiles seleccionados para remediaciones	4	28/09/2024	01/10/2024	23
25	Documentación de la plataforma OpenSCAP implementada	1	01/10/2024	01/10/2024	24
26	Sprint 06 - Implementación de la solución de reportes	3	02/08/2024	05/10/2024	11,17,21
27	Preparación de los sistemas operativos orientados a reportes	1	02/10/2024	02/10/2024	11,17,21
28	Instalación de la solución de reportes	1	03/10/2024	03/10/2024	27
29	Documentación de la plataforma de reportes implementada	1	04/10/2024	04/10/2024	28
30	Sprint 07 - Implementación de la solución de autenticación centralizada	5	05/10/2024	09/10/2024	26
31	Preparación de los sistemas virtuales para IDM	1	05/10/2024	05/10/2024	26
32	Instalación de la solución IDM	1	06/10/2024	06/10/2024	31
33	Creación de los usuarios administradores y operadores de la plataforma	2	07/10/2024	08/10/2024	32
34	Documentación de la plataforma IDM implementada	1	09/10/2024	09/10/2024	33
35	Sprint 08 - Ejecución de pruebas de remediación	18	10/10/2024	30/10/2024	26,30
36	Creación de planes de remediación	7	10/10/2024	16/10/2024	26,30
37	Ejecución de planes de remediación	10	17/10/2024	26/10/2024	36

38	Documentación de resultados de los planes en el software de reportes	3	27/10/2024	30/10/2024	37

Elaboración propia

4.2 Presentación de datos

Se revela los valores de la Pre-Prueba y la Post-Prueba de cada uno de los 5 indicadores logrados en el análisis:

Tabla 10:

Valores de indicadores

	Indicador 01 Tiempo		Indicador 02 Costo		Indicador 03 Complejidad		Indicador 04 Cumplimiento		Indicador 05 Impacto	
Nro	PrePrueba	PostPrueba	PrePrueba	PostPrueba	PrePrueba	PostPrueba	PrePrueba	PostPrueba	PrePrueba	PostPrueba
1	61	47	2100	1700	79	41	29	38	62	41
2	69	56	2000	1700	72	45	44	66	89	66
3	57	48	2600	2300	61	31	29	43	83	62
4	60	47	2900	2500	66	41	30	44	79	52
5	71	60	2300	2000	76	46	41	60	85	58

6	61	46	2900	2500	69	43	25	36	86	59
7	53	40	2100	1700	78	53	42	63	81	60
8	67	57	2700	2400	70	41	32	44	69	46
9	50	40	2700	2300	77	52	34	49	87	62
10	72	56	2800	2300	62	40	43	60	87	61
11	76	58	2200	1800	79	45	41	54	84	60
12	67	50	1900	1600	78	54	38	56	68	46
13	60	45	3400	2800	76	46	43	59	80	54
14	74	56	3300	2900	76	51	34	49	65	47
15	80	61	2300	1900	70	36	38	55	83	58
16	62	49	1900	1600	72	39	38	54	80	53
17	78	66	2700	2300	79	44	33	45	66	46
18	56	45	2900	2400	71	36	26	35	62	44
19	55	43	2500	2300	76	44	45	67	70	49
20	62	52	2100	1700	65	44	35	47	72	48
21	59	46	3200	2800	80	40	35	49	87	65

22	66	55	3300	2800	65	34	40	59	74	53
23	56	48	1900	1700	64	42	40	54	75	55
24	65	53	2600	2100	73	45	43	60	84	58
25	78	59	2300	2000	73	39	26	34	77	52
26	77	65	2800	2400	70	43	34	48	64	48
27	77	65	3300	2700	74	45	36	47	73	53
28	77	62	2600	2300	80	46	41	55	71	51
29	51	39	2600	2200	72	50	35	53	64	45
30	80	66	3400	3100	70	41	28	39	66	47

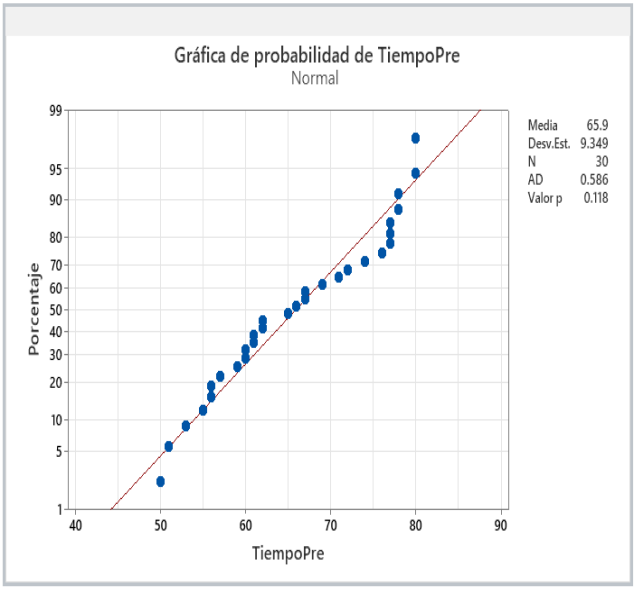
Fuente: Elaboración propia

4.3 Pruebas de normalidad

Efectuamos la prueba de normalidad a los cinco indicadores para comprobar si se debía emplear pruebas de hipótesis paramétricas o no paramétricas.

Tabla 11:

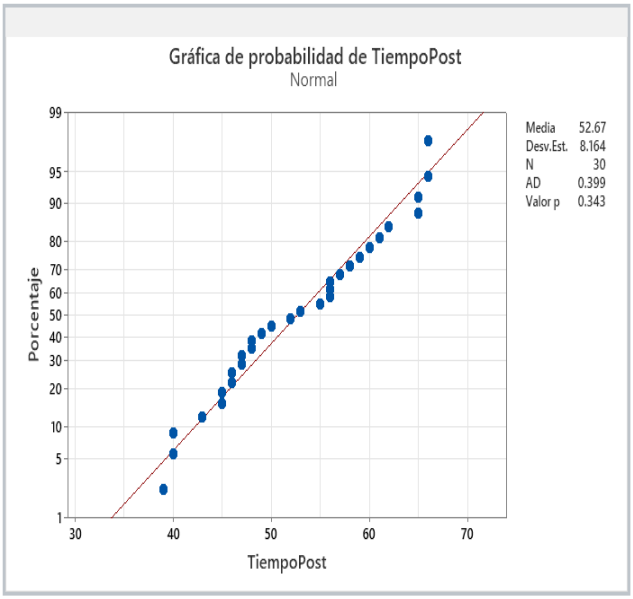
Pruebas de normalidad

Indicador	Prueba de normalidad	Conclusión
Indicador 01: Pre-Prueba Tiempo		El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.118), que el indicador tiempo de la Pre-Prueba **si presenta una distribución normal.**

Indicador 01:

Post-Prueba

Tiempo

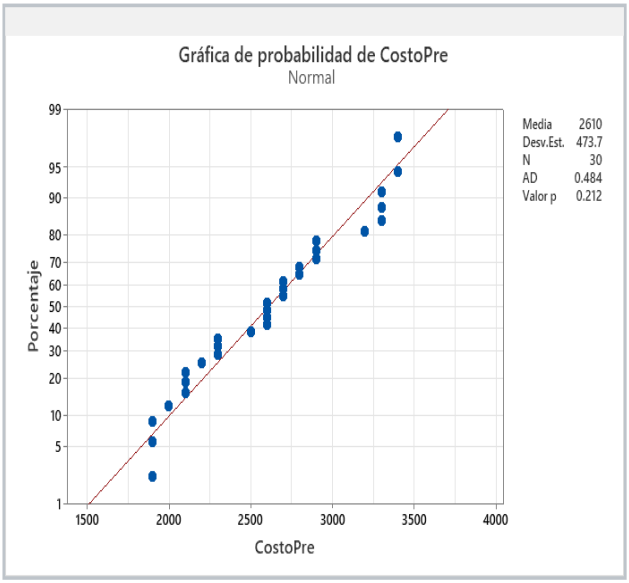


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.343), que el indicador tiempo de la Post-Prueba **si presenta una distribución normal.**

Indicador 02:

Pre-Prueba

Costo

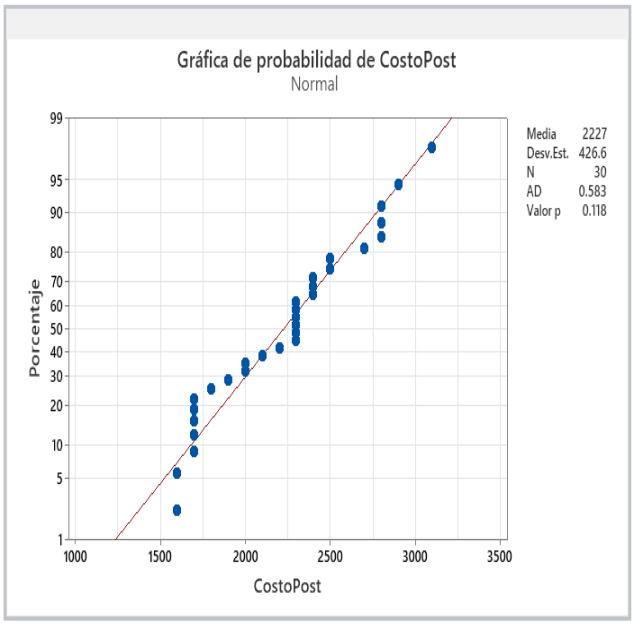


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.212), que el indicador costo de la Pre-Prueba **si presenta una distribución normal.**

Indicador 02:

Post-Prueba

Costo

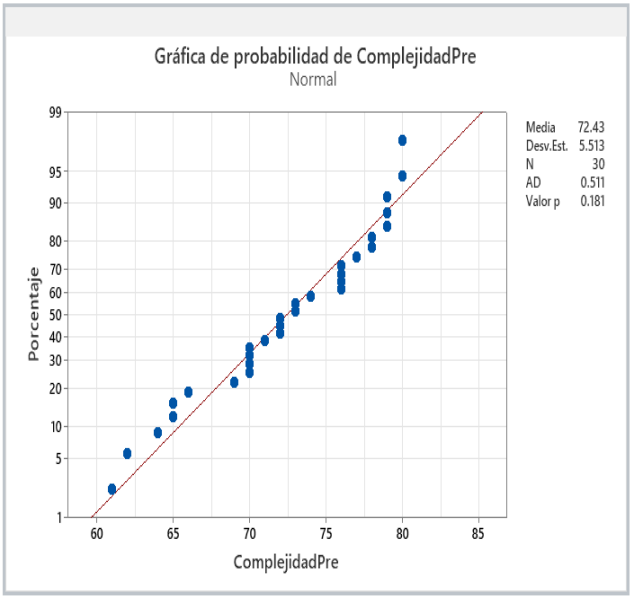


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.118), que el indicador costo de la Post-Prueba **si presenta una distribución normal.**

Indicador 03:

Pre-Prueba

Complejidad

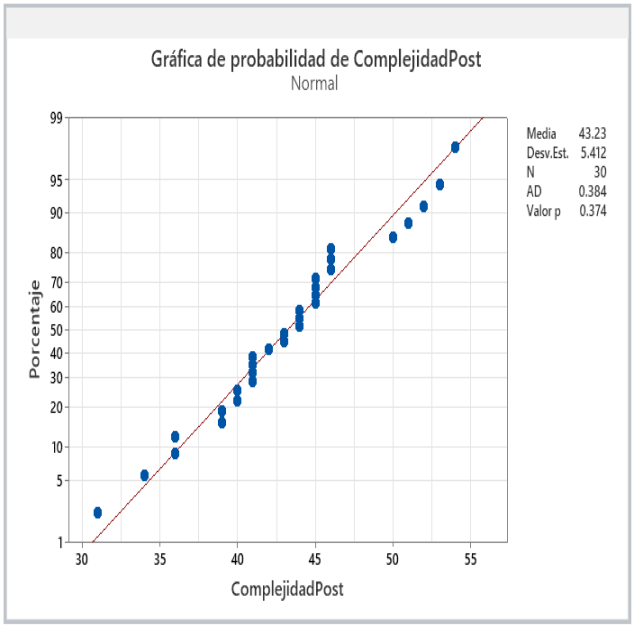


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0181), que el indicador complejidad de la Pre-Prueba **si presenta una distribución normal.**

Indicador 03:

Post-Prueba

Complejidad

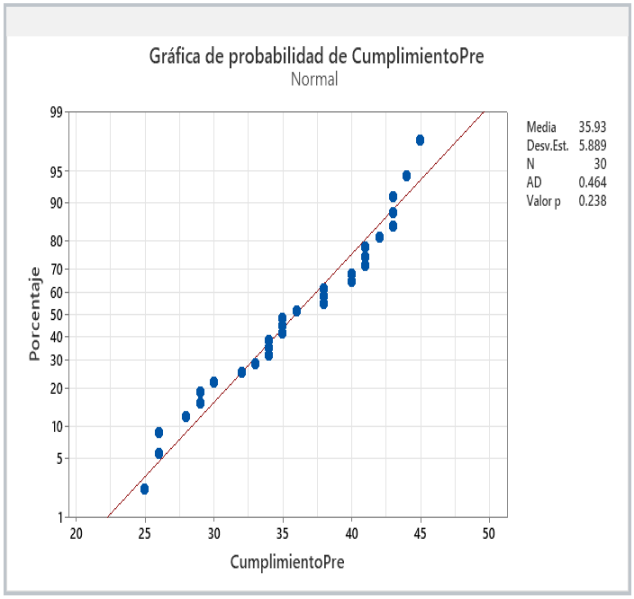


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.374), que el indicador complejidad de la Post-Prueba **si presenta una distribución normal.**

Indicador 04:

Pre-Prueba

Cumplimiento

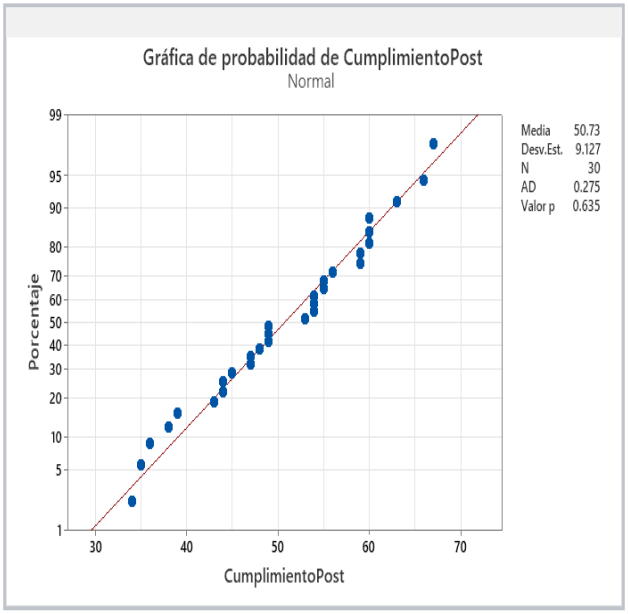


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.238), que el indicador cumplimiento de la Pre-Prueba **si presenta una distribución normal.**

Indicador 04:

Post-Prueba

Cumplimiento

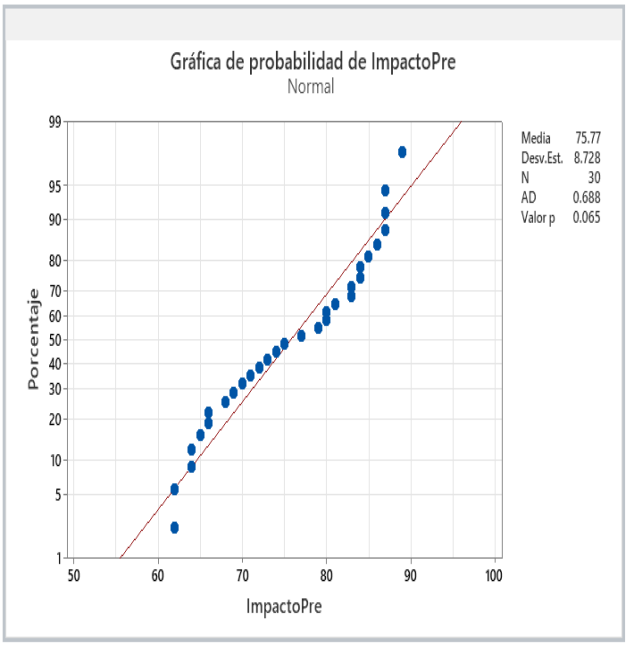


El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.635), que el indicador cumplimiento de la Post-Prueba **si presenta una distribución normal.**

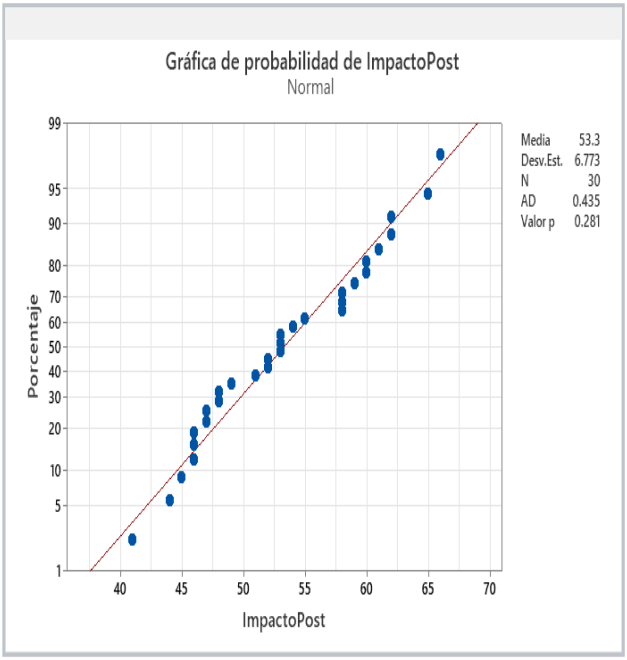
Indicador 05:

Pre-Prueba

Impacto



El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.065), que el indicador impacto de la Pre-Prueba **si presenta una distribución normal.**

Indicador 05: Post-Prueba Impacto		El resultado de la prueba de Anderson-Darling determina por el valor de p (p>0.05;p=0.281), que el indicador impacto de la Post-Prueba **si presenta una distribución normal.**

Fuente: Elaboración propia

4.4 Contrastación de hipótesis

En todos los casos, se aprobaron los criterios de normalidad; por lo tanto, se efectuó la prueba t de Student para dos muestras vinculadas en la prueba de hipótesis.

Hipótesis específica 01: Indicador de tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales:

Ha: La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

Ho: La aplicación del modelo propuesto para la automatización de controles de seguridad no contribuirá a reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

μ1 = Media del indicador tiempo en la PrePrueba

μ2 = Media del indicador tiempo en la PostPrueba

Ha: μ1 > μ2

Ho: μ1 <= μ2

Tabla 12

Prueba estadística t-student del indicador tiempo

	Pre-Prueba	Post-Prueba
Media	65.90	52.67
Desviación Estándar	9.35	8.16
Observaciones (n)	30	

Valor t	5.84
Valor p	0.000

Fuente: Elaboración propia

Puesto que el valor-p < 0.05, los resultados otorgan la adecuada evidencia para negar la hipótesis nula (Ho), por lo tanto, la hipótesis alterna (Ha) es cierta.

Hipótesis específica 02: Indicador de costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales:

Ha: La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

Ho: La aplicación del modelo propuesto para la automatización de controles de seguridad no contribuirá a disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

$\mu 1$ = Media del indicador costo en la PrePrueba

$\mu 2$ = Media del indicador costo en la PostPrueba

Ha: $\mu 1 > \mu 2$

Ho: $\mu 1 <= \mu 2$

Tabla 13

Prueba estadística t-student del indicador costo

	Pre-Prueba	Post-Prueba
Media	2610	2227
Desviación Estándar	474	427
Observaciones (n)	30	
Valor t	3.29	
Valor p	0.001	

Fuente: Elaboración propia

Puesto que el valor-p < 0.05, los resultados otorgan la adecuada evidencia para negar la hipótesis nula (Ho), por lo tanto, la hipótesis alterna (Ha) es cierta.

Hipótesis específica 03: Indicador de complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales:

Ha: La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

Ho: La aplicación del modelo propuesto para la automatización de controles de seguridad no contribuirá a reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

$\mu 1$ = Media del indicador complejidad en la PrePrueba

$\mu 2$ = Media del indicador complejidad en la PostPrueba

Ha: $\mu 1 > \mu 2$

Ho: $\mu 1 <= \mu 2$

Tabla 14

Prueba estadística t-student del indicador complejidad

	Pre-Prueba	Post-Prueba
Media	72.43	43.23
Desviación Estándar	5.51	5.41
Observaciones (n)	30	
Valor t	20.70	
Valor p	0.000	

Fuente: Elaboración propia

Puesto que el valor-p < 0.05, los resultados otorgan la adecuada evidencia para negar la hipótesis nula (Ho), por lo tanto, la hipótesis alterna (Ha) es cierta.

Hipótesis específica 04: Indicador de cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales:

Ha: La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

Ho: La aplicación del modelo propuesto para la automatización de controles de seguridad no contribuirá a aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

$\mu 1$ = Media del indicador cumplimiento en la PrePrueba

$\mu 2$ = Media del indicador cumplimiento en la PostPrueba

Ha: $\mu 1 < \mu 2$

Ho: $\mu 1 >= \mu 2$

Tabla 15

Prueba estadística t-student del indicador cumplimiento

	Pre-Prueba	Post-Prueba
Media	35.93	50.73
Desviación Estándar	5.89	9.13
Observaciones (n)	30	
Valor t	-7.46	
Valor p	0.00	

Fuente: Elaboración propia

Puesto que el valor-p < 0.05, los resultados otorgan la adecuada evidencia para negar la hipótesis nula (Ho), por lo tanto, la hipótesis alterna (Ha) es cierta.

Hipótesis específica 05: Indicador de impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales:

Ha: La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

Ho: La aplicación del modelo propuesto para la automatización de controles de seguridad no contribuirá a minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales.

$\mu 1$ = Media del indicador impacto en la PrePrueba

$\mu 2$ = Media del indicador impacto en la PostPrueba

Ha: $\mu 1 > \mu 2$

Ho: $\mu 1 <= \mu 2$

Tabla 16

Prueba estadística t-student del indicador impacto

	Pre-Prueba	Post-Prueba
Media	75.77	53.30
Desviación Estándar	8.73	6.77
Observaciones (n)	30	
Valor t	11.14	
Valor p	0.000	

Fuente: Elaboración propia

Puesto que el valor-p < 0.05, los resultados otorgan la adecuada evidencia para negar la hipótesis nula (Ho), por lo tanto, la hipótesis alterna (Ha) es cierta.

En consecuencia, al aceptar las cinco hipótesis específicas, se acepta la hipótesis general que indica que la ejecución del modelo expuesto para la automatización de controles de seguridad cooperará a potenciar la fase de remediación de vulnerabilidades en sistemas operativos empresariales.

4.5 Interpretación de los resultados

Con el objetivo de interpretar los resultados estadísticos presentados en las secciones anteriores, es esencial contrastarlos con las metas establecidas en la fase investigativa y constatar su ejecución en función de cada uno de los indicadores e hipótesis fijadas.

Tabla 17

Interpretación de resultados de los indicadores de investigación

N°	Pre Prueba	Post Prueba	Existe mejora	Porcentaje de mejora	Unidades de mejora	Interpretación
Indicador tiempo						
1	61	47	SI	22.95	14	El 100%de los casos de la PostPrueba son mejores que la PrePrueba.
2	69	56	SI	18.84	13	
3	57	48	SI	15.79	9	
4	60	47	SI	21.67	13	
5	71	60	SI	15.49	11	
6	61	46	SI	24.59	15	El indicador tiempo de los casos de la PostPrueba con respecto a la PrePrueba mejoro en un promedio de 20.15%.
7	53	40	SI	24.53	13	
8	67	57	SI	14.93	10	
9	50	40	SI	20.00	10	
10	72	56	SI	22.22	16	
11	76	58	SI	23.68	18	
12	67	50	SI	25.37	17	
13	60	45	SI	25.00	15	El indicador tiempo de los casos de la PostPrueba con
14	74	56	SI	24.32	18	
15	80	61	SI	23.75	19	

16	62	49	SI	20.97	13	respecto a la PrePrueba
17	78	66	SI	15.38	12	mejoro en un promedio
18	56	45	SI	19.64	11	de 13.23 horas.
19	55	43	SI	21.82	12	
20	62	52	SI	16.13	10	El 80.00% de los casos
21	59	46	SI	22.03	13	de la PostPrueba
22	66	55	SI	16.67	11	superan la meta
23	56	48	SI	14.29	8	propuesta en la presente
24	65	53	SI	18.46	12	investigación (60)
25	78	59	SI	24.36	19	indicadas en la Tabla 2.
26	77	65	SI	15.58	12	
27	77	65	SI	15.58	12	
28	77	62	SI	19.48	15	
29	51	39	SI	23.53	12	
30	80	66	SI	17.50	14	
				Indicador costo		
1	2100	1700	SI	19.05	400	El 100%de los casos de
2	2000	1700	SI	15.00	300	la PostPrueba son
3	2600	2300	SI	11.54	300	mejores que la
4	2900	2500	SI	13.79	400	PrePrueba.
5	2300	2000	SI	13.04	300	
6	2900	2500	SI	13.79	400	
7	2100	1700	SI	19.05	400	El indicador costo de
8	2700	2400	SI	11.11	300	los casos de la

