UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Metodología para la elección de software de seguridad informática

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORA:

Julissa Tatiana Sosa Fernández

ASESOR:

Francisco Manuel Hilario Falcón

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y seguridad de la información

LIMA – PERÚ

2018

PAGINA DEL JURADO

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

El Jurado encargado de evaluar la tesis presentada por don (a) **SOSA FERNÁNDEZ JULISSA TATIANA** cuyo título es:

Metodología para la elección de software de seguridad informática

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: CATORCE

Lima, San Juan de Lurigancho 07 de Diciembre del 2018

..... PRESIDENTE

..... SECRETARIO

..... VOCAL

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado

DEDICATORIA

Dedico esta tesis con mucho amor a mi madre y a mi hermana que siempre me apoyan en el cumplimiento de mis metas y que son mi fuerza para seguir adelante.

AGRADECIMIENTO

Agradezco a mis profesores que me apoyaron en la realización de este proyecto, guiándome durante el proceso.

DECLARACIÓN DE AUTENTICIDAD

DECLARACIÓN DE AUTENTICIDAD

Yo Sosa Fernández Julissa Tatiana con DNI N° 48167847, a efecto de cumplir con las disposiciones vigentes consideradas en el Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela de Sistemas, declaro bajo juramento que toda la documentación que acompaño es veraz y auténtica.

Así mismo, declaro también bajo juramento que todos los datos e información que se presentan en la presente tesis son auténticos y veraces.

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 de la Universidad César Vallejo.

Lima, diciembre del 2018

Sosa Fernández Julissa Tatiana
DNI Nº 48167847

PRESENTACIÓN

Señores miembros del jurado:

En cumplimiento de las normas establecidas en el Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada "MERSAM: Metodología para la elección de software de seguridad informática", la misma que someto a vuestra consideración y espero que cumpla con los requisitos para obtener el título profesional de Ingeniero de Sistemas

Esta investigación se ha estructurado en ocho capítulos según el esquema de investigación propuesto por la universidad. En el capítulo I, la introducción de la investigación con la realidad problemática, trabajos previos, teorías relacionadas al tema, formulación del problema, justificación del estudio, hipótesis y objetivos. En el capítulo II se presenta el método con el diseño de investigación, las variables y su operacionalización, la población y la muestra, técnicas e instrumentos, métodos de análisis de datos y aspectos éticos. En el capítulo III se presentan los resultados. En el capítulo IV, se expone la discusión de los resultados. En el capítulo V se formulan las conclusiones. En el capítulo VI se presentan las recomendaciones. Por último, en el capítulo VII se muestran las referencias y en el capítulo VIII los anexos de la investigación.

Con el cumplimiento de los aspectos en mención, se espera actuar de conformidad a las exigencias de la Universidad César Vallejo.

Sosa Fernández Julissa Tatiana

INDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN

La presente investigación titulada: Metodología para la elección de software de seguridad informática. Este estudio se centra en conocer cuál es nivel de protección y las medidas que se adoptan para reducir el riesgo de pérdida de información. A su vez, tiene como objetivo general: Elaborar una metodología para la elección de software de seguridad informática y aplicarla para determinar si la seguridad de la información se ve menos afectada. La metodología empleada fue la cuantitativa, cuyo diseño es experimental y el tipo de investigación es aplicada, contando con una población de 30, y muestra de 30 por ser un menor a 50 En este sentido, la técnica de recolección de datos será la observación a través de una hoja de recolección de datos.

Palabras Clave: Metodología, evaluación, seguridad, tecnología

ABSTRAC

The present research entitled: Methodology for the choice of computer security software. This study focuses on the level of protection and the measures that are adopted to reduce the risk of information loss. At the same time, its general objective is to: Develop a methodology for the choice of computer security software and apply it to determine the security of information. The methodology used was quantitative, whose design is experimental and the type of research is applied, counting on a population of 30, and sample of 30 for being less than 50 in this sense, the technique of data collection is the observation through a data collection sheet.

Keywords: Methodology, evaluation, TI security, technology

I. INTRODUCCIÓN

1.1. Realidad problemática

En la actualidad, las empresas deben proteger sus equipos informáticos de infecciones, ya que esto les generaría una significativa pérdida a nivel económico. Lamentablemente; según estudios realizados por especialistas, se elucidó que las organizaciones no otorgan la debida importancia a la evaluación detallada de software de seguridad. La causa es que se dejan guiar por las marcas posicionadas en el mercado, por los precios o por las especificaciones que dicen cumplir, mas no se cercioran que estas características efectivamente se cumplan y proporcionen la seguridad adecuada a sus equipos y a la información alojada en ellos. (Lalonde L´evesque, Carlton R., Fernandez, Chaisson, & Somayaji, 2012)

Por ello; para realizar una correcta elección de software de seguridad, se debe tener presente evaluar: el tiempo que demora en cargar el sistema y los programas alojados en el equipo y sobre todo la protección que brinda al momento en que dicho equipo se ve amenazado por algún ataque". (Navia Mendoza, Párraga Álava, Molina Garzón, & Vidal Loor, 2015)

Sin embargo en base a la bibliografía consultada; países del primer mundo como Canadá, Estados Unidos, Italia, entre otros, sí han realizado estudios que evalúen la elección de este tipo de software tan importante para las empresas, testeando cada uno de ellos y tomando distintas marcas de software de seguridad informática entre licenciados y libres, usando diferentes tipos de análisis; en donde comprobaron que muchos de estos programas, lamentablemente no cumplen con las características que dicen cumplir o de lo contrario las cumplen sin satisfacer los requerimientos de la organización o usuarios finales.

En el Perú; las instituciones públicas, realizan el análisis comparativo de software de seguridad informática basados en la Guía Técnica sobre la Evaluación de Software (R. M. N° 139-2004-PCM) conforme a Ley 28612 que sólo regula a la administración pública. El cual compara uno con otro dejándose guiar también por el costo (Ministerio

de Educación, 2011)

Basándonos en la investigación bibliográfica consultada, se observa que no existe una metodología oficial adecuada que permita la elección de software de seguridad informática. Esto genera que las empresas no tengan los pasos correctos a seguir para evaluarlos, por ello no realizan una previa evaluación técnica de los software al momento de adquirir una licencia para la protección de sus equipos tanto en hardware como en software.

En consecuencia, al no contar con el software de seguridad informática adecuado las empresas tienen sus equipos infectados o en el peor de los casos malogrados lo cual generan la pérdida de información ocasionando altos costos económicos en tiempo, recursos humanos y materiales, además de dinero.

Por ello, se plantea crear una metodología para la elección de software de seguridad informática para que las empresas tengan las herramientas necesarias para evaluar adecuadamente los software antes de adquirir uno de ellos y puedan tomar la decisión de protección más óptima para sus equipos informáticos, tanto hardware como software y evitar las pérdidas que esto pueda generar.

1.2. Trabajos previos

Alvarez, Nuñez, Reyes y González (2014) en su artículo científico "Selección de productos antivirus. Una mirada actual desde el sector de la salud en Cuba" presentado en la Revista Cubana de Informática Médica tienen como objetivo general de estudio: desplegar una perspectiva actual de los principales sistemas antivirus usados en el sector salud cubanos. (Alvarez Zaldivar, Gonzáles Torres, Nuñez Maturel, & Reyes Dixson, 2014)

La metodología usada para dicha investigación se basa en la revisión de estadísticas sobre el uso de tres antivirus AVG, Avast y Avira en páginas certificadoras de productos de seguridad como AV-Comparatives, Virus Bulletin, ICSA Labs e Instituto AV-TEST.

Adicional a ello se validó el comportamiento de los tres antivirus durante un periodo de tres meses en un mismo equipo de características: Windows XP SP 3, microprocesador Pentium Dual Core a 2.60 Ghz y 1 Gb de memoria RAM, 1 Tb de capacidad del disco duro.

Llegando a la conclusión de que el mejor antivirus a usar será el que resulte viable según los requerimientos de cada usuario y de las condiciones técnicas que lo permitan sostener.

Corrales, Páramo, Gutierrez y Ortega (2015) en su artículo científico titulado "Backdoor de los antivirus" presentado en la revista Pistas Educativas tienen como objetivo diagnosticar si la seguridad que conforman los antivirus más conocidos de año 2015 dispone de herramientas y medidas necesarias para abordar los diversos tipos de ataques amenazan la seguridad e integridad de los equipos electrónicos en red. (Corrales Cortes, Gutiérrez Vera, Ortega González, & Páramo Domínguez, 2015)

La metodología usada para esta investigación fue encuestar al 10% del alumnado del instituto Tecnológico de Celaya para determinar que antivirus usan, como se sienten

con su uso y que protecciones les aportan. Además de ello se realizaron pruebas de seguridad en base a lo indicado por SSTS (Security Software Testing
Suite) de Matousec.

Las pruebas se realizaron en un equipo de 64 bits con Windows 10 instalado además VMware para el manejo controlado de un entorno virtual y contar con las firmas de base de datos de antivirus actualizado.

Haffejee, Irwin (2014) en su artículo científico titulado "Testing antivirus engines to determine their effectiveness as a security layer" presentado en la revista IEEE Xplore tiene como objetivo general de estudio: Medir la efectividad de los motores de antivirus cuando están expuestos a diferentes técnicas de invasión. (Haffejee & Irwin, 2014)

La metodología usada para esta investigación está dividida en cinco puntos: a)Visión general, la cual consiste en saber cómo opera un motor de antivirus; b)VirusTotal, se usa esta herramienta para un análisis previo y como forma de ahorrar tiempo y costo de licencia; c)Baseline Binary, los antivirus serán analizados utilizando un binario que se sabe que es un malware; d)Baseline Tests, Se utilizara VirusTotal para determinar si detecta que el binario es malicioso, con este binario se buscan las técnicas de evasión; e)Técnicas de evasión, se aplica la técnica de evasión después de ser analizados los requerimientos básicos. Esta metodología se aplicó específicamente usando Virustotal como muestra de estudio.

Se llegó a la conclusión de que una vez que una aplicación maliciosa se combina con las técnicas de evasión, esta es capaz de pasar por alto ante el análisis de un significativo número de antivirus, es por ello que un antivirus no debería considerarse un medio eficaz de protección.

Lévesque, Davis, Fernández, Chiasson y Somayaji (2012) en su artículo científico titulado: "Methodology for a Field Study of Anti-malware Software" presentado en la Revista J. Blythe, S. Dietrich, and L.J. Camp tiene como objetivo general de estudio:

Proponer que las pruebas de anti-malware beneficiaran a los estudios de campo que evalúan la eficacia. (Lalonde L´evesque, Carlton R., Fernandez, Chaisson, & Somayaji, 2012)

La metodología usada es un estudio de campo a largo plazo de software anti-malware con usuarios reales, ya que al monitorear el uso real, con el tiempo, se puede obtener una mejor comprensión de cómo los sistemas anti-malware se utilizan y cómo los factores externos influyen en él. Esta metodología fue aplicada en un periodo de cuatro meses con 50 participantes.

Se llega a la conclusión de que aunque en la actualidad hay varios métodos para la evaluación de productos anti-malware, estos no reflejan el rendimiento de los productos en la vida real. Los métodos de evaluación típicos se basan en el escaneo de recogida o sintetizado de software malicioso junto con programas legítimos. Si bien estos enfoques pueden medir la exactitud sin procesar el detector, no tienen en cuenta factores tales como las interacciones del usuario, las amenazas en evolución, y los diferentes ambientes.

Mohaisen y Alrawi (2014) en su artículo científico titulado: "AV-Meter: An Evaluation of Antivirus Scans and Labels" presentado en la Revista S. Dietrich tiene como objetivo general de estudio: responder a varias preguntas referentes a la tasa de detección, corrección de etiquetas de las marcas, y la consistencia en la detección de los escáneres antivirus. (Mohaisen & Alrawi, 2014)

Se utilizó más de 12.000 muestras de familias de malware que fueron inspeccionados y etiquetados de forma manual. Invitando con su investigación a que las organizaciones cuestionen la información que se muestran en las etiquetas de estos software.

La metodología empleada, es un análisis manual de un conjunto datos para la evaluación de los etiquetados de un gran número de motores de antivirus, comparándolo con las verdaderas funciones de cada uno. Usando más de 12000 malware de 11 familias.

Finalmente se concluyó que muchas de las etiquetas de software antivirus son incompletas, inconsistentes e incorrectas generando que las empresas se confíen de ellas para adquirir determinada marca, que no cumplen con las expectativas que tenían.

Morales, Xu, Sandhu (2012) en su artículo científico titulado: "Analyzing Malware Detection Efficiency with Multiple Anti-Malware Programs" presentado en la revista ASE tiene como objetivo general de estudio: Demostrar que es necesario el uso de más de un anti-malware para asegurar una protección eficaz. (Morales, Xu, & Sandhu, 2012)

La metodología usada es instalar cierto número de anti-malware, deshabilitarlos para luego habilitar y correr el primer programa durante un proceso del equipo para obtener un indicador de como este proceso fue infectado, luego deshabilitar la protección del primer programa y habilitar y correr el segundo programa durante otro proceso que fue salida de la detección del primer anti-malware, para así obtener un indicador de como este proceso fue infectado, así continuar la secuencia hasta habilitar y correr el último anti-malware durante el proceso que salió del análisis del anterior para ver como este proceso fue infectado.

Para este estudio se utilizó dos grupos de antimalware, el primero conformado por ESET, AVG y ZoneAlarm y el segundo por Kaspersky, G-Data y BitDefender, todos ellos instalados en un computador con sistema operativo Windows 7 de 32 bit.

La conclusión para este trabajo es que es necesario más de un programa anti-malware en un sistemas para detectar los diversos escenarios de malware o utilizar un anti-malware que use las técnicas de detección de diversos anti-malware.

En este sentido, Murillo, Ramiro (2013), desarrollo una tesis titulada "sistema antivirus multiplataforma en tiempo real usando técnicas heurísticas y proactivas". Cuyo objetivo fundamental fue Desarrollar e implementar un sistema eficiente de antivirus

para la detección, eliminación, prevención y actualización para los computadores personales mediante las técnicas de detección Heurística, Proactiva y la actualización por Internet de la base de firmas de Malwares. Para optar el título profesional de ingeniero estadístico e informático. Realizada Universidad nacional del Altiplano.