9	2700	2300	SI	14.81	400	PostPrueba con respecto a la PrePrueba mejoro en un promedio de 14.79%.
10	2800	2300	SI	17.86	500	
11	2200	1800	SI	18.18	400	
12	1900	1600	SI	15.79	300	
13	3400	2800	SI	17.65	600	
14	3300	2900	SI	12.12	400	
15	2300	1900	SI	17.39	400	El indicador costo de los casos de la PostPrueba con respecto a la PrePrueba mejoro en un promedio de 383.33 soles.
16	1900	1600	SI	15.79	300	
17	2700	2300	SI	14.81	400	
18	2900	2400	SI	17.24	500	
19	2500	2300	SI	8.00	200	
20	2100	1700	SI	19.05	400	
21	3200	2800	SI	12.50	400	El 80.00% de los casos de la PostPrueba superan la meta propuesta en la presente investigación (2500) indicadas en la Tabla 2.
22	3300	2800	SI	15.15	500	
23	1900	1700	SI	10.53	200	
24	2600	2100	SI	19.23	500	
25	2300	2000	SI	13.04	300	
26	2800	2400	SI	14.29	400	
27	3300	2700	SI	18.18	600	
28	2600	2300	SI	11.54	300	
29	2600	2200	SI	15.38	400	
30	3400	3100	SI	8.82	300	
Indicador complejidad						
1	79	41	SI	48.10	38	

2	72	45	SI	37.50	27	El 100%de los casos de la PostPrueba son mejores que la PrePrueba.
3	61	31	SI	49.18	30	
4	66	41	SI	37.88	25	
5	76	46	SI	39.47	30	
6	69	43	SI	37.68	26	
7	78	53	SI	32.05	25	
8	70	41	SI	41.43	29	El indicador complejidad de los casos de la PostPrueba con respecto a la PrePrueba mejoro en un promedio de 40.30%.
9	77	52	SI	32.47	25	
10	62	40	SI	35.48	22	
11	79	45	SI	43.04	34	
12	78	54	SI	30.77	24	
13	76	46	SI	39.47	30	
14	76	51	SI	32.89	25	
15	70	36	SI	48.57	34	
16	72	39	SI	45.83	33	El indicador complejidad de los casos de la PostPrueba con respecto a la PrePrueba mejoro en un promedio de 29.20 unidades.
17	79	44	SI	44.30	35	
18	71	36	SI	49.30	35	
19	76	44	SI	42.11	32	
20	65	44	SI	32.31	21	
21	80	40	SI	50.00	40	
22	65	34	SI	47.69	31	
23	64	42	SI	34.38	22	
24	73	45	SI	38.36	28	El 83.33% de los casos
25	73	39	SI	46.58	34	

26	70	43	SI	38.57	27	de la PostPrueba
27	74	45	SI	39.19	29	superan la meta
28	80	46	SI	42.50	34	propuesta en la presente
29	72	50	SI	30.56	22	investigación (48)
30	70	41	SI	41.43	29	indicadas en la Tabla 2.
Indicador cumplimiento						
1	29	38	SI	31.03	9	El 100%de los casos de
2	44	66	SI	50.00	22	la PostPrueba son
3	29	43	SI	48.28	14	mejores que la
4	30	44	SI	46.67	14	PrePrueba.
5	41	60	SI	46.34	19	
6	25	36	SI	44.00	11	
7	42	63	SI	50.00	21	El indicador
8	32	44	SI	37.50	12	cumplimiento de los
9	34	49	SI	44.12	15	casos de la PostPrueba
10	43	60	SI	39.53	17	con respecto a la
11	41	54	SI	31.71	13	PrePrueba mejoro en un
12	38	56	SI	47.37	18	promedio de 40.94%.
13	43	59	SI	37.21	16	
14	34	49	SI	44.12	15	
15	38	55	SI	44.74	17	El indicador
16	38	54	SI	42.11	16	cumplimiento de los
17	33	45	SI	36.36	12	casos de la PostPrueba
18	26	35	SI	34.62	9	con respecto a la

19	45	67	SI	48.89	22	PrePrueba mejoro en un promedio de 14.80 unidades.
20	35	47	SI	34.29	12	
21	35	49	SI	40.00	14	
22	40	59	SI	47.50	19	
23	40	54	SI	35.00	14	
24	43	60	SI	39.53	17	El 83.33% de los casos de la PostPrueba superan la meta propuesta en la presente investigación (40) indicadas en la Tabla 2.
25	26	34	SI	30.77	8	
26	34	48	SI	41.18	14	
27	36	47	SI	30.56	11	
28	41	55	SI	34.15	14	
29	35	53	SI	51.43	18	
30	28	39	SI	39.29	11	
Indicador impacto						
1	62	41	SI	33.87	21	El 100%de los casos de la PostPrueba son mejores que la PrePrueba.
2	89	66	SI	25.84	23	
3	83	62	SI	25.30	21	
4	79	52	SI	34.18	27	
5	85	58	SI	31.76	27	
6	86	59	SI	31.40	27	El indicador impacto de los casos de la PostPrueba con respecto a la PrePrueba mejoro en un promedio de 29.69%.
7	81	60	SI	25.93	21	
8	69	46	SI	33.33	23	
9	87	62	SI	28.74	25	
10	87	61	SI	29.89	26	
11	84	60	SI	28.57	24	

12	68	46	SI	32.35	22	
13	80	54	SI	32.50	26	El indicador impacto de los casos de la PostPrueba con respecto a la PrePrueba mejoro en un promedio de 22.47 unidades.
14	65	47	SI	27.69	18	
15	83	58	SI	30.12	25	
16	80	53	SI	33.75	27	
17	66	46	SI	30.30	20	
18	62	44	SI	29.03	18	
19	70	49	SI	30.00	21	
20	72	48	SI	33.33	24	
21	87	65	SI	25.29	22	El 83.33% de los casos de la PostPrueba superan la meta propuesta en la presente investigación (60) indicadas en la Tabla 2.
22	74	53	SI	28.38	21	
23	75	55	SI	26.67	20	
24	84	58	SI	30.95	26	
25	77	52	SI	32.47	25	
26	64	48	SI	25.00	16	
27	73	53	SI	27.40	20	
28	71	51	SI	28.17	20	
29	64	45	SI	29.69	19	
30	66	47	SI	28.79	19	

Fuente: Elaboración propia

V. DISCUSIÓN DE RESULTADOS

a) En los análisis de Banchof (2019), Castro (2020) y Khumaidi (2021) se gestionan proyectos aplicando las metodologías agiles, siendo orientados solo al desarrollo de software, dejando para el resto del proyecto el enfoque tradicional. En este punto, la presente investigación mejora la gestión del proyecto al aplicar el enfoque ágil Scrum y las herramientas de DevOps a todo el proyecto al dividirlo en Sprints por cada una de las soluciones tecnológicas que componen al modelo completo.

b) Las investigaciones de Caiza (2019), Gabarrín (2019), Sasidharan (2022) y Yanqui (2023) resaltan la necesidad de aplicar controles de seguridad, lineamientos, afinamientos y buenas prácticas en los sistemas operativos empresariales, tomando cada sistema o versión como un proyecto independiente, en este punto, la presente investigación mejora la aplicabilidad de los lineamientos de sistemas operativos al estandarizar los controles en una solución integral capaz de aplicarlos a todos los sistemas a través de un sistema de automatización.

c) Las investigaciones de Fandiño (2019) y Torchio (2022) aplican de forma exitosa la solución de OpenScap para la aplicaciones de controles de seguridad, sin embargo, estos controles no cuentan con una administración centralizada y por lo tanto no se tiene visibilidad a lo largo de tiempo, en este aspecto, la presente investigación facilita la gestión y control de versiones de openscap al entregar una solución de reportes integrada a la automatización de openscap para su correcta administración de cara a la mejora sucesiva de procesos.

d) En la investigación de Giraldo (2022) se busca la implementación de un marco de referencia con enfoque a la aplicabilidad de controles de seguridad, cumpliendo de forma exitosa el objetivo planteado, pero dejando de lado muchos aspectos de mejora como cumplir parámetros de disponibilidad, escalabilidad, portabilidad y recuperación

ante desastres, en estos puntos, la presente investigación entrega un modelo que cumple todo ello a través de soluciones de código abierto.

e) Las investigaciones de Ramírez (2019), Mera-Aguilar et at. (2020), Payá-Cotarelo et at. (2022) y Rodríguez y Cedeño (2022) aplican diferentes controles de seguridad, siendo los más importantes los de PCI y CIS, en este sentido aplican lo mejor en la industria, pero sin dejar espacio para la custonización de dichos controles, ya que estos podrían a llegar a ser muy restrictivos al momento de certificar los sistemas clientes, en este punto, el presente modelo, permite customizar los controles basados en PCI y CIS para flexibilizar su aplicación en situaciones de emergencia o durante las fases de desarrollo o pre-producción.

f) La investigación de Likitha (2022) presenta una herramienta de automatización, la cual cumple con los objetivos planteados facilitando la ejecución de operaciones, en este punto, el presente modelo, no solo presenta una herramienta de automatización, sino una plataforma integral con modulo especializados y transversal a cualquier sistema operativo empresarial, es decir, no solo se aplica a servidores Linux, sino también a servidores Windows, switches de diferentes marcas, firewalls, aplicaciones web, entre otros, lo cual prepara a la plataforma para extender su alcance a futuro.

VI. CONCLUSIONES

a) El proceso de remediación de vulnerabilidades en sistemas operativos empresariales mejora en un promedio del 23.11% con la ejecución del modelo expuesto para la automatización de controles de seguridad.

b) El indicador de tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales mejora en un promedio del 20.15% con la ejecución del modelo expuesto para la automatización de controles de seguridad.

c) El indicador de costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales mejora en un promedio del 14.79% con la ejecución del modelo expuesto para la automatización de controles de seguridad.

d) El indicador de complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales mejora en un promedio del 40.30% con la ejecución del modelo expuesto para la automatización de controles de seguridad.

e) El indicador de cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales mejora en un promedio del 40.94% con la ejecución del modelo expuesto para la automatización de controles de seguridad.

f) El indicador de impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales mejora en un promedio del 29.69% con la ejecución del modelo expuesto para la automatización de controles de seguridad.

VII. RECOMENDACIONES

a) A fin de mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales puede extender su alcance al agregar nuevos lineamientos, pero orientado a aplicaciones, siendo necesario agregar nuevas capas al modelo de implementación para que soporte nuevos programas que permitan verificar a nivel de middleware, servicios web, bases de datos, firewall perimetral, equipos de comunicaciones, entre otros dispositivos que requieran ser evaluados antes de prestar servicios en producción.

b) El indicador de tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales puede mejorar si se reduce la necesidad de la actualización continua de controles de seguridad a través de una plataforma de interoperabilidad que conecte la plataforma implementada con un repositorio de lineamientos actualizados por el fabricante, siendo solo trabajo del especialista de seguridad aprobar dichas actualizaciones para incluirla en su ciclo de revisiones.

c) El indicador de costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales puede mejorar al reutilizar plataformas basadas en nube, ya que estas plataformas se basan en el consumo, por ello, se optimiza el uso de recursos a través de proveedor que se encargue de mantener los niveles de servicios definidos por la empresa, dejando de lado la necesidad local de mantener la plataforma a invel de infraestructura.

d) El indicador de complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales puede mejorar con el uso de soluciones basada en contenedores, preparando la infraestructura para los microservicios, lo cual reduce la complejidad para actualizar la plataforma o para extender las funcionalidades con nuevas versiones o releases.

e) El indicador de cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales puede mejorar al incluir mayor cantidad de estándares, en la presente investigación se usa los PCI y CIS, sin embargo, están puede extenderse usando otras normativas como GDPR, FedRAMP, NIST y SANS, entre otras.

f) El indicador de impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales puede mejorar extendiendo las funcionalidades de la automatización como respuesta a ciertos controles verificados y automatizando las remediaciones, mitigando el impacto de cada vulnerabilidad con remediaciones que no afecten a las aplicaciones implementadas.

VIII. REFERENCIAS

Alvarez, A., & Gomez, L. (2012). *Guía de aplicación de la Norma UNE-ISO-IEC 27001 sobre seguridad en sistemas de información para Pymes* (1 ed.). AENOR Internacional.

Alvarez, J. (2026). *Ley y Reglamento de Contrataciones Públicas* (1 ed.). Alvarez & Llosa Editores y Consultores.

Amazon Web Services [AWS]. (15 de 04 de 2024). *¿En qué consisten los puntos de referencia del CIS?* Obtenido de https://aws.amazon.com/es/what-is/cis-benchmarks/

Amazon Web Services [AWS]. (02 de 01 de 2024). *OpenSCAP on AWS*. Obtenido de https://icfi.github.io/openscap-aws/docs.html

Ansible. (01 de 07 de 2023). *Automation for everyone*. Obtenido de https://www.ansible.com/

Ardila, C., & Daza, J. (2020). *Verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado.* [Tesis de titulación, Universidad Católica de Colombia]. https://repository.ucatolica.edu.co/entities/publication/b4f480d5-45b7-4d38-a0fb-a24f8e85df01

Atalaya, C. (2023). *Modelo de ciberseguridad en universidades privadas en el Perú.* [Tesis doctoral, Universidad Nacional de Piura]. https://repositorio.unp.edu.pe/items/160a3f6b-0785-4f9f-8423-97a51014d309

Atef, G. (2025). *Linux Hardening Made Easy: Automate Security with Ansible and OpenSCAP* (1a ed.). Independently Published.

Banchoff, M. (2019). *Infraestructura como Cóodigo Caso de estudio: Cientópolis.* [Tesis de maestría, Universidad Nacional de La Plata]. https://sedici.unlp.edu.ar/handle/10915/86142

Burnashev, R. (2024). *Análisis filosófico de la seguridad de la información personal: En la sociedad de la información monográfico* (1a ed.). Nuestro Conocimiento.

Caiza, A. (2019). *Diseño de un proceso de Hardening de servidores para una institución financiera del sector público.* [Tesis de grado, Universidad Internacional SEK]. https://repositorio.uisek.edu.ec/handle/123456789/3346

Castro, J. (2020). DevSecOps: Implementación de seguridad en DevOps a través de herramientas open source. [Tesis de maestría, Universidad Abierta de Cataluña]. https://openaccess.uoc.edu/handle/10609/126766?locale=es

Castro, S. (2012). *Los 27 Controles Criticos de Seguridad Informatica: Una Guía Práctica para Gerentes y Consultores de Seguridad Informática* (1 ed.). CreateSpace Independent Publishing Platform.

Centro de Seguridad en Internet [CIS]. (10 de 02 de 2024). *How to Get Up and Running with CIS WorkBench*. https://www.cisecurity.org/insights/blog/how-to-get-up-and-running-with-cis-workbench

Chávez, E. (2023). *Catalizadores cobit 5 (control para tecnologías de información o relacionadas) y seguridad de la información en la empresa datco S&H, Huaraz, 2020*. [Tesis doctoral, Universidad Nacional Santiago Antúnez de Mayolo]. http://repositorio.unasam.edu.pe/handle/UNASAM/5653

Comisión Económica para América Latina y el Caribe [CEPAL]. (01 de 05 de 2023). *Comisión Económica para América Latina y el Caribe*. Obtenido de Agenda 2030 y los Objetivos de Desarrollo Sostenible : una oportunidad para América Latina y el Caribe [CEPAL]: https://repositorio.minedu.gob.pe/handle/20.500.12799/4559

Comte, A. (2012). *Curso de filosofía positiva. Discurso espíritu positivo* (1a ed.). Claridad.

Edwards, J. (2024). *Critical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls* (1a ed.). Apress.

Fandiño, J. (2019). *Cumplimiento del Esquema Nacional de Seguridad en servidores CentOS 7 con OpenSCAP.* [Tesis de maestría, Universidad Abierta de Cataluña]. https://openaccess.uoc.edu/handle/10609/107667

Fortra. (27 de 07 de 2022). *Gestión de vulnerabilidades: qué es, procesos y buenas prácticas*. Obtenido de https://www.fortra.com/es/blog/gestion-vulnerabilidades

Gabarrín, G. (2019). Integración y automatización de seguridad en procesos de desarrollo de metodologías ágiles. [Tesis de maestría, Universidad de la República, Montevideo, Uruguay]. https://www.colibri.udelar.edu.uy/jspui/handle/20.500.12008/23971

Giraldo, J. (2022). *Herramienta de Ciberseguridad para la auditoría de una línea base de buenas prácticas de seguridad informática en Pymes a través de un prototipo funcional de Chatbot que ofrezca recomendaciones para la mitigación de vulnerabilidades en servidores Windows.* [Tesis de maestría, Institución Universitaria ITM]. https://repositorio.itm.edu.co/handle/20.500.12622/5748

GitLab. (02 de 05 de 2023). *GitLab architecture overview*. Obtenido de https://docs.gitlab.com/ee/development/architecture.html

Goldman, D. (04 de 05 de 2024). *What is Security Compliance?* Panorays. https://panorays.com/blog/what-is-security-compliance/

Gomez, Á. (2011). *Enciclopedia de la Seguridad Informática.* (2 ed.). Ra-Ma.

Hernández, D. (2023). *Investigación policial de la ciberdelincuencia y capacidad de respuesta de la policía nacional en materia de formación y capacitación a través del proyecto c1b3rwall.* [Tesis doctoral, Universidad de Salamanca]. https://portalinvestigacion.uniovi.es/documentos/668448d75ca6d336e9647970

Hogg RV, C. A. (1978). *Introduction to Mathematical Statistics* (4a ed.). Macmillan.

Instituto Nacional de Estándares y Tecnología [NIST]. (01 de 03 de 2024). *Computer Security Resource Center*. Obtenido de https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe

Kennedy, D., Aharoni, M., Kearns, D., O'gorman, J., & Graham, D. (2025). *Metasploit. Análisis de vulnerabilidades y detección de intrusiones* (1a ed.). Alpha Editorial.

Khumaidi, A. (2021). Implementation of devops method for automation of server management using Ansible. *Transformatika, 18*(2), 199-209. https://journals.usm.ac.id/index.php/transformatika/article/view/2447

Lenovo. (21 de 04 de 2024). *¿Qué es Linux?* https://www.lenovo.com/pe/es/faqs/sistemas-operativos/

Likitha, S. (2022). Automation of Server Configuration Using Ansible. *International Journal for Research in Applied Science and Engineering Technology, 10*(6), 4109–4113. https://doi.org/10.22214/ijraset.2022.44840

Lloredo, L. (2012). *Rudolf von Jhering y el paradigma positivista.* Editorial Dykinson.

Meijer, B., Hochstein, L., & Moser, R. (2017). *Ansible: Up and Running: Automating Configuration Management and Deployment the Easy Way* (2a ed.). O'Reilly Media.

Mera, C., Aguilar, I., & Vera, D. (2020). Herramienta de Software para la automatización de la construcción del catálogo de servicios de tecnologías de la información. *Revista Ibérica de Sistemas y Tecnologías de la Información, 37*(11), 14-27. https://repositorioslatinoamericanos.uchile.cl/handle/2250/6595107?show=full

OpenScap. (20 de 04 de 2024). *OpenScap audit, fix and merry*. Obtenido de https://www.open-scap.org/

Organización Internacional de Normalización [ISO]. (15 de 01 de 2024). *ISO/IEC 27001:2022*. Obtenido de https://www.iso.org/standard/27001

Ortego, M. (2025). *Manual de privacidad, protección de datos y ciberseguridad* (2a ed.). Tirant Lo Blanch.

Payá, A., Cotarelo, A., & Redondo, J. (2022). Automated security configuration deployment systems with early error detection. *Computers and Security, 116*, 102638. https://doi.org/10.1016/j.cose.2022.102638

Ramírez, J. (2019). *Implementación de lineamientos base de seguridad en bases de datos Oracle y SQL Server en una entidad bancaria.* [Tesis de grado, Universidad San Ignacio de Loyola]. https://hdl.handle.net/20.500.14005/9155

RedHat. (01 de 05 de 2023). *La automatización*. Obtenido de https://www.redhat.com/es/topics/automation

RedHat. (01 de 04 de 2023). *Red Hat Ansible Automation Platform*. Obtenido de https://www.redhat.com/en/technologies/management/ansible

Renales, R. (2024). *Marco de Ciberseguridad NIST 2.0: Guía Integral para la Gestión de Riesgos en la Era Digital* (1 ed.). Amazon Kindle.

Rivera, J., & Cervantes, L. (2014). *Perú 2030. Educación para el desarrollo sostenible* (1a ed.). Universidad Inca Garcilaso de la Vega.

Rodríguez, V., & Cedeño, M. (2022). *Marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación, comercialización y exportación de muebles.* [Tesis de grado, Universidad Internacional SEK]. https://repositorio.uisek.edu.ec/handle/123456789/4676

Sasidharan, R. (2022). A Case Study to Implement Windows System Hardening using CIS Controls. *International Journal of Computer Trends and Technology, 70*(7), 1–7. https://doi.org/10.14445/22312803/ijctt-v70i7p101

Smith, W. (2024). *GitLab Guidebook: From Basics to Expert Proficiency* (1a ed.). HiTeX Press.

Superintendencia Nacional de Educación Superior Universitaria [SUNEDU]. (19 de 05 de 2025). *Plan Estratégico Institucional 2025-2030*. Obtenido de https://repositorio.minedu.gob.pe/handle/20.500.12799/11358

Telang, T. (2020). *Introduction to YAML: Demystifying YAML Data Serialization Format* (2a ed.). Lets Practice Academy.

Torchio, M. (2022). *Security assessment and threat response through SCAP.* [Tesis de maestría, Politécnico de Torino]. https://webthesis.biblio.polito.it/secure/22850/1/tesi.pdf

Yanqui, V. (2023). *Implementación de hardening en sistemas operativos de servidor : implememementación de hardening en sistemas operativos de servidor linux de base debian.* [Tesis de grado, Escuela Politécnica Nacional, Quito, Ecuador]. https://bibdigital.epn.edu.ec/handle/15000/24962

IX. ANEXOS

Anexo A: Matriz de consistencia

Tabla 18:

Matriz de consistencia

Problema general	Ibjetivo general	Hipótesis general	Problemas específicos	Objetivos específicos	Hipótesis específicas	Investigación
¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales?	Mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad	La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a mejorar el proceso de remediación de vulnerabilidades en sistemas operativos empresariales	¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?	Reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad	La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a reducir el tiempo del proceso de remediación de vulnerabilidades en sistemas operativos	Tipo: Básica Nivel: Relacional

	Indicador	Indice	Medida	Jnidad de observació				
Variable independiente	Tiempo	[No...Si]	-	-	¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?	Disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad	La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a disminuir el costo del proceso de remediación de vulnerabilidades en sistemas operativos	Muestra 30 observaciones del proceso Muestreo: Intencionado
	Costo	[1..3500]	horas	Planes de remediación	¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?	Minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad	La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a minimizar el impacto del proceso de remediación de vulnerabilidades en sistemas operativos empresariales	Tecnicas: Entrevistas Observación
Variable dependiente	Riesgo	[1..10000]	Soles	Presupuestos del área de seguridad informática	¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?	Aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad	La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a aumentar el cumplimiento del proceso de remediación de vulnerabilidades en sistemas operativos	Instrumentos: Cuestionarios y entrevistas Guías de observación
	Impacto	[1..100]	unidades	Matriz de riesgos	¿En qué medida, la aplicación del modelo propuesto para la automatización de controles de seguridad contribuye a reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales?	Reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales aplicando el modelo propuesto para la automatización de controles de seguridad	La aplicación del modelo propuesto para la automatización de controles de seguridad contribuirá a reducir la complejidad del proceso de remediación de vulnerabilidades en sistemas operativos empresariales	
	Cumplimiento	[1..100]	unidades	Análisis de vulnerabilidades				
	Complejidad	[1..100]	unidades	Reporte de proveedores				

Anexo B: Validación y confiabilidad de instrumentos

CONSTANCIA DE VALIDACIÓN DE INSTRUMENTOS

Lima, 01 de octubre del 2024

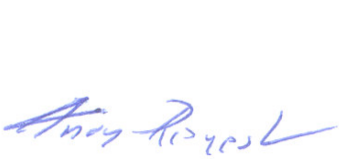
Sres. Escuela Universitaria de Posgrado de la Universidad Nacional Federico Villareal

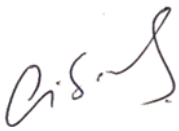
Presente

Reciba un cordial saludo

Quien suscribe como especialista en materia de aplicación de principios, procedimientos, métodos y técnicas de la ciencia estadística y los algoritmos computacionales en el análisis, administración, dirección, supervisión y control de procesos de producción de bienes y/o servicios y procesos de investigación, me complace dirigirme a usted para **dar validación de los instrumentos** que servirán para recolectar información relativa a la investigación denominada: ***Modelo de aseguramiento para la automatización de controles de seguridad basado en estándares abiertos,*** que será presentado para optar al grado de Doctor en Ingeniería de Sistemas por el **Mg. Saavedra Jiménez, Robert Roy**.

Muy Cordialmente,





Andy Reyes Vargas	Wilder Cribillero Cordova	Alejandro Reategui Pezo
DNI: 42296062	DNI: 32858461	DNI: 06182363
Dr. Ingeniería de sistemas	Dr. Ingeniería de sistemas	Dr. Ingeniería de sistemas

CONSTANCIA DE CONFIABILIDAD DE INSTRUMENTOS

Lima 01 de octubre del 2024

Sres. Escuela Universitaria de Posgrado de la Universidad Nacional Federico Villareal

Presente

Quien suscribe como especialista en materia de aplicación de principios, procedimientos, métodos y técnicas de la ciencia estadística y los algoritmos computacionales en el análisis, administración, dirección, supervisión y control de procesos de producción de bienes y/o servicios y procesos de investigación, me complace dirigirme a usted para **aprobar el resultado de la prueba de confiabilidad de los instrumentos** que servirán para recolectar información relativa a la investigación denominada: ***Modelo de aseguramiento para la automatización de controles de seguridad basado en estándares abiertos***, que será presentado para optar al grado de Doctor en Ingeniería de Sistemas por el **Mg. Saavedra Jiménez, Robert Roy**.