De esta manera, la metodología que se empleo fue la Programación Extrema (XP) por su amoldamiento en la creación de aplicaciones pequeñas y eficaces, sobre todo porque el antivirus es cambiado e reforzado con mejoras necesarias por la constante evolución de los Malwares. El Modelamiento fundamentado siempre en el Lenguaje de Modelamiento Unificado (UML) y la Métrica de Validación ISO/IEC 9126. Mediante el incorporación de datos de Malwares y la optimización iterativa de los procedimientos de detección para la psterior eliminación, proponiendo así un software estable y eficiente.

Concluyendo, que luego de hacer un análisis, hacer el diseño e implementar el Software Antivirus que es capaz de detectar una gran cantidad de Malwares en relación a las pruebas en un 80%, siendo un 50% detección en base a firmas de virus y un 30% por el Escanner Heurístico Proactivo. Al ser dinámico permite la detección en tiempo real para las unidades de almacenamiento extraíble para prevenir infecciones en la PC local, dando la seguridad de protección mediante las técnicas desarrolladas y descritas en dicho trabajo de investigación.

Navia, Parraga, Molina y Vidal (2015) en su artículo científico titulado: “Effectiveness and efficiency of free antivirus software against malware”, presentado en la Revista EspamCiencia, tiene como objetivo general de estudio: Observar el rendimiento y carga de trabajo producida por cuatro antivirus gratuitos, tanto en forma individual como combinando estos cuatro, al momento de velar por la protección de un computador contra el malware, para determinar si es conveniente emplear varios antivirus a la vez. Se tomó como muestra un computador. (Navia Mendoza, Párraga Álava, Molina Garzón, & Vidal Loor, 2015)

Respecto a la metodología empleada, para realizar las pruebas de estudio se basó en los instrumentos señalados por Lai y Wren (2011) que fueron reformulados de acuerdo a los objetivos. Dentro los cuales se evaluó los parámetros: Carga de Sistema y Protección. (Lai & Wren, 2011)

Las pruebas se realizaron en computadoras con procesador Intel Core i5 a 3 GHz, 6 GB de memoria RAM a 1333 MHz, disco duro ATA de 1.5 TB, unidad óptica de DVDR/W en un equipo con un sistema operativo de 64 bits Windows 7 Profesional. Usando cuatro antivirus, Avast, AVG, Avira, y Panda Cloud.

Finalmente, se elucidó que el uso de recursos a nivel de memoria RAM, así como el tiempo de arranque y carga del sistema operativo, en general suele ser mayor cuando hay dos antivirus instalados en comparación a cuando hay solo uno.

Norouzi y Parsa (2014) en su artículo científico titulado: "Verification of the protection services in antivirus systems by using NuSMV model checker" presentado en la Revista International Journal in Foundations of Computer Science & Technology tiene como objetivo general de estudio: proponer un modelo de servicios de protección en el sistema antivirus, extrayendo las propiedades que se espera a partir del modelo de enfoque de sistema antivirus de comportamiento de control en forma de CTL y LTL fórmulas lógica temporal. (Norouzi, Parsa, & Mahjur, 2014)

Respecto a la metodología, se observó el comportamiento de antivirus mediante el uso de modelos de técnicas de control formales, que separan estos comportamientos en prevención y control, usando la semántica statechart para modelar conductas preventivas y de control.

Se concluyó que las propiedades esperadas de sistemas antivirus se extraen de comportamiento de control en forma de fórmulas lógica temporal. También se implementó los modelos de comportamiento de enfoque de sistemas antivirus por la herramienta ArgoUML y el comprobador de modelos NuSMV.

Solarte, Enriquez y Benavides (2015) en su artículo científico titulado: “Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001" presentado en la revista Tecnológica ESPOL, tiene como objetivo principal de estudio: desarrollar capacidades en los ingenieros de sistemas, que les permitan liderar proyectos de diagnóstico, para la inserción de sistemas de seguridad de la información – SGSI alineados con el estándar de seguridad ISO/IEC 27001 y el sistema de control planteado en la norma ISO/IEC 27002.

La metodología empleada se basa en los dominios delimitados en la ISO/IEC 27001, se utiliza la metodología para realizar el análisis y determinación de riesgos fundamentados en los tres criterios de información que son la confidencialidad, la integridad y la disponibilidad de la información. También se comprueba la existencia de controles de seguridad en la empresa y la aplicación de ellos; ya que pueden estar contenidos dentro de los procesos de calidad organizacionales. Los controles de seguridad se contrastan con los controles determinados en la norma ISO/IEC 27002 como políticas y procedimientos.

El procedimiento se dividió en etapas subsecuentes y ordenadas; en cada una de ellas se trata de fijar objetivos y metas claras con productos entregables, donde los productos finales de la primera etapa servirán para anticiparse en la segunda y los de las segunda servirán para continuar con la tercera etapa y así gradualmente, ya que se plantea que la auditoría debe ser habitual o permanente dependiendo de la organización y los cambios en la tecnología de información usada en el tratamiento y procesamiento de la información.

Del proceso de diagnóstico realizado, se pudo concluir que no hay existencia de una cultura de seguridad de la información dentro de las instituciones, tampoco se encontró sistemas de control de seguridad informática y de información, y mucho menos, procesos y procedimientos documentados para protección de la información.

1.3. Teorías relacionadas

Seguridad informática: Según Baca (2016) la seguridad informática es aquella que fundamentada en políticas y normas internas y externas de la organización se encarga de proteger la información que las organizaciones o personas tienen alojadas en sus equipos o sistemas ante cualquier ataque, reduciendo el peligro físico o lógico al que se ve exhibida. (Baca Urbina, 2016)

Por otro lado Aguilera (2010) define como seguridad informática a la disciplina encargada de diseñar los métodos y técnicas para reducir el riesgo de pérdida de información al que puede estar expuesto un sistema de información. (Aguilera López, 2010)

Solarte haciendo una evaluación de seguridad determina que contar con software sin licencia es una vulnerabilidad y representa un riesgo muy alto causando un daño catastrófico con probabilidad muy baja de un 5% e impacto catastrófico

Seguridad de Información

Existen diversos conceptos sobre seguridad de información, en diferentes medios, rescatando algunos de estos podemos recalcar la que nos brinda la normativa técnica peruana:

> "Preserva la confidencialidad, integridad, disponibilidad de información; además, también puede ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad". (ISO/IEC, 2014)

También la norma nos indica que deben existir documentos de políticas de seguridad de la información los cuales "la gerencia deberá aprobar, publicar y comunicar a todos los empleados y terceras partes que lo requieran", así también se detalla que "la política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva", además deben definir el proceso

para nuevos planes de gestión de la información. (ISO/IEC, 2014)

Estas políticas de seguridad serán adecuadamente aplicadas si se tiene a las personas adecuadas asignadas para el cumplimiento de las mismas.

> "Todas las responsabilidades sobre la seguridad de la información deben ser claramente definidas". (ISO/IEC, 2013)

Estas responsabilidades deben ser dadas a personas de distintas áreas de la organización con roles relevantes ya que esto generaría un menor porcentaje de distorsión en el cumplimiento de los planes de seguridad de la información y no se genere una divulgación de información.

Así mismo dentro de cada área de la empresa que está relacionada con la gestión de la información, se deben mantener claro las personas que están autorizadas a realizar estos procesos y evitar el acceso a terceros.

> "Se elaborará y mantendrá un inventario de todos los activos importantes que sean claramente definidos. Se debe de identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones de procesamiento de información". (ISO/IEC, 2013)

Como podemos apreciar ambos conceptos están relacionados y uno depende del otro, por un lado la seguridad de la información nos brinda las la parte estratégica como análisis, normas y planes de seguridad y la seguridad informática se enfoca en el ámbito operacional abarcando la configuración, técnicas de protección y mecanismos de seguridad.

ISO/IEC 27001

"Este estándar internacional especifica los requerimientos para establecer,

implementar, operar, monitorear, revisar, mantener y mejorar la formalización de un sistema de gestión seguridad de información". (ISO/IEC, 2014)

La ISO 27000 define ataque como intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo. (ISO/IEC, 2014). Por ello se deben buscar medios para poder mitigar estos ataques.

Confidencialidad: Según Vivanco Percy la confiabilidad se encarga de asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian. (Vivanco)

Integridad: Según Vivanco Percy la integridad se encarga de garantizar que los datos sean los que se supone que son. (Vivanco)

Disponibilidad: Según Vivanco Percy la disponibilidad se encarga de garantizar el correcto funcionamiento de los sistemas de información. (Vivanco)

Nivel de infección: A la cantidad de archivos infectados ante un ataque de virus.

Anti-malware: Según Rainer y Cegielski (2010) un sistema Anti malware o también llamado AV son paquetes de software que identifican y eliminan virus, gusanos entre otros software malicioso, el cual es implementado por el departamento de sistemas de información. (p. 216) Estos software anti malware pueden ser libres o licenciados, siendo libres aquellos que no requieren de un pago para ser utilizados y licenciado aquellos que es necesario adquirir una licencia para poder usarlo completamente.

Antispyware: Tecnología que ayuda a proteger a un equipo contra ataques de spyware o cualquier software no deseado, ayuda a reducir los mensajes emergentes, cambios de configuración de internet no deseado y uso no autorizado de la información privada. (Valdés, 2010, p. 11)

Antivirus: Programa que se instala en una computador, el cual hace un escaneo de los

archivos con la finalidad de detectar, identificar y eliminar el malware detectado. (Padilla, 2010, p. 6) Un software antivirus está compuesto por la interface de usuario, la base de definición de virus y el motor de búsqueda.

Interface de usuario: Medio por el cual el usuario puede interactuar con el software antivirus, realizar análisis y configuraciones en general. (Padilla, 2010, p. 6)

Base de definición de virus: Es la cual contiene los archivos actualizados sobre las firmas de malware y es utilizado por el software para detectar los mismos. Es por ello que esta base de datos siempre debe estar actualizada y asegurar una eficaz y pronta detección. (Padilla, 2010, p. 6)

Motor de búsqueda: Es el cerebro del software antivirus, el cual se encarga de la búsqueda y detección del malware, utiliza para ello la base de datos de definición de virus. Por ello cada vez que nuevos virus son creados, la base de datos debe actualizarse para que con ello pueda revisar en archivos, sistemas, etc. Que no se hayan buscado. (Padilla, 2010, p. 6)

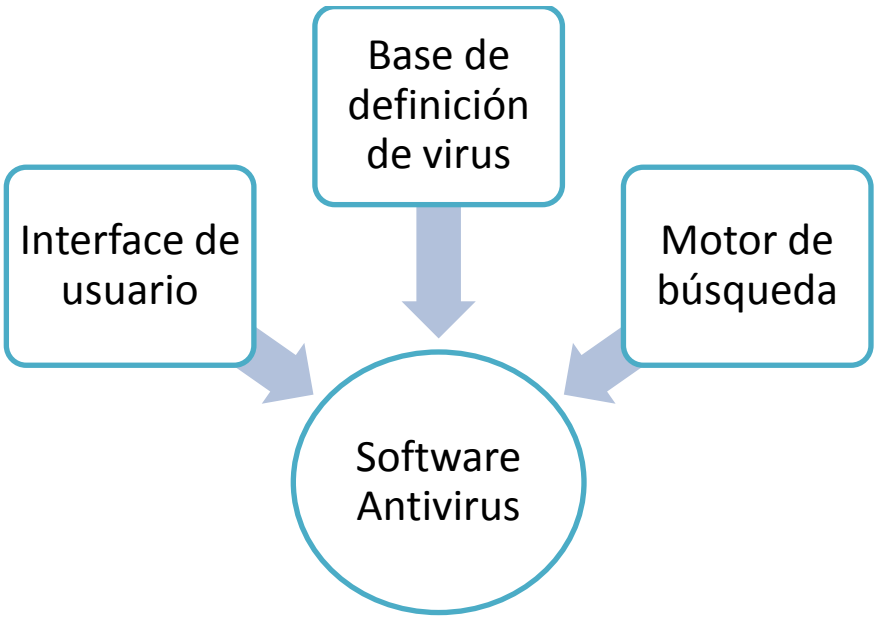


Figura 1: Componentes de un software antivirus

Malware: Se utiliza para referirse a todo aquel software que daña a un equipo de cómputo. Esta palabra proviene originalmente del término en inglés "malicious software", traducido al español como código malicioso, dentro de esta clasificación están los virus, los caballos de Troya, ad-ware, spy-ware, las puertas traseras, los gusanos de Internet, bots, entre otros. (Padilla, 2010, p. 6)

Tipos de Malware:

Virus

Los Virus se definen como programas que han sido creados para infectar archivos y así provocar efectos desagradables, destructivos o irreparables en un sistema, perdiendo información o incluso hardware. Los virus actúan cuando se ejecuta el programa infectado o al cumplirse una condición específica (una fecha, una acción del usuario, etc.). (González Medina & Salazar Rubio, 2012)

Gusanos: Estos programas se replican a sí mismos en distintas ubicaciones del equipo. Tienen como principal objetivo dispersarse y contagiar la mayor cantidad posible de equipos para saturar computadoras y redes. En diferencia con los virus, estos no infectan archivos. Puede transmitirse a través de emails, mensajería instantánea y programas point to point (P2P), usan estos medios con el objetivo de convencer a las personas de abrir el archivo que contiene al gusano. (González Medina & Salazar Rubio, 2012).

Troyanos: Son códigos maliciosos que aparentan ser programas inofensivos. Instalan programas en la computadora infectada para que pueda ser controlada remotamente. Son capaces de destruir archivos, capturar y reenviar información, permitir a un intruso controlar la computadora de forma remota, etc. (González Medina & Salazar Rubio, 2012).