Análisis de Confiabilidad

Método: Alfa de Cronbach (S.P.S.S.)

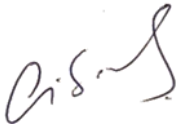
****** Method 1 (space saver) will be used for this analysis ******

RELIABILITY ANALYSIS - SCALE (ALPHA)

Reliability Coefficients

N of Cases = 30,0 N of Items = 20

Alpha = 0.980



Andy Reyes Vargas	Wilder Cribillero Cordova	Alejandro Reategui Pezo
DNI: 42296062	DNI: 32858461	DNI: 06182363
Dr. Ingeniería de sistemas	Dr. Ingeniería de sistemas	Dr. Ingeniería de sistemas

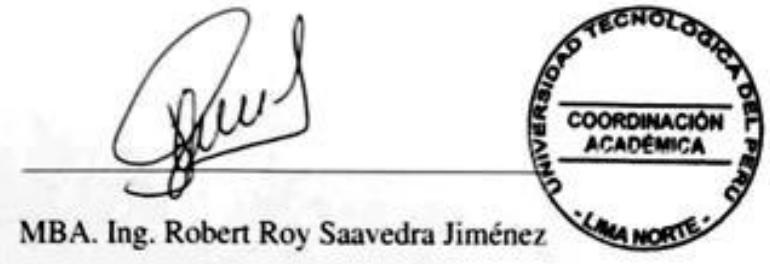
Anexo C: Autorización de investigación

Autorización de investigación

DECLARACIÓN JURADA

Quien suscribe, Robert Roy Saavedra Jiménez con DNI 40832175, bajo la modalidad de contrato indeterminado en la Universidad Tecnológica del Perú bajo el cargo de Coordinador Académico de Ingeniería de Sistemas e Informática, como parte de mis funciones, estoy autorizado a realizar investigaciones en el dominio de tecnologías de la información. La presente investigación de tesis doctoral se realizó a modo de prueba de concepto en una nube contratada por mi persona para estos fines sin manipular ningún servidor corporativo de la UTP, además de no exponer información confidencial de la universidad ni de su infraestructura tecnológica.

Lima, 24 de junio de 2026



MBA. Ing. Robert Roy Saavedra Jiménez

DNI: 40832175| CIP: 104403

Coordinador Académico de Ingeniería de Sistemas e Informática

Gestión Académica Lima Norte

Anexo D: Documentación del modelo propuesto

Como parte del desarrollo y aplicación del modelo, se presentan las fases propuestas y sus respectivas actividades y entregable por cada fase:

Fase 01: Analizases de requerimientos

En esta fase de analiza los requerimientos de infraestructura de los sistemas operativos y aplicaciones que se quieren analizar, remediar y mejorar de forma continua en el modelo propuesto, por ello se debe realizar tener pleno conocimiento de los estándares y lineamientos de referencia usados por las empresas en el dominio de seguridad.

Actividades:

- Identificar cada uno del sistema requeridos en la solución propuesta.
- Documentar los lineamientos y marcos de referencia de seguridad.
- Establecer de forma conceptual los servicios de a implementar.
- Determinar el alcance de las remediaciones propuestas

Entregables:

- Diseño conceptual de la plataforma a implementar.

Fase 02: Diseño e implementación de plataformas tecnológicas

En esta esta se diseña e implementa todos los componentes tecnológicos de las capas del modelo de implementación propuestos, en este punto los diseños son implementados en soluciones de software libre pero los clientes a evaluar podrán ser libre o propietarios.

Actividades

- Diseñar la plataforma general integrada con un diseño de capas.
- Diseñar la plataforma de gestión de identidades IDM.

- Diseñar el repositorio de código GIT.
- Diseñar la plataforma de automatización Ansible.
- Diseñar el componente de balanceo de carga haproxy
- Diseñar la plataforma de gestión de reportes basada en JBoss.
- Implementar las plataformas tecnológicas.

Entregables:

- Diseños de arquitectura de plataformas tecnológicas.
- Manuales de implementación de plataformas tecnológicas.

Fase 03: Análisis de sistemas operativos empresariales

En esta fase se realiza a través de la plataforma de automatización propuesta, el escaneo y análisis de todos los sistemas operativos empresariales que forma parte del alcance del proyecto de remediación de vulnerabilidades. Estos sistemas deberán ser escaneados con algún lineamiento y perfil seleccionado según la criticidad de las aplicaciones primarias implementadas en dichos sistemas.

Actividades:

- Selección de los perfiles de aseguramiento requeridos.
- Registro de inventarios.
- Escaneo de sistemas seleccionados.
- Generación de línea base de aseguramiento.

Entregables:

- Reporte estado de sistemas operativos empresariales.

Fase 04: Mejora continua de plataforma

Esta fase es analiza los reportes generados en la fase anterior, ponderando según su criticidad, impacto, complejidad, entre otros criterios el orden correcto de remediación de las vulnerabilidades encontradas en los sistemas, siendo necesario crear programas de remediación y su posterior aplicación.

Actividades:

- Seleccionar las vulnerabilidades encontradas para el presente ciclo de remediación.
- Programar las tareas de remediación en la plataforma de automatización.
- Validación de la remediación aplicada.
- Definición del alcance del siguiente ciclo de remediación.

Entregables:

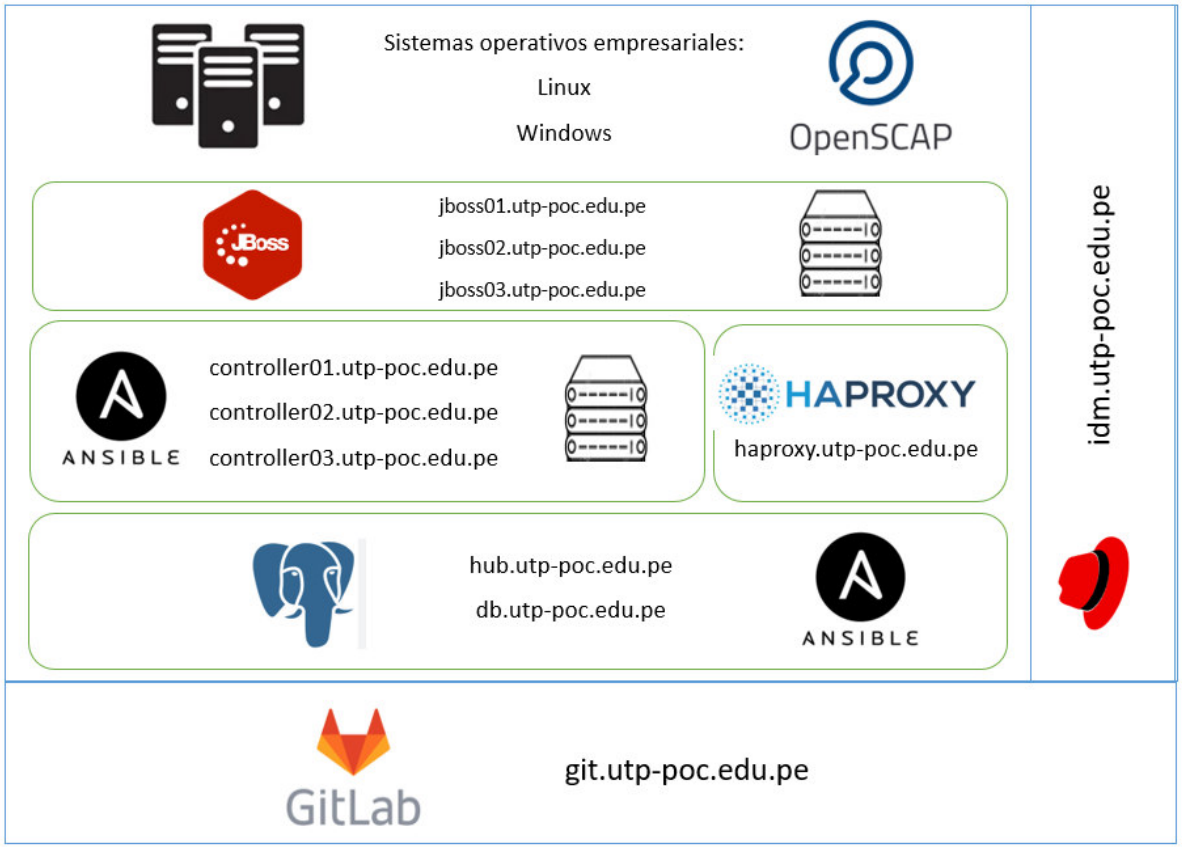
- Certificación de aplicabilidad de remediación.

Anexo E: Aplicación del modelo propuesto

En esta sección se detalla la implementación de la prueba de concepto virtual implementada en el dominio de pruebas utp-poc.edu.pe el reservado para la implementación como se muestra en la la Figura 11, se presenta la arquitectura general de implementación de la base tecnológica para aplicar el modelo:

Figura 11

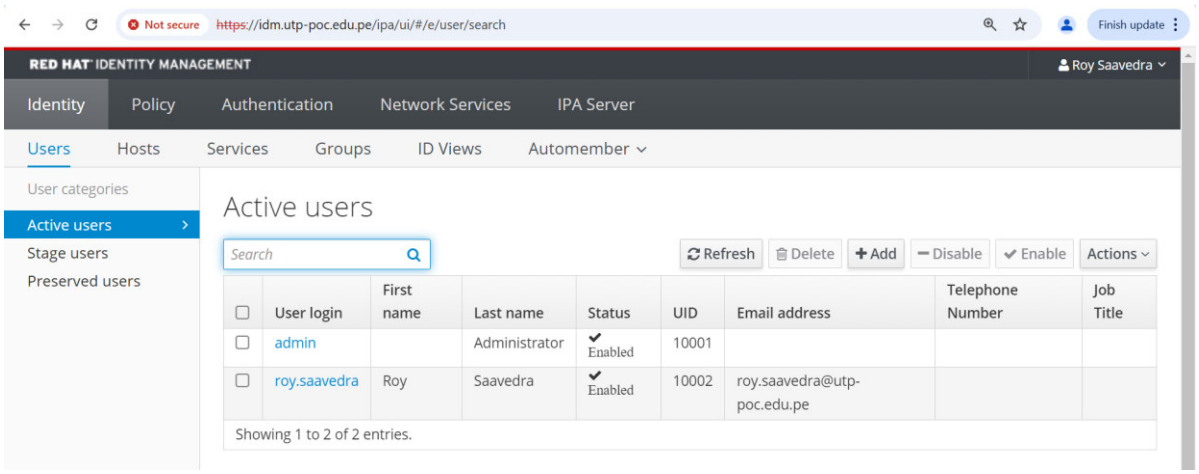
Arquitectura de la prueba de concepto



Considerando que se debe gestionar el acceso a los recursos de todos los componentes que integran la solución del modelo propuesto, se implementa el servidor de Red Ha Identitiy Management sobre el servidor con fqdn idm.utp-poc.edu.pe para disponer de los usuarios que serán administradores, operadores o cualquier otro rol como se muestra en la Figura 12

Figura 12

Plataforma de gestión de identidades



El componente principal de la infraestructura es la plataforma de automatización Red Hat Ansible Automation Platform la cual se implemento en 3 servidores para generar balanceo de carga debido a la gran cantidad de peticiones que se podrían generar, en este componente se usaron tres servidores con los fpdn controller01.utp-poc.edu.pe, controller02.utp-poc.edu.pe y controller03.utp-poc.edu.pe los cuales fueron activados como se muestra en la Figura 13, 14 y 15

Figura 13

Primer controlador de automatización

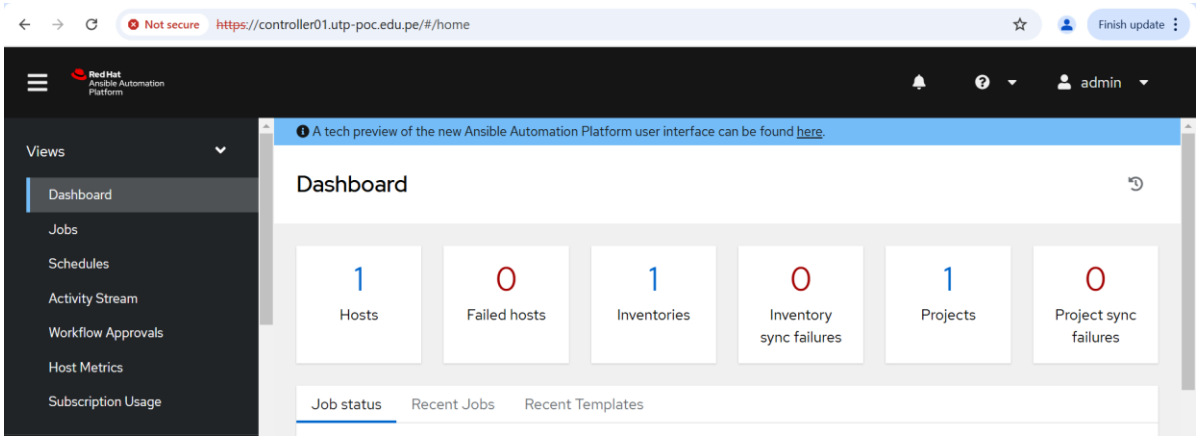


Figura 14

Segundo controlador de automatización

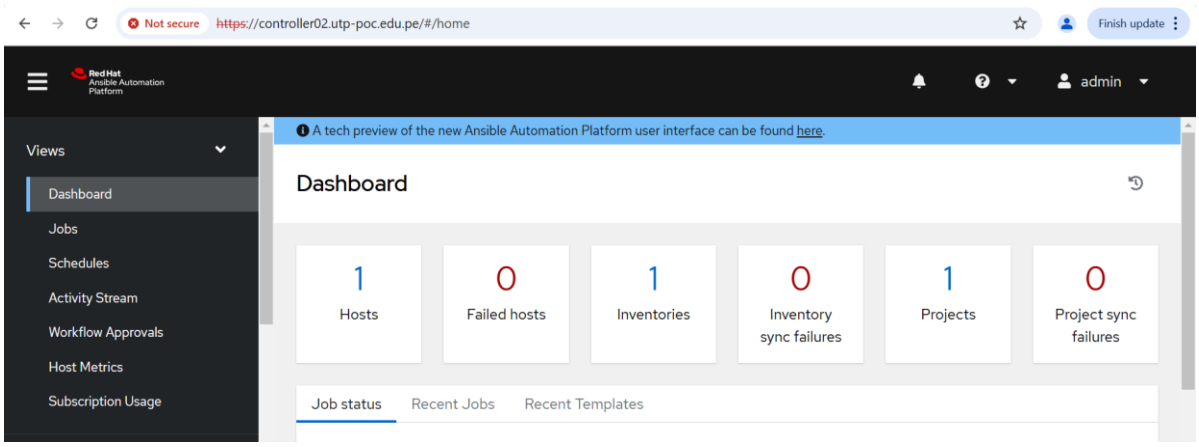
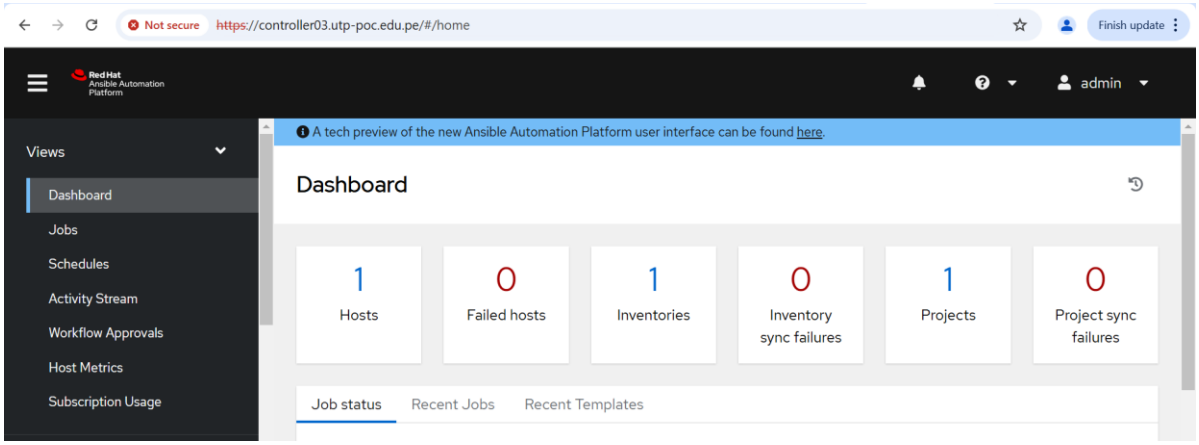


Figura 15

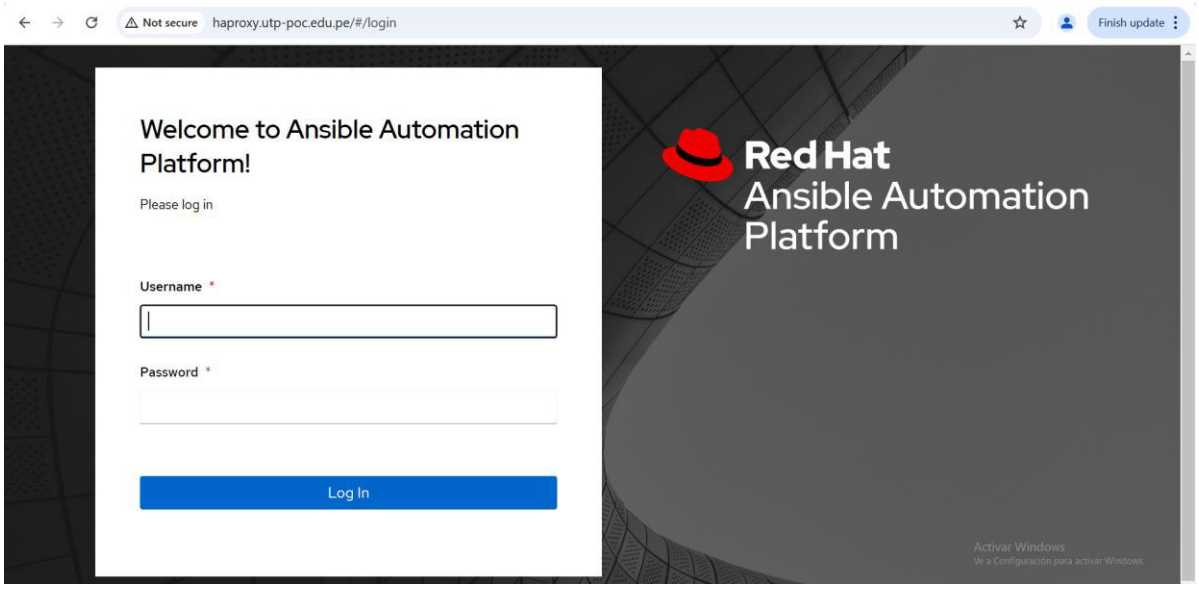
Tercer controlador de automatización



Para darle disponibilidad y balanceo a los tres servidores, se implemta el balanceador de aplicaciones haproxy bajo el fqdn haproxy.utp-poc.edu.pe para que transfiera la carga de las operaciones de los tres nodos bajo un solo servicio como se muestra en la Figura 16

Figura 16

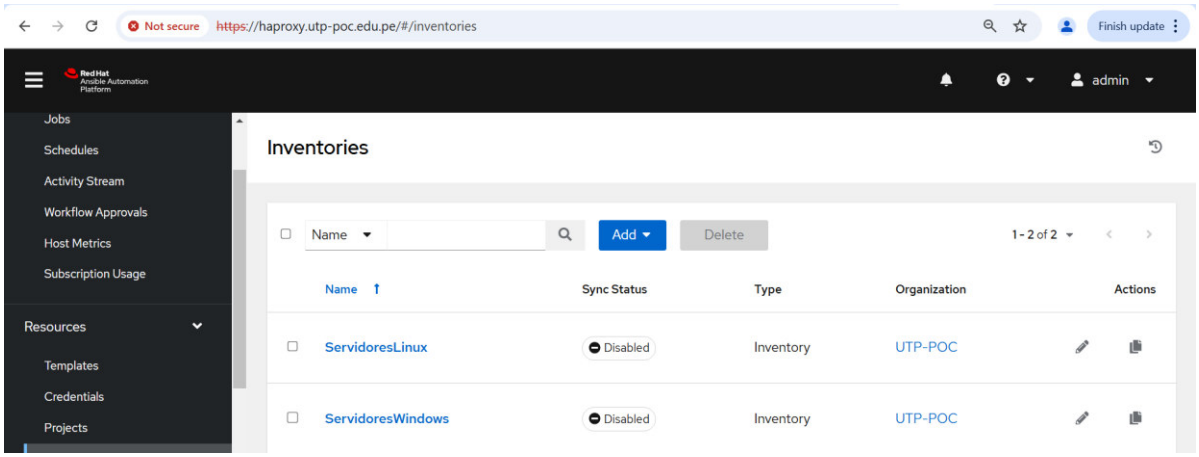
Balanceador de aplicaciones haproxy



Es necesario crear inventarios con los servidores que se desea remediar, por ello se destinan inventarios para servidores Windows y Linux teniendo la capacidad de crear tantos inventarios como se desee, los inventarios de la prueba de concepto se muestran en la Figura 17

Figura 17

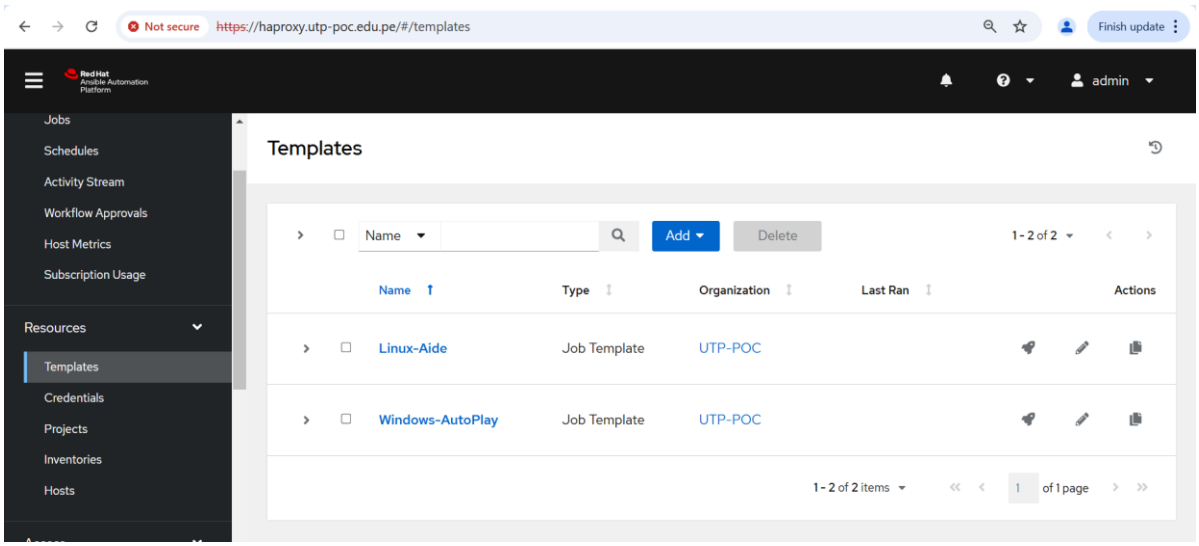
Inventarios de servidores



Luego se deberán cargar programas de automatización, los cuales tienen la capacidad realizar correcciones, remediaciones, configuraciones, actualizaciones entre otros, como se muestra en la Figura 18

Figura 18

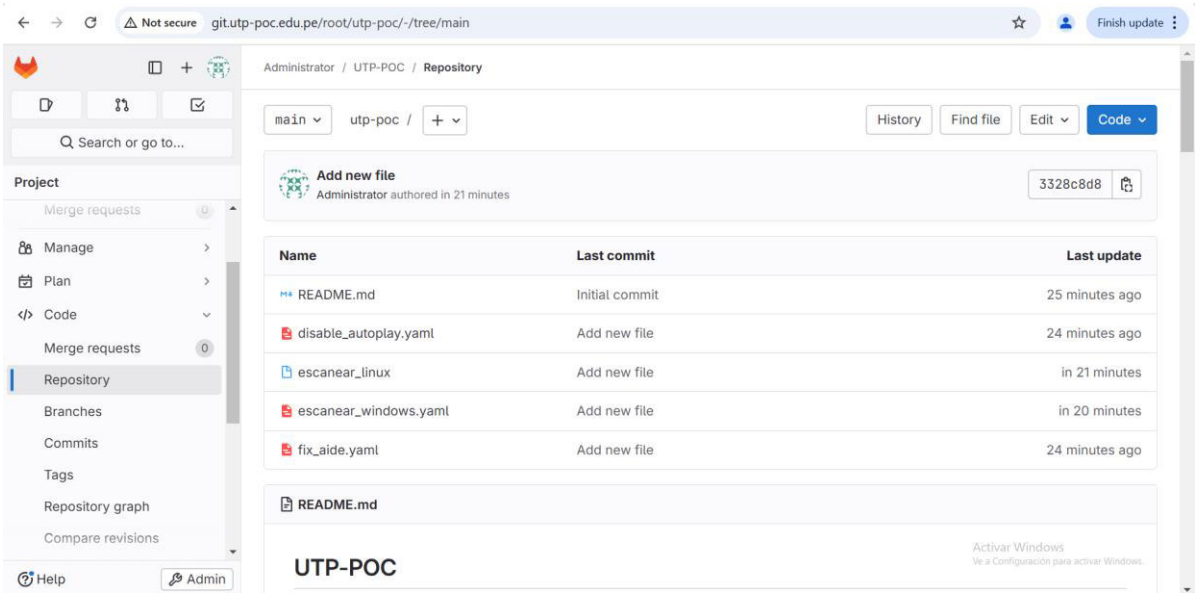
Programas de automatización



Aunque el cluster de servidores Ansible tiene la capacidad de almacenar los programas de automatización en lenguaje YAML en su disco local, una buena práctica es almacenar dichos programas en un repositorio de código como el que se implementó en el fqdn git.utp-poc.edu.pe como se muestra en la Figura 19 para facilitar la gestión de dicho código siguiendo los lineamientos del ciclo de vida del desarrollo de software.