Spyware: Este tipo de malware recolecta información de acceso de los usuarios para

enviársela a personas extrañas además de modificar algunas configuraciones de los navegadores. Los spyware disminuyen el rendimiento del equipo, mas no lo daña. Utilizan la interacción con el usuario para una mayor confiabilidad de los datos obtenidos. (Cardozo González & García Severiche, 2010)

Adware: Malware que envía al usuario pop up u otro medio de publicidad, la cual aparece constantemente generando molestias al usuario, la cual es uno de sus efectos, además consume memoria, procesador y ancho de banda. Este tipo de malware no causa daños al sistema operativo. (Cardozo González & García Severiche, 2010)

Rootkits: El nombre proviene ya que este malware apareció en el sistema UNIX y el atacante tenía acceso al usuario privilegiado llamado "root". Este tipo de malware oculta objetos, por ello no es del todo malicioso, ya que se usa para ocultar evidencia de la presencia de otro malware, por ejemplo, en los sistemas infectados.

Rootkits se ejecuta como parte del sistema utilizando funciones del mismo para no ser detectado, es por ello que el sistema estará bajo el control del atacante sin ser visto, dándole la posibilidad de alojarse la mayor cantidad de tiempo ayudando a otros malware. (Cardozo González & García Severiche, 2010)

Backdoors: Traducido al español como puerta trasera o también conocidos como troyanos de acceso remoto, ya que permiten al atacante conectarse remotamente al equipo infectado, dejándole la libertad de realizar cualquier actividad. Este troyano se puede disfrazar de archivos inofensivos como imágenes, correo, etc. Y una vez que obtiene el acceso al sistema instala una puerta trasera, la cual solo puede ser usada por el atacante. (Cardozo González & García Severiche, 2010)

Keyloggers: Uno de los malware más usados, ya que obtienen la información a través de las pulsaciones del teclado y se la envían al atacante. Puede obtener información como usuarios y contraseñas, número de tarjetas y claves o inclusive chats. El uso de este malware puede tener fines de lucro a través de la distribución de la información

obtenida en el ataque. (Cardozo González & García Severiche, 2010)

Banker: Su finalidad es obtener información bancaria de los usuarios infectados, específicamente claves de acceso de todo tipo de entidad bancaria, es por ello que también son llamados troyanos bancarios. Actúan reemplazando los sitios web de dichas entidades de tal manera que al utilizar los medios de dicha página, como el teclado virtual, se capture la información. (Cardozo González & García Severiche, 2010)

Botnets: Con este tipo de malware el atacante puede controlar cierta cantidad de computadores con fines lucrativos. Se pueden usar para generar ataques de denegación de servicio, enviar correo Spam, ect. Es por ello que se considera una de las amenazas más importantes, ya que el atacante tendría toda una red de computadores infectados a su disposición. (Cardozo González & García Severiche, 2010)

Password Stealer: Malware que al ejecutarse en un equipo buscan programas o navegadores para extraer información privada como contraseñas guardadas. (Cardozo González & García Severiche, 2010)

Dialer: Ataca al modem tomando el control de este, usualmente se infectan a través de descargas gratuitas, su ataque consiste en generar llamadas a números de costo alto, generando el aumento en la tarifa del usuario. (Cardozo González & García Severiche, 2010)

Ransomware: Este tipo de malware es comparado con un secuestro por su forma de ataque, ya que toma los archivos del usuario y los cifra, esto genera que el usuario no pueda acceder a ellos; luego el atacante pide un rescate para que le dé al usuario la contraseña y así pueda recuperar sus archivos. (Avalos & Gómez, 2015)

Características de un software de seguridad informática

Tiempo de respuesta: se define como el tiempo transcurrido entre el inicio de un proceso y el término de este. (Alimenti, y otros, 2012)

Restricciones en el uso de los recursos: La restricción de recursos no permite el correcto desarrollo de un proceso, ya que al no tener los elementos necesarios no se consigue una mejora. (Xuan et. al., 2016, p13)

Tiempo de arranque del sistema: Se refiere al tiempo transcurrido desde que se presiona el botón de encendido de un equipo hasta que ya se puede usar completamente. (Navia Mendoza, Párraga Álava, Molina Garzón, & Vidal Loor, 2015)

Tiempo de inicio de aplicaciones: Tiempo que demora una aplicación para que el usuario pueda hacer uso de ella. (Navia Mendoza, Párraga Álava, Molina Garzón, & Vidal Loor, 2015)

Tiempo de análisis de malware: Tiempo en que cada sistema antimalware demora en realizar un análisis. (Navia Mendoza, Párraga Álava, Molina Garzón, & Vidal Loor, 2015)

Cantidad de Malware detectado: Cantidad de malware que un sistema antimalware puede detectar durante un escaneo. (Navia Mendoza, Párraga Álava, Molina Garzón, & Vidal Loor, 2015)

Cantidad de memoria de acceso aleatorio (RAM) ocupada: Se refiere el uso de la RAM durante un proceso o después de la instalación de un software nuevo en el equipo. (Jarrín Zambrano, 2010)

Uso de la unidad central de procesamiento (CPU) durante escaneo. Refiere al uso que determinado software hace del CPU al ser instalado y ejecutado (Jarrín Zambrano, 2010)

Calidad: según Cuatrecasas y Gonzalez se define como el conjunto de atributos que posee un producto o servicio, así como el nivel de satisfacción de cada uno de los requerimientos del usuario y deberá cumplir con las funciones y especificaciones para los que ha sido elaborado y deberán ajustarse a lo exigido por el cliente. (Cuatrecasas Arbós & González Babón, 2017)

Orlandoni define a la calidad como ciertas cualidades mensurables de un producto, servicio o proceso, para los que se ha establecido cierto estándar. Se puede decir que un producto o servicio es de calidad cuando satisface los requerimientos de los usuarios en cuanto a seguridad, fiabilidad y servicio. (Orlandoni, 2012, p.269)

Proceso: Es el conjunto de actividades o pasos interrelacionadas que convierten las entradas en salidas. (ISO/IEC, 2014)

Procedimiento: Para Melinkoff (1990) Los procedimientos describen las actividades que se deben seguir en un proceso administrativo en forma detallada, para disminuir errores y obtener un proceso más productivo o efectivos". (Melinkoff, 1990)

Por otro lado según Gómez (1997) "Son planes que siguen un método habitual para manejar actividades futuras. Son guías que se enfocan en la acción más que en el pensamiento, las cuales d etallan la forma exacta en la que ciertas actividades deben realizarse". (Gómez Ceja, 1997)

Elección de un antivirus

Según Pérez (2015) se deben formular unas preguntas al momento de elegir un antivirus, como son:

1. ¿Qué uso tendrá el ordenador en el que se instalará el antivirus?

   Refiriéndose en el ámbito de una organización a las funciones que cumple ordenador dentro de la misma

2. ¿Cuáles son las funciones del usuario que lo utilizará?

Definir la experiencia del usuario con el uso de software en general y con el tipo de software antivirus, ya que una persona inexperta en el tema puede resultarle incómodo y en cierto punto le dificultaría en la realización de sus funciones regulares.

3. ¿Cuáles son las características del ordenador?

Se detallan las características del equipo en el que se va a instalar el software de seguridad informática, ya que si selecciona un antivirus muy potente pero el equipo no tiene las características necesarias para soportarlo este entorpecerá el trabajo del equipo.

1.4. Formulación del problema

1.4.1. Problema general

¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática?

1.4.2. Problemas específicos

- ¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática para la protección de la información?

- ¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática para la reducción del peligro?

1.5. Justificación

1.5.1. Justificación del estudio

Debido a las dificultades dentro de las empresas por preservar la seguridad informática y el óptimo trabajo de sus equipos, es necesario que cuenten con un adecuado software de seguridad informática, por ello deben elegir adecuadamente cual de la amplia gama de productos que está actualmente en el mercado debe adquirir, la presente investigación contribuirá con la creación de una metodología única y adecuada para la evaluación de estos software, apoyando así en la decisión que tomaran las empresas.

1.5.2. Justificación Económica

Al implementar esta nueva metodología, las empresas tendrán la herramienta correcta para seleccionar un software de seguridad informática así poder evitar gastos adicionales en reparaciones y en personal para ello o en el caso extremo no será necesario la adquisición de nuevos equipos ya que será menor la posibilidad de que sean infectados por un malware.

1.5.3. Justificación Tecnológica

Esta nueva metodología ayudará a evitar que las empresas tomen una mala decisión al adquirir un software de seguridad informática y las consecuencias que aquejan si tomaran esta mala decisión. Este estudio también aportará conocimientos sobre determinados pasos a seguir para evaluar el rendimiento de dichos software.

Al crear esta nueva metodología las empresas reducirán sus costos económicos en tiempo, ya que se reducirá el tiempo que se empleaba en la reparación o restauración de un equipo; en recursos humanos, ya que no se tendrá que contratar personal adicional para realizar estos trabajos; materiales, ya que se reducirá la

necesidad de comprar nuevos equipos o adquirir nuevo software además de dinero ya que por lo mencionado no se generará gastos.

1.6. Hipótesis

1.6.1. Hipótesis General

El uso de una metodología tiene beneficio significativo para la selección de software de seguridad informática

1.6.2. Hipótesis Específicas

- El uso de una metodología tiene beneficio significativo para la selección de software de seguridad informática para la protección de la información.

- El uso de una metodología tiene beneficio significativo para la selección de software de seguridad informática para la reducción del peligro.

1.7. Objetivos

1.7.1. Objetivo General

Determinar los beneficios del uso de una metodología para la selección de software de seguridad informática.

1.7.2. Objetivo Específico

- Determinar los beneficios del uso de una metodología para la selección de software de seguridad informática para la protección de la información

- Determinar los beneficios del uso de una metodología para la selección de software de seguridad informática para la protección de la información.

II. MÉTODO

2.1. Diseño de Investigación

2.1.1. Tipo de Estudio

La presente investigación sigue el enfoque cuantitativo también llamado positivista, el cual según Hurtado (2010), es "aquel que se fundamenta en el uso de instrumentos de medición controlada presentando poca atención a los estados subjetivos de quien actúa" (p.6). Haciendo énfasis en la confiabilidad de los datos y orientado al resultado, además utiliza técnicas cuantitativas asumiendo la realidad como estable. (Hurtado de Barrera, 2010)

Así mismo Hernández (2006) indica que la investigación de tipo experimental es aquella en la que se crea la situación y se manipula intencionalmente la variable independiente para ver el efecto de esta manipulación sobre la variable dependiente. Es decir, se altera la variable independiente con el fin de lograr un efecto, en este caso, de manera favorable a la variable dependiente, bajo condiciones rigurosamente controladas con la intención de describir de qué modo y debido a que se produce una situación o acontecimiento particular. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

Así mismo Hernández (2006) define a la investigación aplicada como aquella en la que su finalidad es buscar la resolución de problemas prácticos. Es por ello que esta investigación es de tipo aplicada experimental. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

2.1.2. Diseño de Investigación

El diseño de investigación, para Hernández (2014) "es un plan o estrategia que se desarrolla para obtener la información que se requiere en una investigación y responder al planteamiento". (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

En este sentido el diseño de esta investigación es experimental el cual estudia variables que son manipuladas deliberadamente, al menos una variable independiente para observar su efecto sobre la otra variable.

2.2. Operacionalización de Variables

Tabla 1: Operacionalización de variables

VAR	DEFINICION CONCEPTUAL	DIMEN.	INDICADORES	INSTR
Seguridad informática	La seguridad informática es aquella que fundamentada en políticas y normas internas y externas de la organización se encarga de proteger la información que las organizaciones o personas tienen alojadas en sus equipos o sistemas ante cualquier ataque, reduciendo el peligro físico o lógico al que se ve exhibida. (Baca Urbina, 2016)	Protección de la información	• Confidencialidad: N° de archivos vulnerados/ N° de archivos totales • Integridad: N° de archivos Dañados/ N° de archivos totales • Disponibilidad: N° de archivos Disponibles/ N° de archivos totales	Ficha de observación
		Reducción del peligro	• Nivel de infección: N° de archivos infectados/ N° de archivos totales	

2.3. Población y Muestra

La población es el universo que comprende el conjunto de todos los casos que concuerdan con una serie de especificaciones (lepkowski, 2008).

La muestra es un subgrupo de la población de interés sobre el cual se recolectaran datos con precisión, además de que debe ser representativa de la población. La muestra será de 30 equipos con las mismas condiciones. Por lo tanto es una muestra censal debido a que es finita pequeña y fácil de ubicar (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

2.4. Técnicas e Instrumentos

Arias (2006), define técnica "al procedimiento o forma particular de obtener datos o información. Las técnicas son particulares y específicas de una disciplina, por lo que sirven de complemento al método científico, el cual posee una aplicabilidad general. La aplicación de una técnica conduce a la obtención de información. Como técnicas a emplear son: observación y pruebas (pruebas de normalidad y pruebas de promedios)". (Arias Odón, 2012)

Esta última, tienen como objetivo principal determinar si los datos se ajustan a una determinada distribución. Dado que, se busca elaborar una metodología para la elección de software de seguridad informática y aplicarla para determinar si existe un beneficio de aplicar dicha metodología. De esta manera, como instrumento se utilizará la hoja de recolección de datos, que sirve como recurso al investigador para registrar la información sobre las variables presentes en la investigación.

2.5. Métodos de análisis de datos

El método será a través de la estadística descriptiva la cual permite tabular y reflejar mediante gráficos los resultados emitidos por la muestra en estudio. Se analizara la desviación estándar, media, coeficiente de variabilidad. T- Student.

Para la cual se hará uso de la herramienta SPSS Statistics para realizar el procesamiento de datos y así generar los gráficos a analizar.

2.6. Aspectos Éticos

El presente trabajo de investigación se basará respetando los valores éticos y en la veracidad de la recolección de los datos. Así mismo los principios, normas, políticas y conductas para la representación de los datos obtenidos.

III. RESULTADOS

En este capítulo se especifican los resultados obtenidos de las investigaciones efectuando el uso de los indicadores “confidencialidad”, “Integridad”, “disponibilidad” y medidas de protección”. Además, se aplicara la metodología desarrollada para evaluar el rendimiento de software de seguridad informática, los datos obtenidos de las muestras aplicando los indicadores (tanto en el pre-test y el post-test) se evaluaran con el software IBM SPSS Statistics v.25.

Luego de analizar los resultados del Pre-test y Post-Test, se tienen los siguientes resultados:

Indicador: Confidencialidad

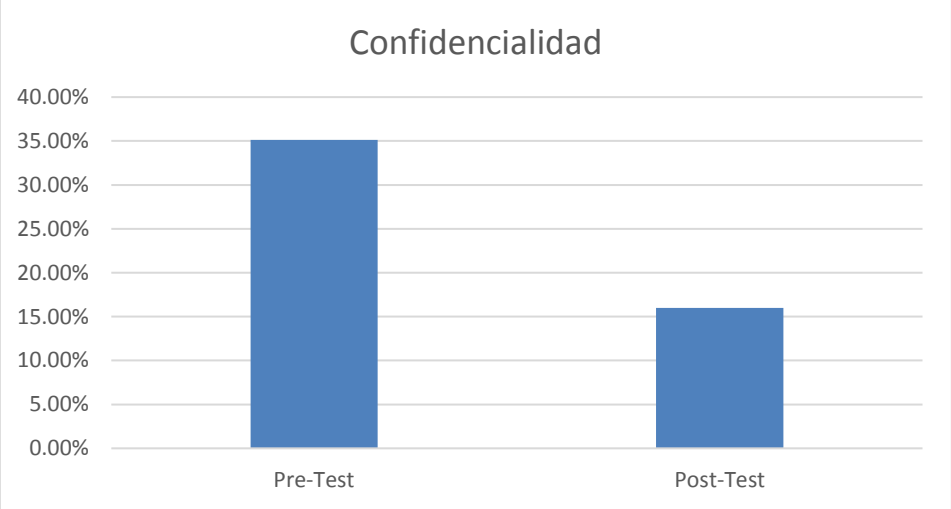


Figura 2: Comparación Pre y Post indicador Confidencialidad

Indicador: Integridad

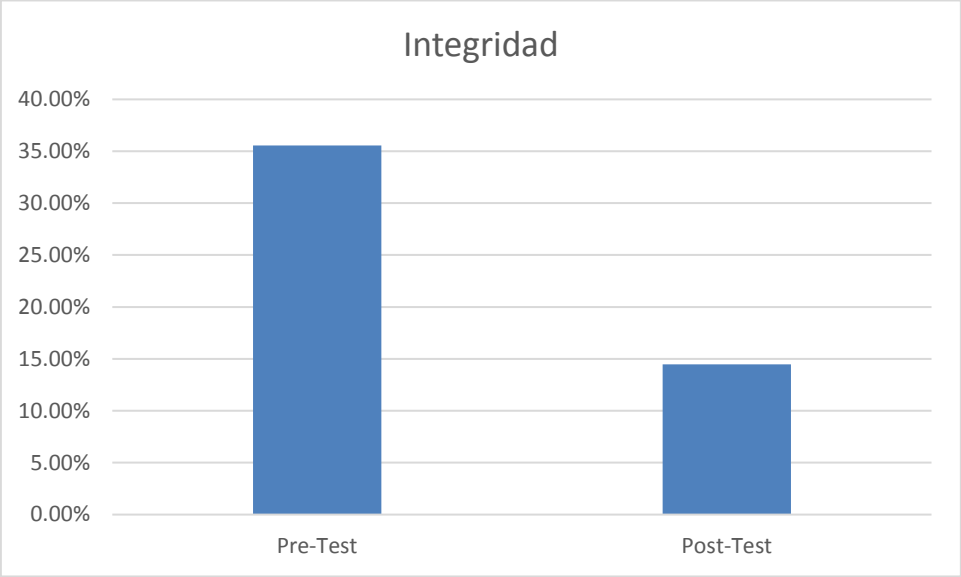


Figura 3: Comparación Pre y Post indicador Integridad

Indicador: Disponibilidad

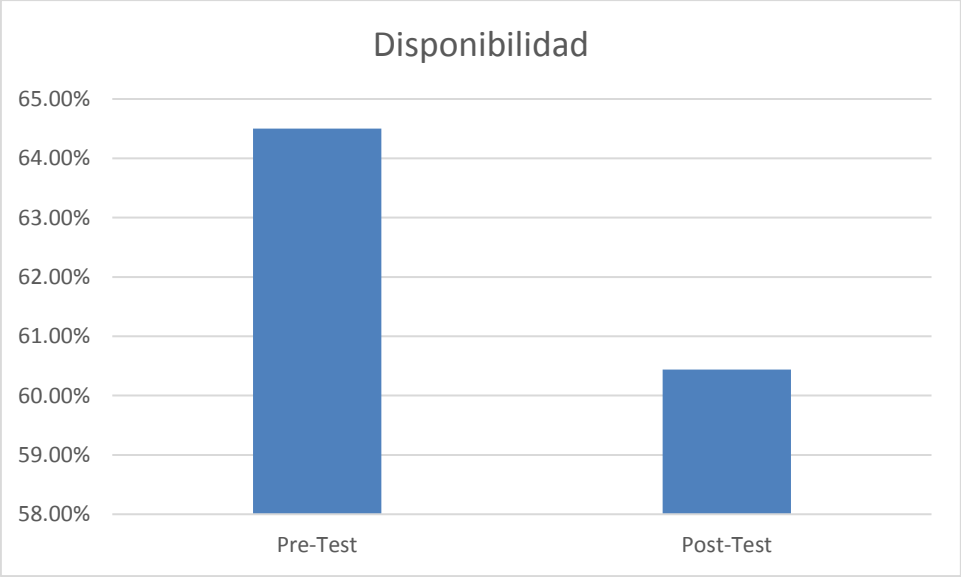


Figura 4: Comparación Pre y Post indicador Disponibilidad

Indicador: Nivel de Infección

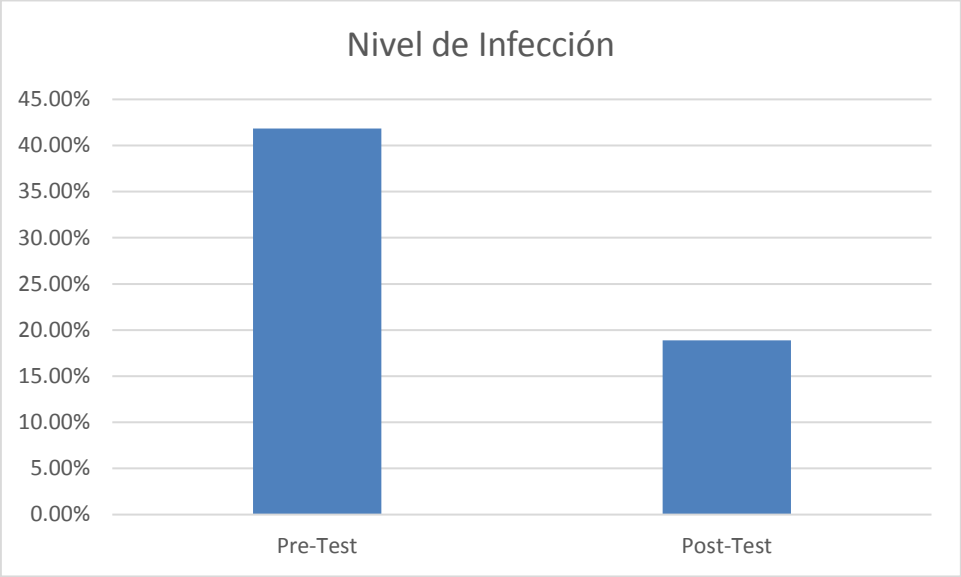


Figura 5: Comparación Pre y Post indicador Nivel de Infección

Podemos apreciar que en cuanto a Confidencialidad hubo una mejora del 19.16% al aplicar la metodología, asi mismo para el indicador Integridad se observo una mejora de un 21.08%, de la misma manera la disponibilidad mejoró en un 4.06% y por ultimo el nivel de infección se redujo en un 22.96%.

Prueba de normalidad según Shapiro y Wilks

Según Dagoberto Salg87uado Horta las pruebas de normalidad:

> "Mide el ajuste de la muestra al dibujarla en papel probabilístico normal a una recta. Se rechaza la normalidad cuando el ajuste es malo, que corresponde a valores pequeños del estadístico."

Se utiliza este tipo de prueba de normalidad para cada una de las dimensiones, asi también en sus indicadores. Puesto que

- Si la muestra es mayor a 50 se deberá usar la las pruebas según Kolmogorov

- Si la muestra es menor a 50 se deberá usar la las pruebas según Shapiro y Wilks

Como se mencionó nuestra muestra es de 30 frecuencias o pruebas realizadas, por lo tanto al ser menor a 50 el ingreso de datos se realizó en base a la recopilación según las pruebas realizadas para cada uno de los indicadores en ambos casos para el pre-test como para el post-test.

Con el uso de la herramienta SPSS con un nivel de confiabilidad del 95%, bajo las siguientes indicaciones:

- Si Sig<0.05 entonces tiene una distribución no normal.
- Si Sig=>0.05 entonces tiene una distribución normal.

Donde:

Sig= Nivel crítico del contraste

Posterior al análisis de las pruebas de normalidad a los indicadores se obtuvieron los resultados siguientes:

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Confidencialidad_Post	,087	30	,200*	,962	30	,353
Integridad_Post	,117	30	,200*	,969	30	,503
Disponibilidad_Post	,117	30	,200*	,969	30	,503
Nivel_Infección_Post	,089	30	,200*	,961	30	,324

Figura 6: Prueba de normalidad

Se observa que para cada indicador el grado de significancia es mayor a 0.05 en cada uno de los casos analizados, por lo tanto adopta una distribucion normal.

Estadísticas de grupo

	Tipo	N	Media	Desv. Desviación	Desv. Error promedio
Confidencialidad	PreTest	30	,35143	,031205	,005697
	PosTest	30	,15982	,032009	,005844
Integridad	PreTest	30	,35497	,039029	,007126
	PosTest	30	,14481	,020923	,003820
Disponibilidad	PreTest	30	,64503	,039029	,007126
	PosTest	30	,85519	,020923	,003820
Nivel_Infección	PreTest	30	,41832	,028845	,005266
	PosTest	30	,18874	,021635	,003950

Figura 7: Estadísticas de Grupo

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Confidencialidad	Se asumen varianzas iguales	,075	,785	23,478	58	,000	,191611	,008161	,175274	,207948
	No se asumen varianzas iguales			23,478	57,963	,000	,191611	,008161	,175274	,207949
Integridad	Se asumen varianzas iguales	23,824	,000	25,993	58	,000	,210155	,008085	,193971	,226338
	No se asumen varianzas iguales			25,993	44,397	,000	,210155	,008085	,193864	,226445
Disponibilidad	Se asumen varianzas iguales	23,824	,000	-25,993	58	,000	-,210155	,008085	-,226338	-,193971
	No se asumen varianzas iguales			-25,993	44,397	,000	-,210155	,008085	-,226445	-,193864
Nivel_Infección	Se asumen varianzas iguales	3,626	,062	34,874	58	,000	,229581	,006583	,216403	,242758
	No se asumen varianzas iguales			34,874	53,785	,000	,229581	,006583	,216381	,242780

Figura 8: Prueba de muestras independientes

Prueba T-Studen

H1: EXISTE una diferencia significativa entre la media de cada indicador entre cada uno de los

software de seguridad informática.

H0: NO EXISTE una diferencia significativa entre la media de cada indicador entre cada uno de los software de seguridad informática.

IV. DISCUSION

Contrastando la información de los resultados tanto en el pre-test como en el post-test, teniendo como resultado que al aplicar la metodología de elección de software de seguridad informática se observa que cada uno de los indicadores se ve afectados dependiendo sea el caso. Como se aprecia en cada equipo se tiene diferente impacto en los indicadores descritos anteriormente mostrando un beneficio significativo el aplicar la metodología.

1) En la Confidencialidad hubo una mejora del 19.16% en cuanto a la protección de la información, ya que en el pretest se tuvo un resultado promedio de 35.14% y al aplicar la metodología se logró reducir el porcentaje de confidencialidad vulnerada a un 15.98%.

En comparación con la investigación ejecutada por Alvarez, Nuñez, Reyes y González en su artículo científico Selección de productos antivirus. Una mirada actual desde el sector de la salud en Cuba, se indica que llegan a la conclusión de que el mejor antivirus a usar será el que resulte viable según los requerimientos de cada usuario y de las condiciones técnicas que lo permitan sostener. Mencionando que el porcentaje de confidencialidad al elegir en correcto software de seguridad fue de 16.63%.

2) En la Integridad se observo una mejora de un 21.08% en cuanto a la protección de la información ya que en el pretest se tuvo un resultado promedio de 35.56% y al aplicar la metodología se logró reducir el porcentaje de Integridad vulnerada a un 14.48%.

En comparación con la investigación realizada por Haffejee e Irwin en su artículo científico Testing antivirus engines to determine their effectiveness as a security layer, se indica que llegan a la conclusión de que una vez que una aplicación maliciosa se combina con las técnicas de evasión, esta es capaz de pasar por alto ante el análisis de un significativo número de antivirus, es por ello que un antivirus no debería considerarse un medio eficaz de protección. Además se menciona que al verificar la integridad de los datos durante el análisis tuvo una mejora del 18.76%

3) La Disponibilidad mejoró en un 4.06% en cuanto a la protección de la información ya que en el pretest se tuvo un resultado promedio de 64.50% y al aplicar la metodología se logró

reducir el porcentaje de Disponibilidad vulnerada a un 60.44%.

En comparación con la investigación realizada por Solarte, Enriquez y Benavides en su artículo científico Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001 se indica que llegan a la conclusión de que no hay existencia de una cultura de seguridad de la información dentro de las instituciones, tampoco se encontró sistemas de control de seguridad informática y de información, y mucho menos, procesos y procedimientos documentados para protección de la información. Además se menciona que al analizar la disponibilidad de la información durante el proceso, se vio afectada en un 16.74% aplicando lo indicado en la ISO / IEC 27001.