Figura 19

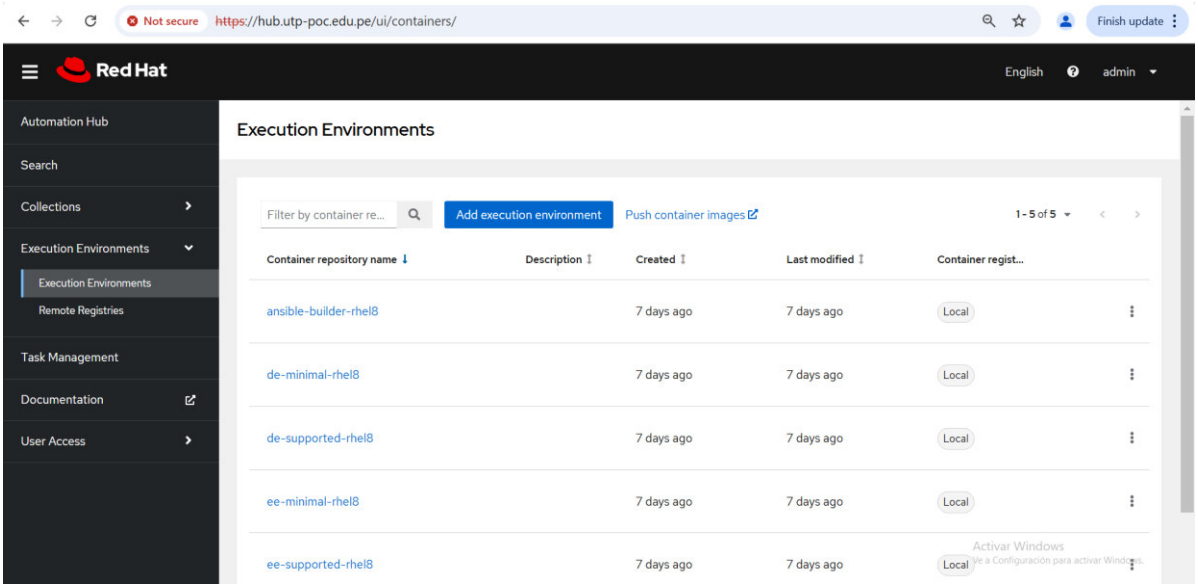
Repositorio de código



Como el sistema Ansible puede administrar diferentes entornos de trabajo, donde se requiere conexión a servidores Linux, Windows, VMware, nube, entre otros, se implementa bajo el fqdn hub.utp-poc.edu.pe un servidor de entorno de ejecución que facilite el trabajo como se muestra en la Figura 20

Figura 20

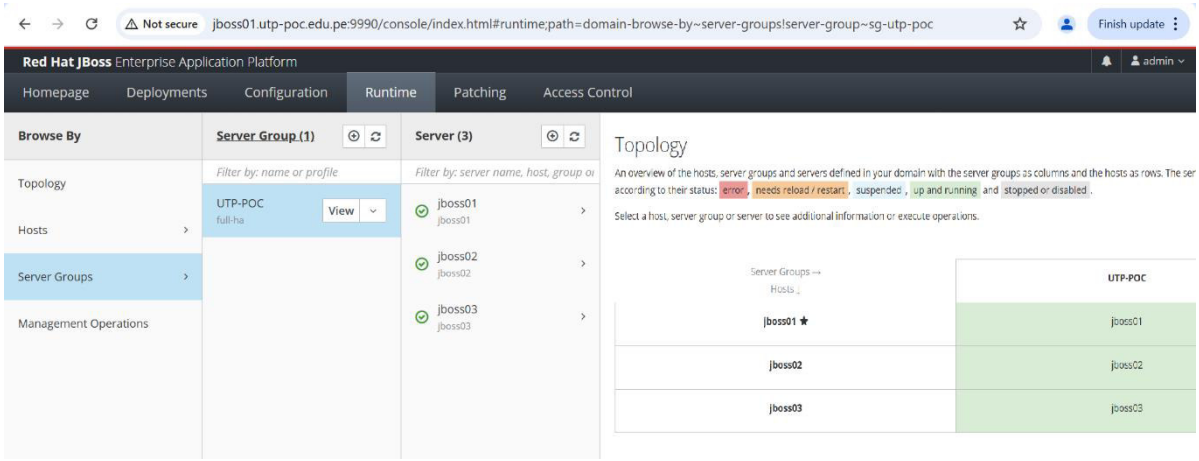
Entornos de ejecución de automatización



Finalmente se implementa el cluster de servidores Red Hat JBoss Enterprise Application Platform para la publicación de reportes de indicadores necesarios para el procesamiento de datos del modelo propuesto, para ello se implementó en tres nodos bajo el perfil full-ha como se muestra en la Figura 21

Figura 21

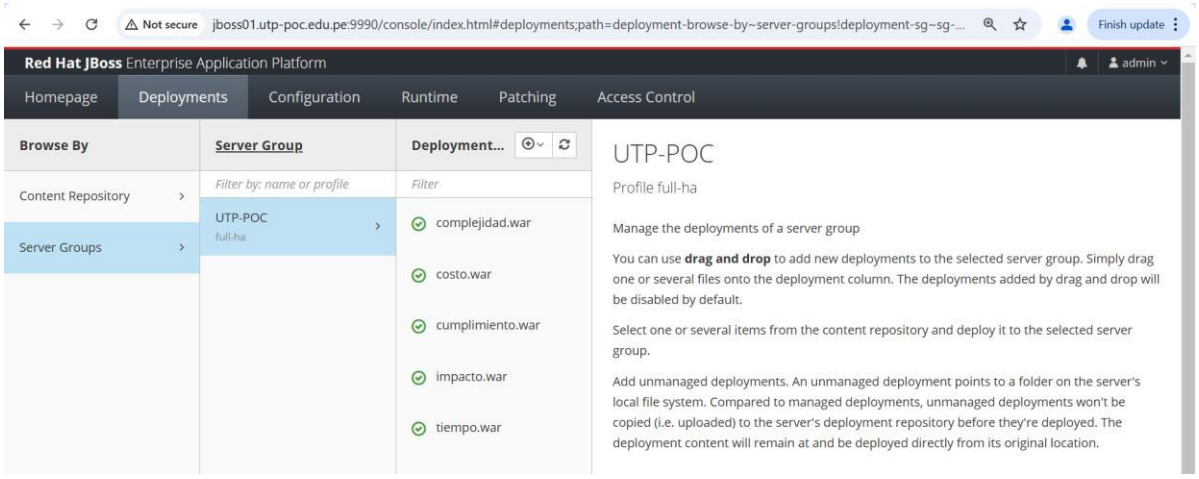
Cluster de aplicaciones



Dentro del cluster implementado para reportes, se publican los 5 componentes correspondiente a la publicación de los indicadores claves de la investifacion como se muestra en la Figura 22

Figura 22

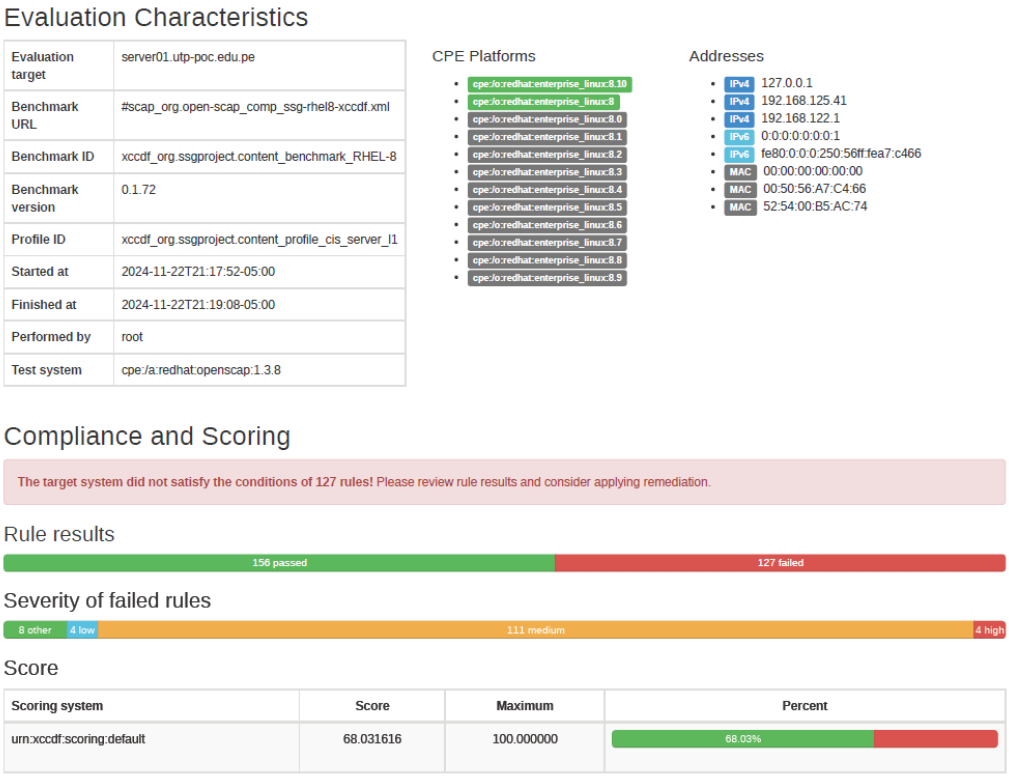
Publicación de reportes



Finalmente, con el modelo implementado, tómanos como primera prueba un servidor Red Hat Enterprise Linux 8, el cual se ejecutó una tarea de análisis para establecer la línea base de escaneo usando el lineamiento CIS nivel 1, el cual se ejecuto como se muestra en la Figura 23 obteniendo una calificación de 68.031616%

Figura 23

Reporte del servidor Linux



Como parte de la prueba de concepto, se evalúa las pruebas que resultaron fallidas, enfocándonos en el componente Aide como se muestra en la Figura 24

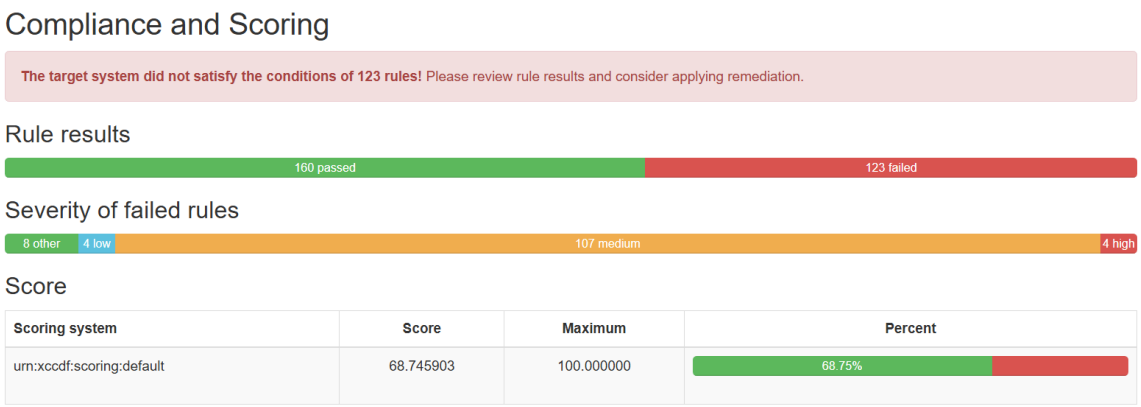
Figura 24

Detalle de componente Linux

Por ello, vamos a utilizar la tarea de automatización de remediación pre-cargada en la plataforma para obtener un reporte nuevo post-ejecución del fix_aide el cual ahora indica una calificación de 68.745903% como se muestra en la Figura 25