4) En el nivel de infección se redujo en un 22.96% en cuanto a la reducción del peligro ya que en el pretest se tuvo un resultado promedio de 41.83% y al aplicar la metodología se logró reducir el porcentaje del nivel de infección a un 18.87%.

En comparación con la investigación realizada por Norouzi y Parsa en su artículo científico Verification of the protection services in antivirus systems by using NuSMV model checker se indica que llegan a la conclusión de que las propiedades esperadas de sistemas antivirus se extraen de comportamiento de control en forma de fórmulas lógica temporal. También se implementó los modelos de comportamiento de enfoque de sistemas antivirus por la herramienta ArgoUML y el comprobador de modelos NuSMV. En dicha investigación se muestra que el nivel de infección al aplicar un antivirus a un equipo se redujo en un 26.34%

V. CONCLUSIONES

Según este análisis de los indicadores mencionados se llegó a concluir que al aplicar la metodología el nivel de seguridad de información en cuanto a protección de datos y reducción de peligro se ven beneficiados de manera positiva, dando así a los usuarios una herramienta más para proteger su información.

Además, en base a la aplicación de la metodología se determinó que los software antimalware licenciados en cuanto al tiempo de respuesta en base a los indicadores Tiempo de Arranque del sistema, Tiempo de inicio de aplicaciones, Tiempo de análisis de Malware tiene mejor rendimiento que los software antimalware libre al ser evaluados en los mismos indicadores.

También se determinó que los software antimalware licenciados en cuanto a restricciones en el uso de los recursos en base a los indicadores cantidad de memoria ocupada y uso del CPU durante escaneo tiene mejor rendimiento que los software antimalware libre al ser evaluados en los mismos indicadores.

Podemos concluir que en cuanto a Confidencialidad hubo una mejora del 19.16% al aplicar la metodología pasando de un 35.14% a un 15.98%.

Asi mismo para el indicador Integridad se observo una mejora de un 21.08% reduciendose de un 35.56% hasta un 14.48%.

De la misma manera la disponibilidad mejoró en un 4.06% disminuyendo de un 64.50% a un 60.44%.

Por ultimo el nivel de infección se redujo en un 22.96% visualizando una redución desde 41.83% hasta 18.87%.

VI. RECOMENDACIONES

Dejar en reposo luego de cada instalación para evitar alteraciones en los datos recolectados en las pruebas.

Revisar adecuadamente las características del software antimalware a adquirir con la finalidad de que los equipos estén adecuadamente protegidos.

Utilizar los lineamientos planteados como guía para futuras evaluaciones de este tipo de software.

En el caso de usarse para una empresa realizar las pruebas en un ambiente aislado para evitar perjudicar a otras áreas de trabajo.

VII. REFERENCIAS

Aguilera López, P. (2010). *Seguridad Informática.* Madrid: Editex.

Alimenti, O., Friedrich, G., Reggiani, G., Tonietti, S., Velazquez, G., & Cofre, L. (2012). Análisis del Tiempo de Respuesta en entorno de Tiempo Real sobre el MAC 802.11e. *AST*, 132 - 142.

Alvarez Zaldivar, Y., Gonzáles Torres, M., Nuñez Maturel, L., & Reyes Dixson, Y. (2014). Selección de productos antivirus. Una mirada actual desde el sector de la salud en Cuba. *Revista Cubana de Informática Médica*, 140-150.

Arias Odón, F. (2012). *El Proyecto de Investigación. Introducción a la Metodología Científica.* Caracas: Episteme C.A.

Avalos, H., & Gómez, E. (2015). Seguridad de la información, Generación y Mitigación de un Ataque de Denegación de Servicios. *Revista Tecnológica ESPOL – RTE*, 54-72.

Baca Urbina, G. (2016). *Ningún eBook disponible.* México DF: Grupo Editorial Patria.

Botella, P., Burgués, X., Carvallo, J., Franch, X., Grau, G., Marco, J., & Quer, C. (2004). ISO/IEC 9126 in practice: what do we need to know? *In Proceedings of the 1st Software Measurement European Forum*.

Cardozo González, L. F., & García Severiche, B. (s.f.). Malware: Historia y Clasificación. 1-5.

Corrales Cortes, T., Gutiérrez Vera, F., Ortega González, C., & Páramo Domínguez, V. (2015). Backdoor de los antivirus. *Pistas Educativas*, 48-61.

Cuatrecasas Arbós, L., & González Babón, J. (2017). *Gestión integral de la calidad: Implantación, control y certificación.* Barcelona: Profit Editorial.

Gómez Ceja, G. (1997). *SISTEMAS ADMINISTRATIVOS: ANÁLISIS Y DISEÑO.* McGraw-

Hill.

González Medina, L., & Salazar Rubio, J. (2012). Clasificación de malware mediante clusterización. *Memorias del primer concurso de investigación, desarrollo e innovación tecnológica idit*, 25-30.

Haffejee, J., & Irwin, B. (2014). Testing antivirus engines to determine their. *IEEE Xplore*, 1-6.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la investigación.* México: Mcgraw-Hill.

Hurtado de Barrera, J. (2010). *El proyecto de investigación: Comprensión holistica de la investigación y la metodología.* Caracas: Sypal.

ISO/IEC. (2013). *Information technology - Security techniques - Information security.*

ISO/IEC. (2014). *Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

Jarrín Zambrano, G. (Junio de 2010). Análisis de rendimiento de los servidores de firewall, mail, y aplicaciones externas para la organización Illiniza S.A. *Tesis de Pregrado*. Quito, Ecuador.

Lai, K., & Wren, D. (09 de Febrero de 2011). Small Business Endpoint Protection Performance Benchmarks.

Lalonde L´evesque, F., Carlton R., D., Fernandez, J., Chaisson, S., & Somayaji, A. (2012). Methodology for a Field Study. *J. Blythe, S. Dietrich, and L.J. Camp (Eds.)*, 80-85.

Melinkoff, R. (1990). *Los procesos administrativos.* Caracas.

Ministerio de Educación. (2011). *Guía tecnica sobre evaluación de software para la administración pública.* Obtenido de

http://www.gobiernodigital.gob.pe/Bancos/Banco_Normas/archivos/Guia-Evaluacion-SW.pdf

Mohaisen, A., & Alrawi, O. (2014). AV-Meter: An Evaluation of Antivirus Scans and Labels. *S. Dietrich*, 112-131.

Morales, J., Xu, S., & Sandhu, R. (2012). Analyzing Malware Detection Efficiency with Multiple Anti-Malware Programs. *ASE*, 56-66.

Mosquera Quinto, A. (2011). Guía de Referencia: Los antivirus y sus tendencias futuras. *Tesis de pregrado*. Colombia.

Navia Mendoza, M., Párraga Álava, J., Molina Garzón, G., & Vidal Loor, J. (2015). Efectividad y eficiencia de los antivirus gratuitos combinados frente al malware. *Espamciencia*, 45-49.

Norouzi, M., Parsa, S., & Mahjur, A. (2014). A new approach for formal behavioral modeling of protection services in antivirus systems. *International Journal in Foundations of Computer Science & Technology (IJFCST)*, 77-85.

Orlandoni Merli, G. (2012). Gestión de la Calidad: Control Estadístico y Seis Sigma. *TELOS. Revista de Estudios Interdisciplinarios en Ciencias Sociales*, 269-274.

Padilla Espinoza, M. (2010). Antivirus: Una herramienta indispensable para nuestra seguridad. *Punto de seguridad*, 6-10.

Pérez Carvajal, R. (2015). *Mantenimiento del software. IFCT0510.* Málaga: IC Editorial.

Rainer, K., & Cegielski, C. (2010). *Introduction to Information Systems: Enabling and Transforming Business.* Estados Unidos de America: John Wiley & Sons.

Santilla, J. (2010). Firewalls, controlando el acceso a la red. *Punto de Seguridad*, 3-5.

Scalone, F. (2006). Estudio comparativo de los modelos y estándares de calidad del software.

Tesis de maestría. Buenos Aires, Argentina.

Solarte Solarte, F., Enriquez Rosero, E., & Benavides Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE*, 492-507.

Trudel, S., Lavoie, J.-M., Paré, M.-C., & Suryn, W. (2006). PEM: The small company-dedicated software process quality evaluation method combining CMMI and ISO/IEC 14598. *Software Quality Control*, 7-23.

Valdés Rodriguez, M. (2010). Antispyware: Protegiendote de los Espías. *Punto de Seguridad*, 11-12.

Vivanco Muñoz, P., Cortez Vásquez, A., & Bustamante Olivera, V. (2011). La seguridad de la información. *Revista de Investigación de Sistemas e Informática*, 25-30.

VIII. ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VAR	DIMENSIONES	INDICADORES
General	General	General	**VI**		
¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática?	Determinar los beneficios del uso de una metodología para la selección de software de seguridad informática	El uso de una metodología tiene beneficio significativo para la selección de software de seguridad informática	**Metodología**		
Especifico	Especifico	Especifico	**VD**		
¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática para la protección de la información?	Determinar los beneficios del uso de una metodología para la selección de software de seguridad informática para la protección de la información	El uso de una metodología tiene beneficio significativo para la selección de software de seguridad informática para la protección de la información	**seguridad informática**	Protección de la información	Confidencialidad Integridad Disponibilidad
¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática para la reducción del peligro?	¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática para la reducción del peligro?	¿Cuáles serían los beneficios del uso de una metodología para la selección de software de seguridad informática para la reducción del peligro?		Reducción del peligro	Nivel de infección

ANEXO 2: METODOLOGÍA PARA LA ELECCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA

1. Objetivo

El objetivo de la metodología es evaluar el software de seguridad informática, con la finalidad de identificar si dichos software brindan la protección necesaria que deben proporcionar para evitar pérdidas a la organización.

2. Alcance

El alcance para esta metodología incluye la evaluación de tres software de seguridad informática por tipo, es decir tres software libre y tres licenciados previamente seleccionados para las pruebas, siendo estos Avast, Eset, Kaspersky, Comodo, Moon Secure Antivirus y ClamWin. La evaluación se basa en:

A. Evaluar el Tiempo de arranque del sistema el cual implica realizar el proceso de encendido y apagado del equipo antes y después de la instalación del software de seguridad informática.

B. Al evaluar el Tiempo de inicio de aplicaciones implica abrir y cerrar una o más aplicaciones antes y después de la instalación del software de seguridad informática.

C. Al evaluar el Tiempo de análisis de malware implica tomar los resultados después del proceso de escaneo de cada software de seguridad informática instalado.

D. Al evaluar el Cantidad de memoria RAM ocupada implica evaluar la cantidad de memoria del computador antes y después de la instalación del software de seguridad informática.

E. Al evaluar el Uso del CPU durante escaneo implica evaluar la cantidad de CPU usado antes y después de la instalación del software de seguridad informática.

3. Herramientas

Para las pruebas de esta metodología se instaló los software de seguridad informática seleccionados (Avast, Eset, Kaspersky, Comodo, Moon Secure Antivirus y ClamWin) además herramientas para evaluar aspectos de rendimiento como tiempo de arranque, tiempo de inicio de aplicaciones, cantidad de memoria RAM, uso del CPU, todos ellos software opensource detallados de la siguiente manera:

A. Para evaluar el Tiempo de arranque del sistema se utiliza la herramienta BootRacer, herramienta de uso libre no comercial que permite medir los valores de arranque de un equipo Windows bajo tres parámetros: el arranque en sí, el tiempo de espera por contraseña, y el tiempo en el que se considera que el escritorio está listo para dar acceso a las aplicaciones.

B. Para evaluar el Tiempo de inicio de aplicaciones se utiliza la herramienta AppTimer, la cual cronometra la velocidad de apertura de cualquier aplicación, al abrir y cerrar la aplicación el programa mide el tiempo de carga.

C. Para evaluar el Tiempo de análisis de malware se toma los datos brindados por cada software de seguridad informática utilizado.

D. Para evaluar el Cantidad de memoria RAM ocupada se utiliza la herramienta CPU-Z, la cual nos brinda cuanto se consume en memoria estando el computador en reposo y usando algún programa, en este caso los software de seguridad informática seleccionados.

E. Para evaluar el Uso del CPU durante escaneo se utiliza la herramienta NovaBench, la cual nos brinda cuanto en recursos se consume estando el computador en reposo y usando en este caso los software de seguridad informática seleccionados.

4. Proceso

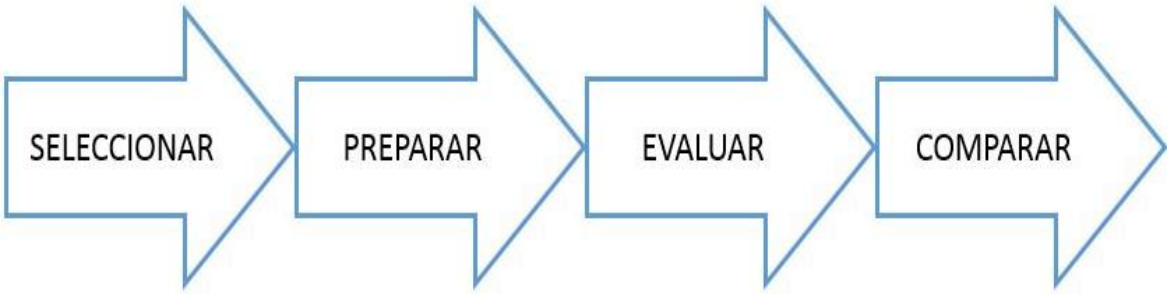


Figura 9: Proceso MERSAM

A. Selección del software de seguridad informática a evaluar:

Se considera la selección del software de seguridad informática en base a la investigación realizada y a la documentación encontrada. Previamente seleccionados, siendo estos (Avast, Eset, Kaspersky, Comodo, Moon Secure Antivirus y ClamWin)

B. Preparar los equipos y software para el análisis:

Las pruebas se realizaron en equipos con las características descritas en la tabla 4. En cada uno de ellos se instalaran los softwares de análisis de rendimiento y los software de seguridad informática previamente seleccionados.

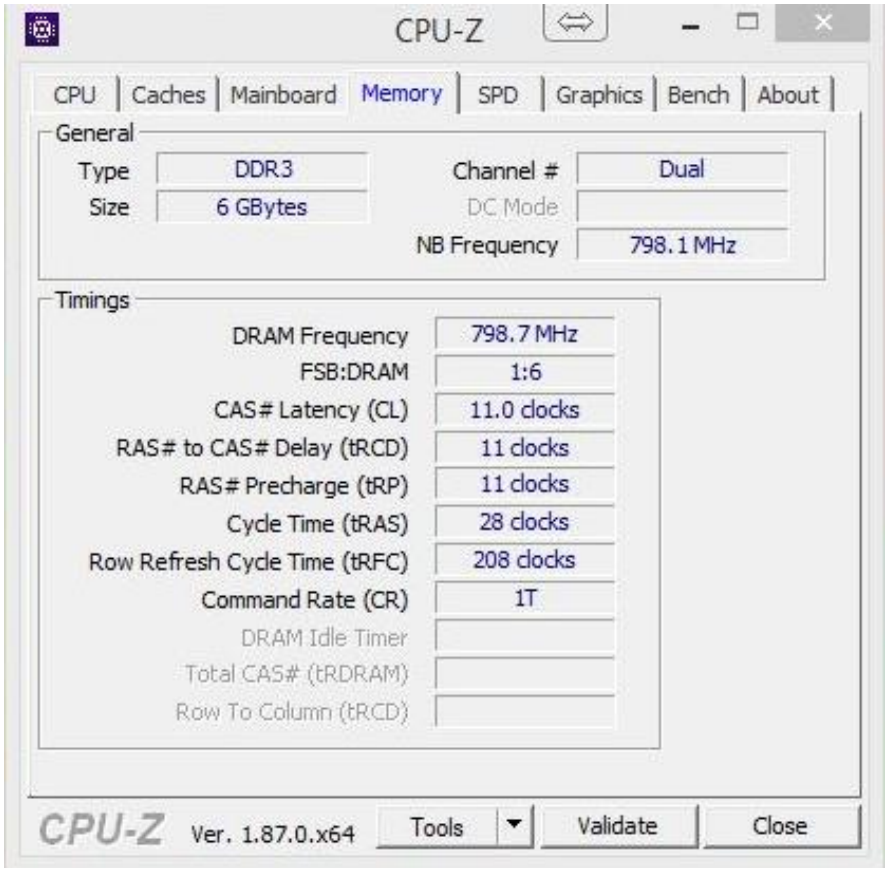


Figura 10: CPU-Z Datos iniciales de memoria RAM

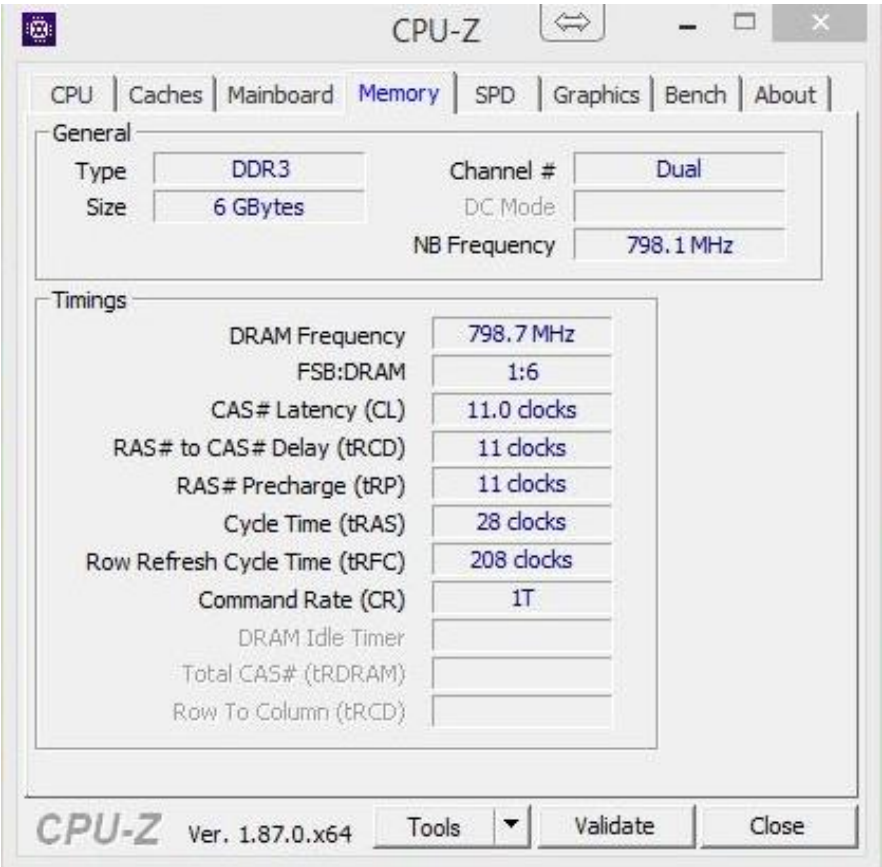


Figura 11: CPU-Z Datos iniciales de CPU

Tabla 2: Especificación de Equipos

Equipo	**Memoria RAM**	**Procesador**	**Windows**	**Tipo de Sistema**
Laptop	6 GB	Core i5	Windows 8.1	x64

C. Realizar la evaluación con cada una de los indicadores de rendimiento:

En los equipos descritos anteriormente se procedió con la instalación de las herramientas para la evaluación del rendimiento del equipo, luego de instalarlas se le dio un tiempo de reposo, es decir se dejó de utilizar algún software para que dicha instalación no afecte en los resultados de la evaluación, posteriormente se procedió con la instalación de cada uno de los software de seguridad informática.

Después de instalar cada software de seguridad informática es necesario identificar los indicadores a evaluar, los cuales se definieron en base a la investigación realizada. Serán medidos para determinar la comparación entre cada software de seguridad informática. Estos indicadores se definen en la siguiente tabla.

Tabla 3: Herramienta por indicador

Indicadores	Definición
Tiempo de arranque del sistema	Tiempo en el que demora en arrancar el sistema operativo.
Tiempo de inicio de aplicaciones	Tiempo en el que demora en iniciar las aplicaciones
Tiempo de análisis de malware	Tiempo en el cada software demora en realizar el análisis
Cantidad de Malware detectado	Cantidad de malware detectado por software
Cantidad de memoria RAM ocupada	Cantidad de memoria usada después de la instalación de cada software de seguridad informática y durante un análisis.
Uso del CPU durante escaneo	Cantidad de CPU usado después de la instalación de cada software de seguridad informática y durante un análisis.

Para evaluar cada uno de los indicadores se usara las siguientes herramientas Open Source:

BootRacer: Luego de instalar cada software de seguridad informática y del tiempo de reposo, haciendo uso de esta herramienta se analizó el tiempo transcurrido desde que se presiona el botón de encendido hasta que el equipo carga completamente, es decir está listo para ser usado por el usuario.

Figura 12: Interface BootRacer

AppTimer: Luego de instalar cada software de seguridad informática y del tiempo de reposo, haciendo uso de esta herramienta se analizó el tiempo en que un software como Excel.

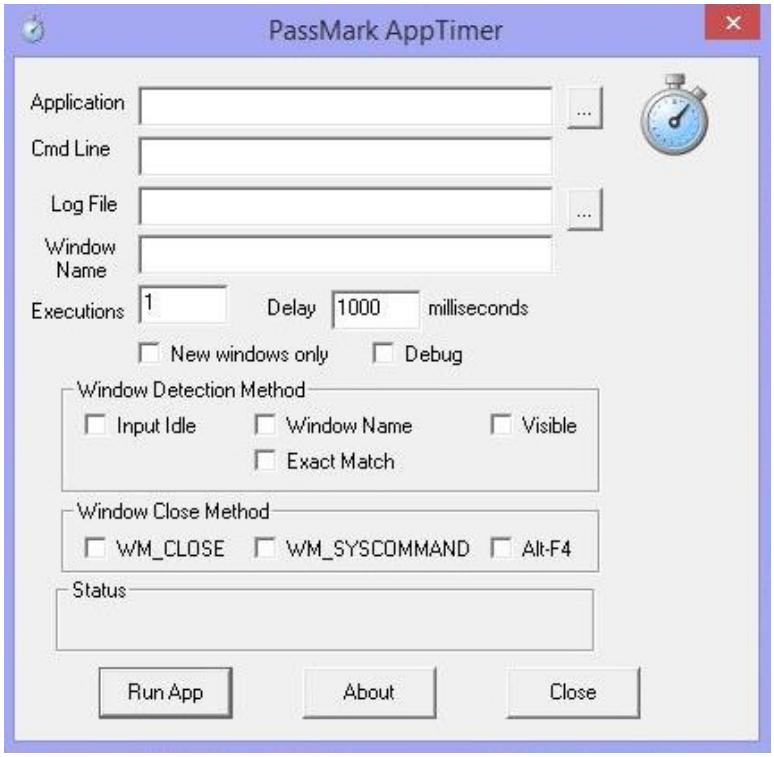


Figura 13: Interface AppTimer

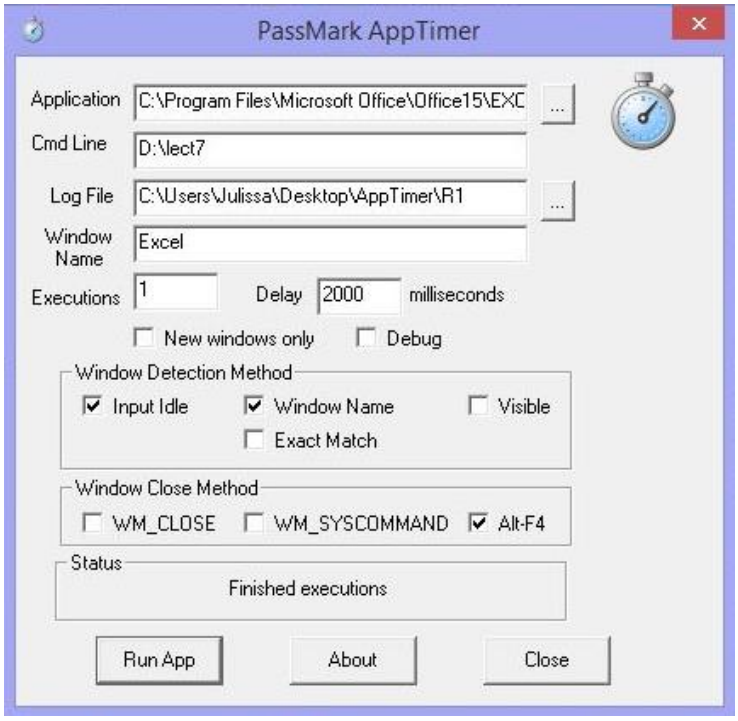


Figura 14: Configuración AppTimer

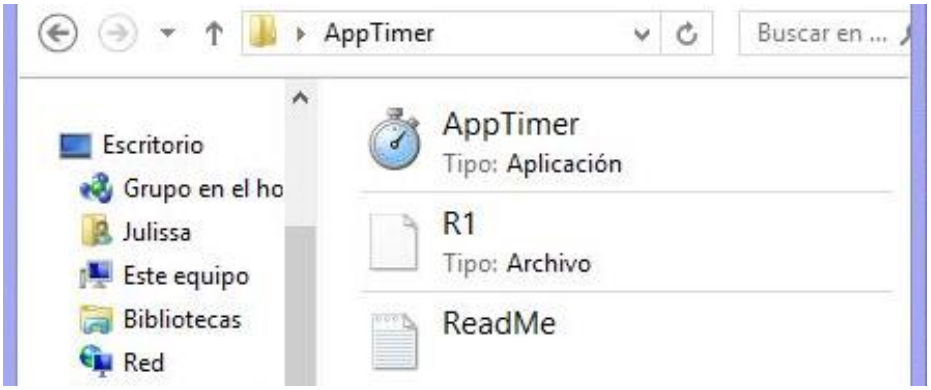


Figura 15: Carpeta AppTimer

CPU-Z: Luego de instalar cada software de seguridad informática y del tiempo de reposo, haciendo uso de esta herramienta se analizó cantidad de CPU usado después de la instalación de cada software de seguridad informática.

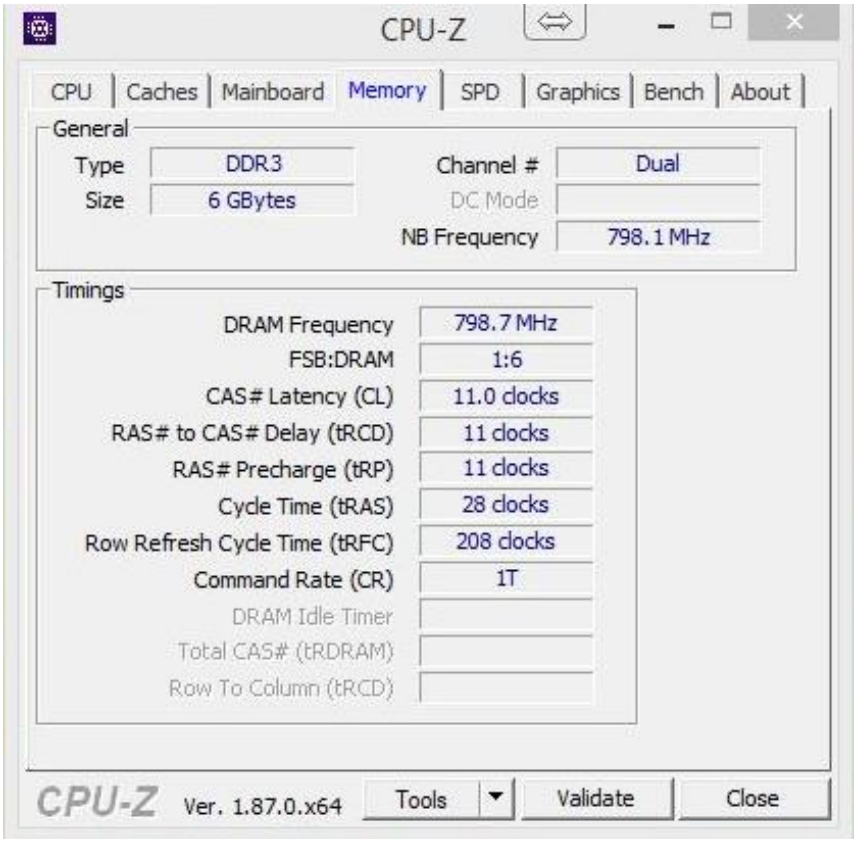


Figura 16: Interface CPU-Z

NovaBench: Luego de instalar cada software de seguridad informática y del tiempo de reposo, haciendo uso de esta herramienta se analizó la cantidad de memoria RAM ocupada cuando cada software de seguridad informática está instalado.