Figura 25

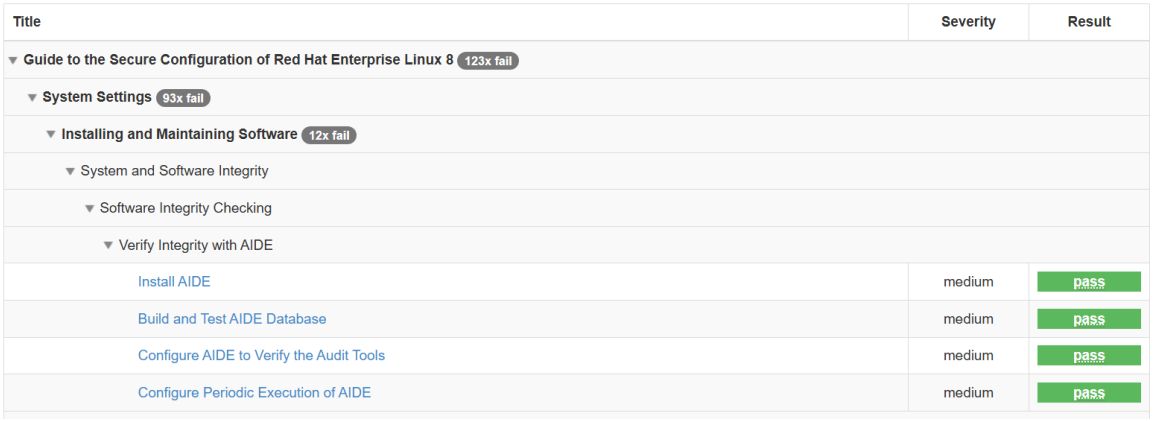
Nuevo reporte del servidor Linux



Volvemos a examinar el detalle del nuevo reporte y vemos que la configuración de Aide ahora si pasa las pruebas como se muestra en la Figura 26, determinando una mejora en indicadores medidos

Figura 26

Nuevo detalle de componente Linux

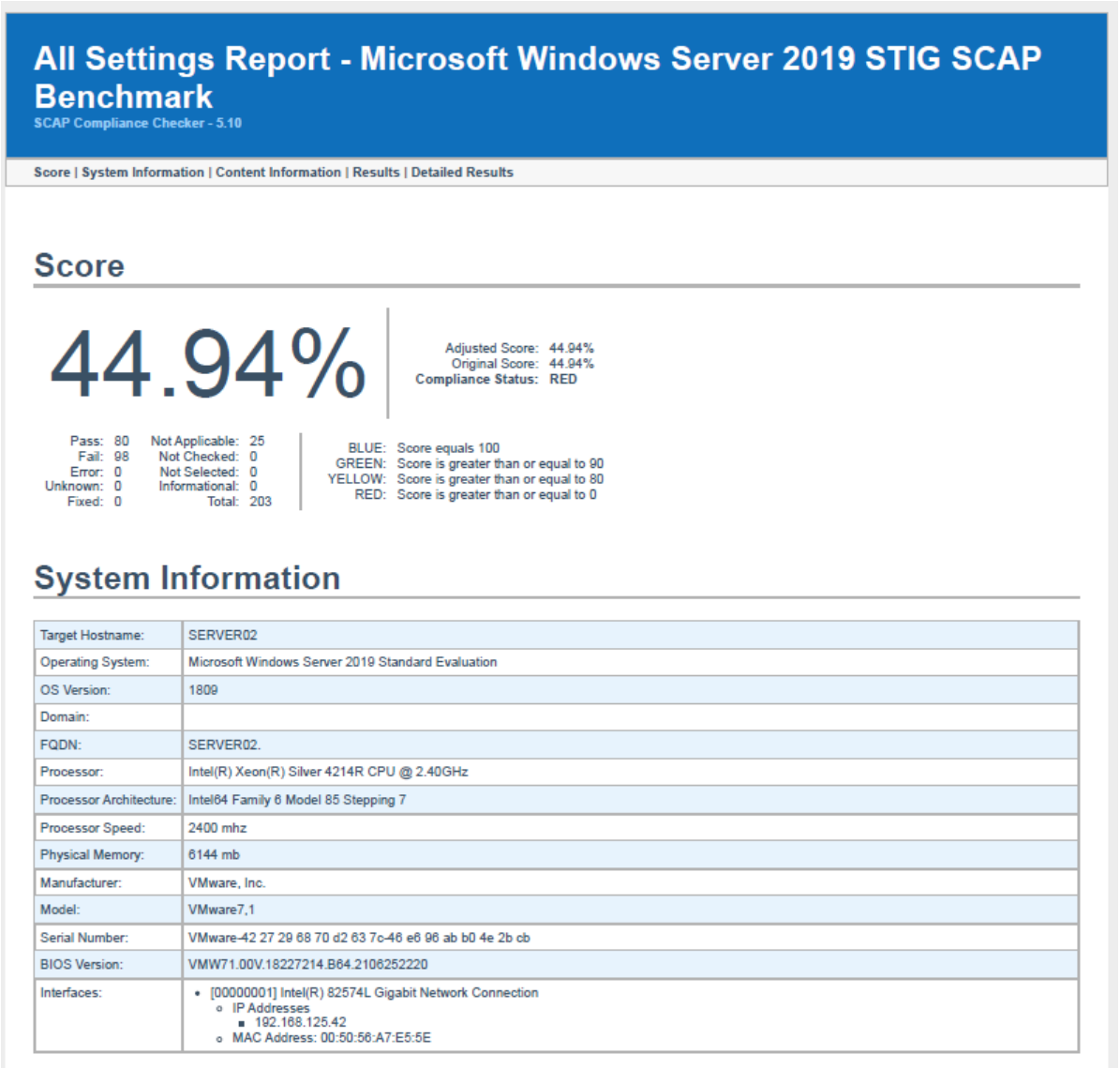


Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise Linux 8 123x fail		
System Settings 93x fail		
Installing and Maintaining Software 12x fail		
System and Software Integrity		
Software Integrity Checking		
Verify Integrity with AIDE		
Install AIDE	medium	pass
Build and Test AIDE Database	medium	pass
Configure AIDE to Verify the Audit Tools	medium	pass
Configure Periodic Execution of AIDE	medium	pass

Aunque la plataforma está basada en servidores Linux, su aplicación se puede dar también el clientes Windows, como se muestra en la Figura 27, se realiza el escaneo de vulnerabilidades del servidor con una calificación de 44.94%

Figura 27

Reporte del servidor Windows



All Settings Report - Microsoft Windows Server 2019 STIG SCAP Benchmark

SCAP Compliance Checker - 5.10

Score | System Information | Content Information | Results | Detailed Results

Score

44.94%

Adjusted Score: 44.94%
Original Score: 44.94%
Compliance Status: RED

Pass: 80 Not Applicable: 25
Fail: 98 Not Checked: 0
Error: 0 Not Selected: 0
Unknown: 0 Informational: 0
Fixed: 0 Total: 203

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

System Information

Target Hostname:	SERVER02
Operating System:	Microsoft Windows Server 2019 Standard Evaluation
OS Version:	1809
Domain:	
FQDN:	SERVER02.
Processor:	Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz
Processor Architecture:	Intel64 Family 6 Model 85 Stepping 7
Processor Speed:	2400 mhz
Physical Memory:	6144 mb
Manufacturer:	VMware, Inc.
Model:	VMware7,1
Serial Number:	VMware-42 27 29 68 70 d2 63 7c-46 e6 96 ab b0 4e 2b cb
BIOS Version:	VMW71.00V.18227214.B64.2106252220
Interfaces:	• [00000001] Intel(R) 82574L Gigabit Network Connection ◦ IP Addresses ▪ 192.168.125.42 ◦ MAC Address: 00:50:56:A7:E5:5E

Se examina las pruebas más importantes, al igual que el análisis del servidor Linux, nos enfocamos en algunas pruebas como la desactivación de la función de autoplay de Windows como se muestra en la Figura 28

Figura 28

Detalle de componente Windows

Results: High Severity (CAT I)

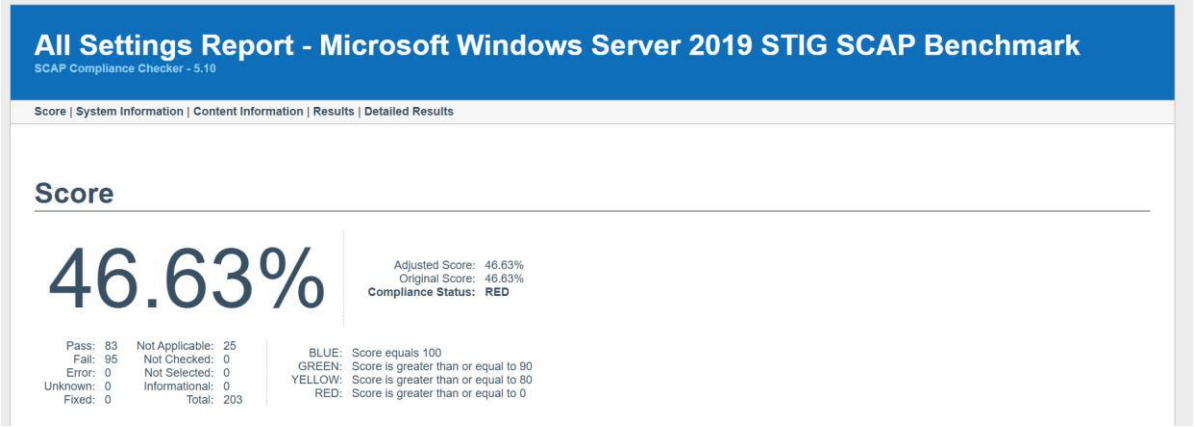
Automated Checks

- V-205653 - Windows Server 2019 reversible password encryption must be disabled. - Pass
- V-205654 - Windows Server 2019 must be configured to prevent the storage of the LAN Manager hash of passwords. - Pass
- V-205663 - Windows Server 2019 local volumes must use a format that supports NTFS attributes. - Pass
- V-205711 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-205713 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-205724 - Windows Server 2019 must not allow anonymous enumeration of shares. - Fail
- V-205725 - Windows Server 2019 must restrict anonymous access to Named Pipes and Shares. - Pass
- V-205739 - Windows Server 2019 permissions on the Active Directory data files must only allow System and Administrators access. - Not Applicable
- V-205750 - Windows Server 2019 Act as part of the operating system user right must not be assigned to any groups or accounts. - Pass
- V-205753 - Windows Server 2019 Create a token object user right must not be assigned to any groups or accounts. - Pass
- V-205757 - Windows Server 2019 Debug programs: user right must only be assigned to the Administrators group. - Pass
- V-205802 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option. - Fail
- V-205804 - Windows Server 2019 Autoplay must be turned off for non-volume devices. - Fail
- V-205805 - Windows Server 2019 default AutoRun behavior must be configured to prevent AutoRun commands. - Fail
- V-205806 - Windows Server 2019 AutoPlay must be disabled for all drives. - Fail
- V-205849 - Windows Server 2019 must be maintained at a supported servicing level. - Pass
- V-205908 - Windows Server 2019 must prevent local accounts with blank passwords from being used from the network. - Pass
- V-205914 - Windows Server 2019 must not allow anonymous enumeration of Security Account Manager (SAM) accounts. - Pass
- V-205919 - Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. - Fail

Luego se ejecuta la tarea de remediación disable_autoplay.yaml para corregir la configuración recomendada, obteniendo un nuevo reporte como se muestra en la Figura 29 con una calificación de 46.63%

Figura 29

Nuevo reporte del servidor Windows



La calificación mejoro ya que la configuración de autoplay fue aplicada como se muestra en la Figura 30

Figura 30

Nuevo detalle de componente Windows

Results: High Severity (CAT I)

Automated Checks

- V-205653 - Windows Server 2019 reversible password encryption must be disabled. - Pass
- V-205654 - Windows Server 2019 must be configured to prevent the storage of the LAN Manager hash of passwords. - Pass
- V-205663 - Windows Server 2019 local volumes must use a format that supports NTFS attributes. - Pass
- V-205711 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication. - Fail
- V-205713 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-205724 - Windows Server 2019 must not allow anonymous enumeration of shares. - Fail
- V-205725 - Windows Server 2019 must restrict anonymous access to Named Pipes and Shares. - Pass
- V-205739 - Windows Server 2019 permissions on the Active Directory data files must only allow System and Administrators access. - Not Applicable
- V-205750 - Windows Server 2019 Act as part of the operating system user right must not be assigned to any groups or accounts. - Pass
- V-205753 - Windows Server 2019 Create a token object user right must not be assigned to any groups or accounts. - Pass
- V-205757 - Windows Server 2019 Debug programs: user right must only be assigned to the Administrators group. - Pass
- V-205802 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option. - Fail
- V-205804 - Windows Server 2019 Autoplay must be turned off for non-volume devices. - Pass
- V-205805 - Windows Server 2019 default AutoRun behavior must be configured to prevent AutoRun commands. - Pass
- V-205806 - Windows Server 2019 AutoPlay must be disabled for all drives. - Pass
- V-205849 - Windows Server 2019 must be maintained at a supported servicing level. - Pass
- V-205908 - Windows Server 2019 must prevent local accounts with blank passwords from being used from the network. - Pass
- V-205914 - Windows Server 2019 must not allow anonymous enumeration of Security Account Manager (SAM) accounts. - Pass
- V-205919 - Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. - Fail

Finalmente se muestra en la Figura 31 todos los servidores implementados para la prueba de concepto con el dominio utp-poc.edu.pe bajo plataforma de virtualización vSphere

Figura 31

Servidores virtuales de la plataforma implementada