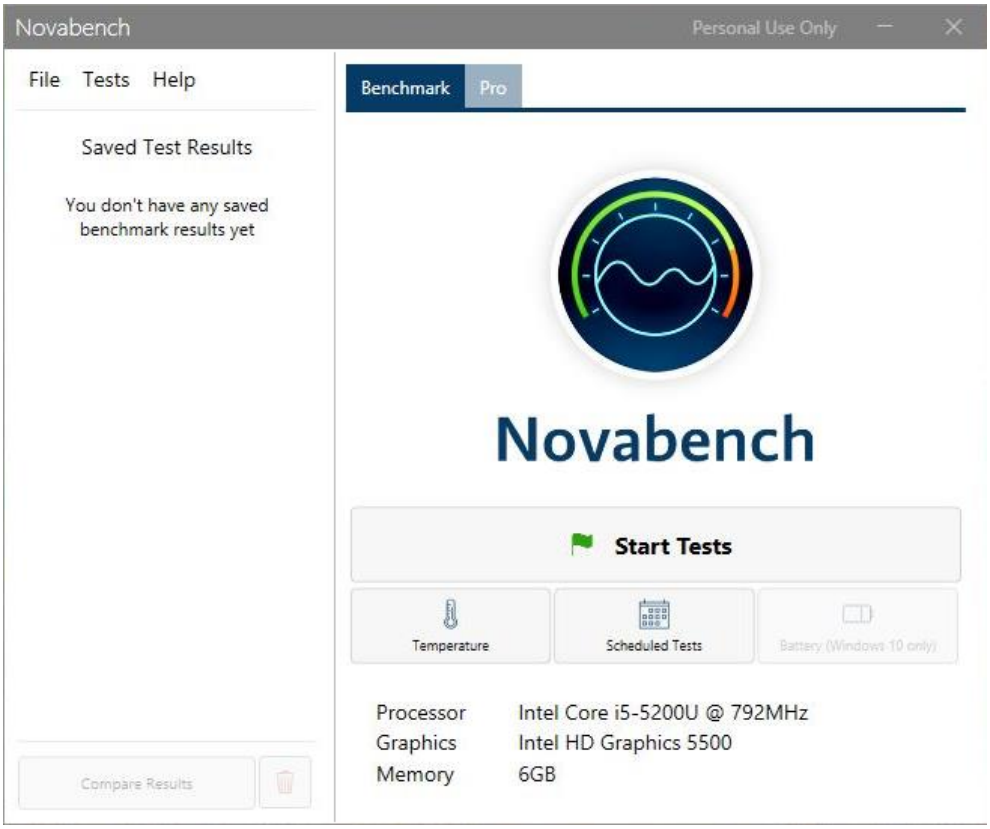


Figura 17: Interface Novabench

D. Evaluar los datos brindados: Los datos obtenidos de cada una de las herramientas o información de cada software son anotados en el formato de resultados de evaluación (ver anexo a). El cual nos detalla cada uno de los resultados para luego ser comparados y elegir así dos de ellos.

E. Elaborar un informe preliminar de rendimiento de software de seguridad informática: Con todos los datos obtenidos se elaborará el informe preliminar de evaluación. (ver anexo a) en el cual solo se seleccionara dos de los software con mejores resultados en la evaluación para luego elegir solo uno de ellos.

F. Elaborar informe final: Luego de revisar y hacer un análisis con los datos obtenidos, los cuales han sido plasmados en el informe preliminar se seleccionará solo uno de ellos dependiendo al análisis hecho.

5. Salidas

Documentación del proceso.

ANEXO 3: RENDIMIENTO EN CUANTO A TA

Hoja de Recolección de Datos

Dirigido a la Muestra en estudio

Frecuencia	Avast	Eset	Kaspersky	Comodo	Moon Secure Antivirus	ClamWin

TA: Tiempo de Arranque del sistema

ANEXO 4: RENDIMIENTO EN CUANTO A TIA

Hoja de Recolección de Datos

Dirigido a la Muestra en estudio

Frecuencia	Avast	Eset	Kaspersky	Comodo	Moon Secure Antivirus	ClamWin

TIA: Tiempo de inicio de aplicaciones

ANEXO 5: RENDIMIENTO EN CUANTO A TAn

Hoja de Recolección de Datos

Dirigido a la Muestra en estudio

Frecuencias	Avast	Eset	Kaspersky	Comodo	Moon Secure Antivirus	ClamWin

TAn: Tiempo de análisis de Malware

ANEXO 6: RENDIMIENTO EN CUANTO A MD

Hoja de Recolección de Datos

Dirigido a la Muestra en estudio

Frecuencias	Avast	Eset	Kaspersky	Comodo	Moon Secure Antivirus	ClamWin

MD: Malware detectado

ANEXO 7: RENDIMIENTO EN CUANTO A CMO

Hoja de Recolección de Datos

Dirigido a la Muestra en estudio

Frecuencia	Avast	Eset	Kaspersky	Comodo	Moon Secure Antivirus	ClamWin

CMO: Cantidad de memoria ocupada

ANEXO 8: RENDIMIENTO EN CUANTO A UDE

Hoja de Recolección de Datos

Dirigido a la Muestra en estudio

Frecuencia	Avast	Eset	Kaspersky	Comodo	Moon Secure Antivirus	ClamWin

UDE: Uso del CPU durante escaneo

ANEXO 9: RESULTADOS DE LA EVALUACIÓN

Toma de datos en base a los indicadores para cada uno de los antivirus

Software	TA	TIA	Tan	MD	CMO	UDE

TA: Tiempo de Arranque del sistema

TIA: Tiempo de inicio de aplicaciones

TAn: Tiempo de análisis de Malware

MD: Malware detectado

CMO: Cantidad de memoria ocupada

UDE: Uso del CPU durante escaneo

ANEXO 10: EVALUACIÓN PRELIMINAR DE SOFTWARE DE SEGURIDAD INFORMÁTICA

Resultados en base a solo dos de los software evaluados

INDICADORES		
TA		
TIA		
Tan		
MD		
CMO		
UDE		

Evaluación Comparativa:

_____

_____

_____

_____

_____

_____

_____

TA: Tiempo de Arranque del sistema

TIA: Tiempo de inicio de aplicaciones

TAn: Tiempo de análisis de Malware

MD: Malware detectado

CMO: Cantidad de memoria ocupada

UDE: Uso del CPU durante escaneo

ANEXO 11: INFORME FINAL

En base a los resultados obtenidos para la evaluación de rendimiento de software antimalware, se llega a elegir el software descrito posteriormente debido a que cuenta con las características necesarias para una protección optima de la información sin perjudicar el rendimiento de los mismos

INDICADORES	
TA	
TIA	
Tan	
MD	
CMO	
UDE	

Adicional a ello:

_____

_____

_____

_____

_____

Donde:

TA: Tiempo de Arranque del sistema

TIA: Tiempo de inicio de aplicaciones

TAn: Tiempo de análisis de Malware

MD: Malware detectado

CMO: Cantidad de memoria ocupada

UDE: Uso del CPU durante escaneo

ANEXO 12: RESULTADOS DE LA METODOLOGÍA

Tabla 4: Condiciones iniciales del equipo

Equipo	TA	TIA	Tan	MD	CMO	UDE
Laptop	69.312	0.3289	0	0	136	798.1

Tabla 5: Resultados del análisis para cada caso

	TA	TIA	Tan	MD	CMO	UDE
Avast	69.875	0,9837	165	52	156	1197.57
Eset	154,703	0,4156	232	37	141	798,67
Kaspersky	161,203	1.6313	195	55	147	1297,37
Comodo	127,703	1.1229	147	43	142	1179,64
Moon Secure Antivirus	144,751	0,7559	167	39	163	2054,42
ClamWin	123,296	0,6868	23	35	140	798,67

Donde:

TA: Tiempo de Arranque del sistema

TIA: Tiempo de inicio de aplicaciones

TAn: Tiempo de análisis de Malware

MD: Malware detectado

CMO: Cantidad de memoria ocupada

UDE: Uso del CPU durante escaneo

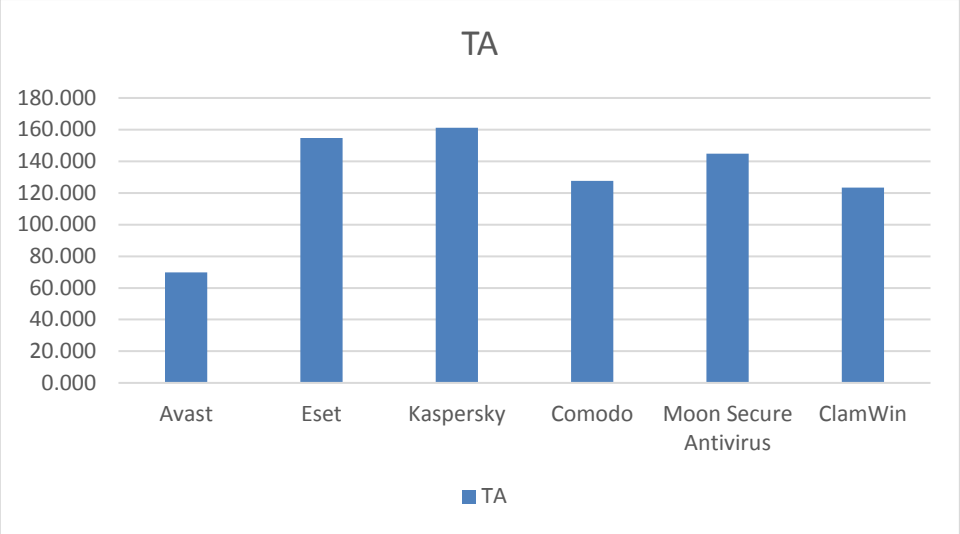


Figura 18: Tiempo de arranque del sistema

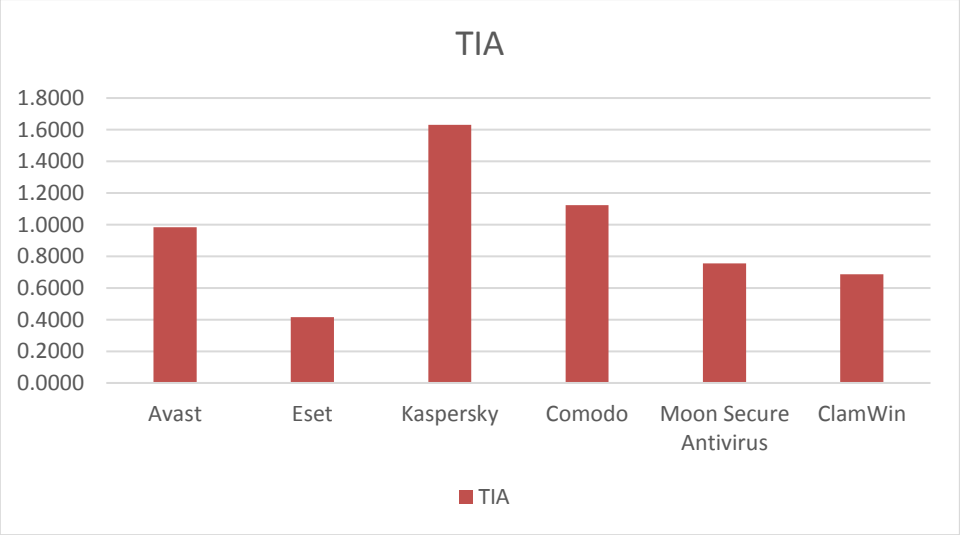


Figura 19: Tiempo de inicio de aplicaciones

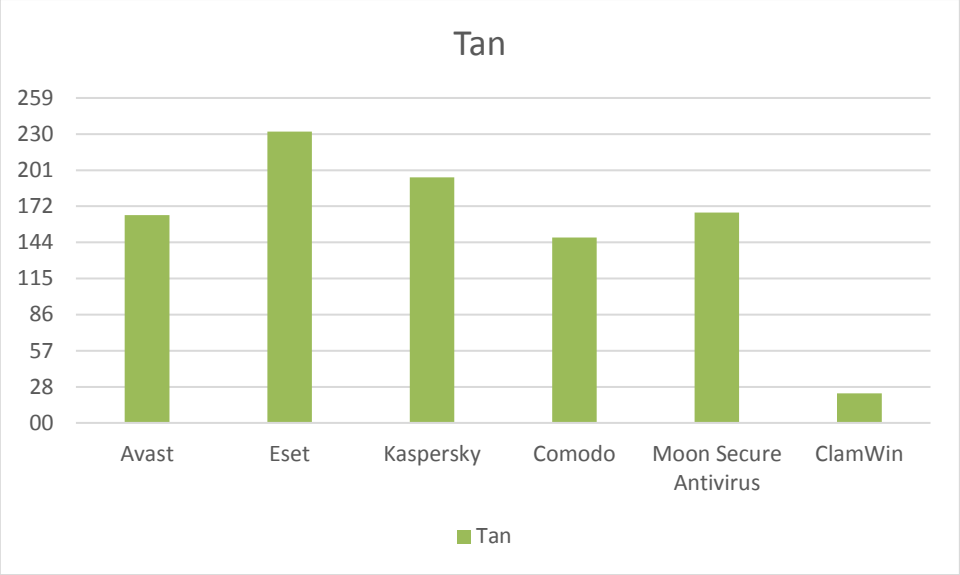


Figura 20: Tiempo de análisis

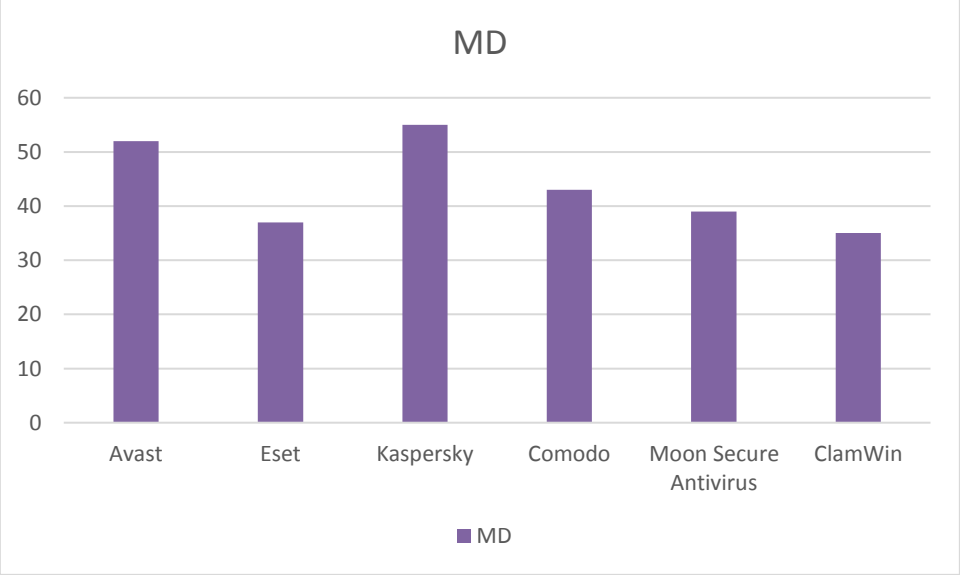


Figura 21: Malware detectado

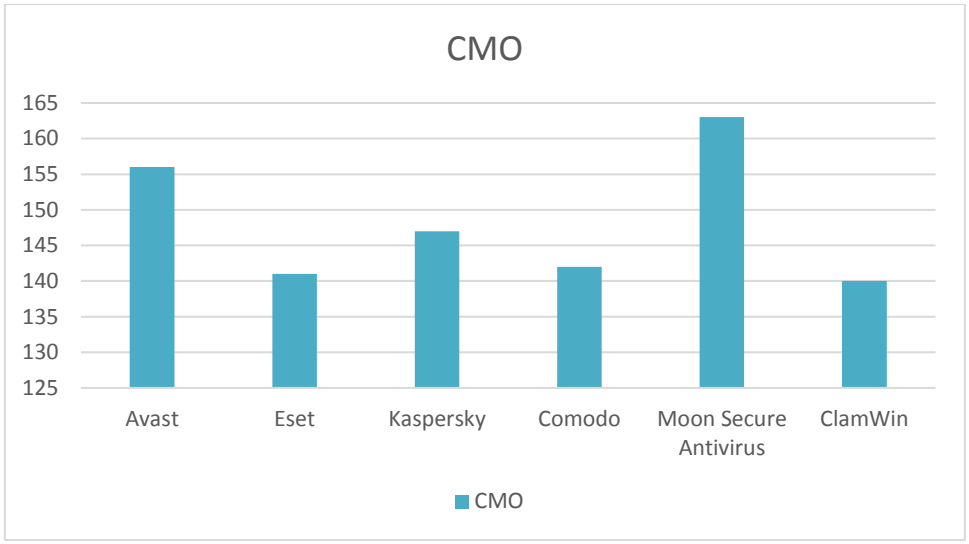


Figura 22: Cantidad de memoria ocupada

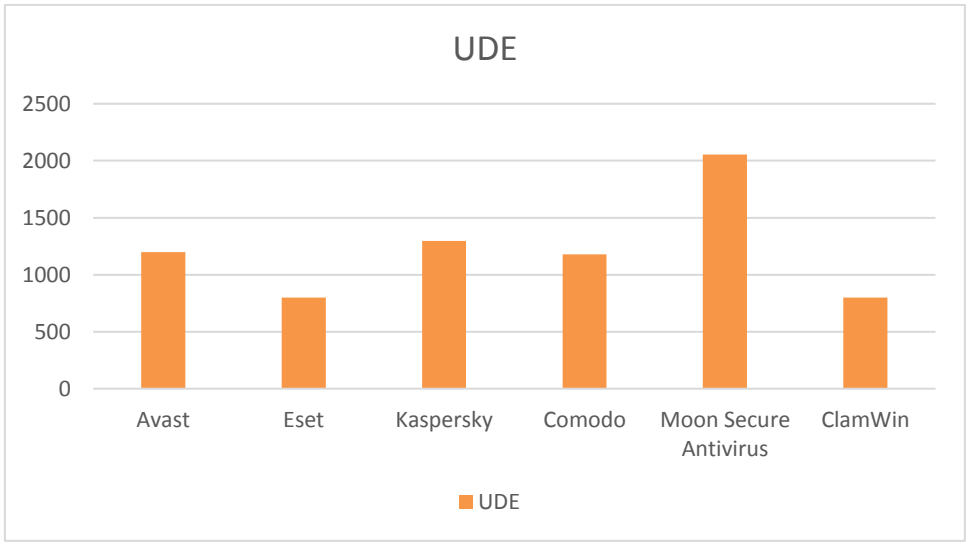


Figura 23: Uso del CPU durante escaneo

ANEXO 13: FICHA DE OBSERVACIÓN

Objetivo: Recolectar información en base a los indicadores para determinar las condiciones de seguridad de los equipos.

Confidencialidad	
1.- ¿Cualquier persona accede a los archivo?	SI NO
2.- ¿Las modificaciones de archivos son autorizadas?	SI NO
3.- Si se modifica un archivo ¿Afectaría notablemente?	SI NO
4.- ¿Existe un medio en el cual guardar archivos confidenciales?	SI NO
5.- ¿El equipo cuenta con contraseña de ingreso?	SI NO
6.- ¿Más de una persona tiene la clave del equipo?	SI NO
Integridad	
1.- ¿Encuentra datos modificados sin autorización?	SI NO
2.- ¿Son revisadas las modificaciones?	SI NO
3.-¿las modificaciones afectan notoriamente?	SI NO
4.- ¿Se modifican datos sin autenticación?	SI NO
Disponibilidad	
1.- ¿ha habido casos en el que no se puede acceder a un archivo?	SI NO
2.- ¿Los archivos afectados son importantes?	SI NO
3.-¿Tiene los medios para recuperar dicha información?	SI NO
4.- ¿Siempre se tiene acceso a los archivos?	SI NO

ANEXO 14: RECOLECCIÓN DE DATOS

Registro	Confidencialidad		Integridad		Disponibilidad		Nivel de Infección	
	Pre	Post	Pre	Post	Pre	Post	Pre	Post
1	0.325	0.106	0.285	0.139	0.715	0.611	0.430	0.219
2	0.311	0.126	0.318	0.119	0.682	0.631	0.391	0.199
3	0.338	0.146	0.311	0.132	0.689	0.618	0.384	0.172
4	0.377	0.159	0.338	0.159	0.662	0.591	0.457	0.225
5	0.298	0.126	0.391	0.146	0.609	0.604	0.377	0.192
6	0.325	0.106	0.397	0.172	0.603	0.578	0.384	0.172
7	0.344	0.146	0.364	0.132	0.636	0.618	0.411	0.205
8	0.384	0.139	0.391	0.146	0.609	0.604	0.457	0.219
9	0.325	0.106	0.404	0.159	0.596	0.591	0.411	0.199
10	0.371	0.172	0.397	0.146	0.603	0.604	0.424	0.192
11	0.318	0.159	0.417	0.172	0.583	0.578	0.391	0.166
12	0.384	0.179	0.377	0.132	0.623	0.618	0.444	0.219
13	0.298	0.152	0.318	0.185	0.682	0.565	0.384	0.152
14	0.391	0.166	0.298	0.119	0.702	0.631	0.457	0.192
15	0.358	0.159	0.338	0.146	0.662	0.604	0.411	0.172
16	0.391	0.192	0.325	0.159	0.675	0.591	0.437	0.212
17	0.344	0.172	0.364	0.166	0.636	0.584	0.391	0.179
18	0.397	0.212	0.384	0.146	0.616	0.604	0.450	0.219
19	0.364	0.192	0.325	0.119	0.675	0.631	0.411	0.185
20	0.318	0.159	0.404	0.179	0.596	0.571	0.384	0.146
21	0.351	0.205	0.397	0.159	0.603	0.591	0.417	0.185
22	0.338	0.152	0.338	0.146	0.662	0.604	0.430	0.205
23	0.318	0.106	0.325	0.113	0.675	0.637	0.371	0.146
24	0.325	0.139	0.404	0.172	0.596	0.578	0.411	0.179
25	0.351	0.152	0.318	0.119	0.702	0.628	0.417	0.179
26	0.358	0.172	0.338	0.139	0.662	0.611	0.404	0.172
27	0.384	0.219	0.364	0.106	0.636	0.623	0.457	0.185
28	0.391	0.199	0.391	0.126	0.609	0.624	0.437	0.179
29	0.404	0.192	0.311	0.132	0.689	0.618	0.477	0.205
30	0.364	0.185	0.338	0.159	0.662	0.591	0.444	0.192

ANEXO 15: F06-PP-PR-02.02 ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo, **Francisco Manuel Hilario Falcon**, docente de la Facultad Ingeniería y Escuela Profesional Ingeniería de Sistemas de la Universidad César Vallejo Sede Lima Este, revisor (a) de la tesis titulada

"Metodología para la elección de software de seguridad informática", del estudiante **SOSA FERNÁNDEZ JULISSA TATIANA,** constató que la investigación tiene un índice de similitud de 20% verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito (a) analizó dicho reporte y concluyó 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.

Lima, San Juan de Lurigancho 15 de noviembre del 2018

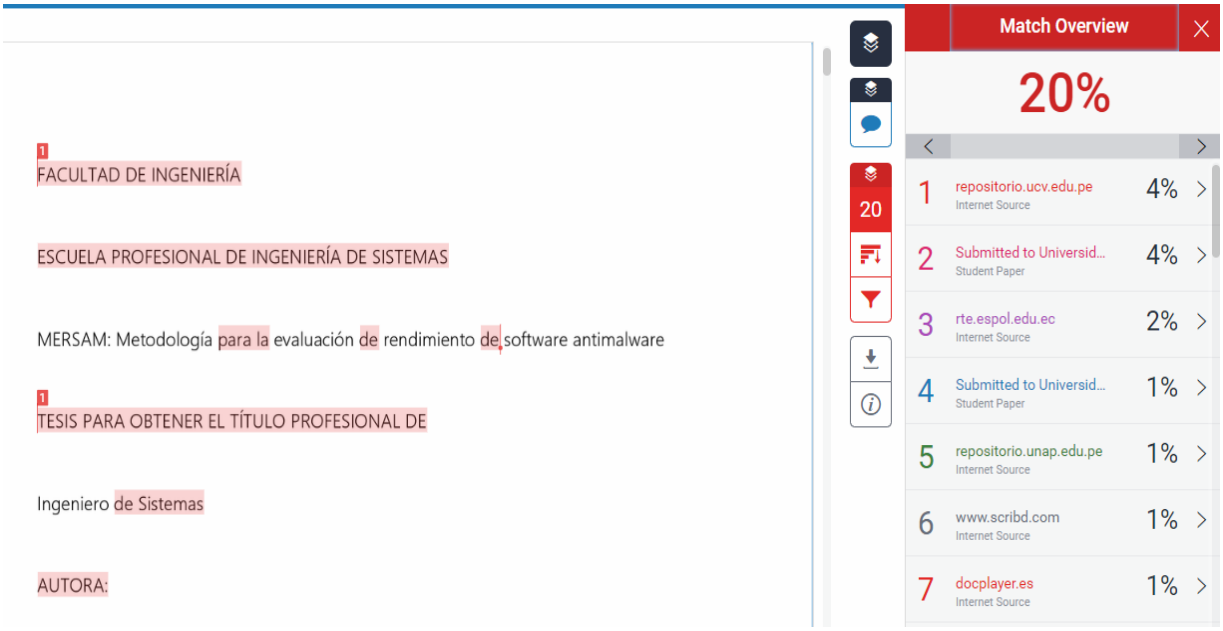
.....

Francisco Manuel Hilario Falcon

DNI: 10132025

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado

ANEXO 16: CONSTANCIA TURNITIN



ANEXO 17: F08-PP-PR-02.02 AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

UCV UNIVERSIDAD CÉSAR VALLEJO	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo **SOSA FERNÁNDEZ JULISSA TATIANA**, identificado con DNI N° **48167847**, egresado(a) de la Carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo, autorizo (**X**), no autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado **"METODOLOGÍA PARA LA ELECCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA".** en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33

Fundamentación en caso de no autorización:

.....
.....
.....
.....
.....
.....
.....
.....

.....
SOSA FERNÁNDEZ JULISSA TATIANA

DNI: **48167847**

Fecha: 19 de marzo del 2019

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Vicerrectorado de Investigación

ANEXO 18: AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

Mg. María Acuña Meléndez

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

Sosa Fernández Julissa Tatiana

INFORME TÍTULADO:

Metodología para la elección de software de seguridad informática

PARA OBTENER EL TÍTULO O GRADO DE:

Ingeniera de Sistemas

SUSTENTADO EN FECHA: 07 DE DICIEMBRE DE 2018

NOTA O MENCIÓN: 14 (CATORCE)

UNIVERSIDAD CÉSAR VALLEJO UCV COORDINACIÓN ACADÉMICA DE LA ESCUELA DE INGENIERÍA DE SISTEMAS LIMA - ESTE

Mg. María Acuña Meléndez
de Ingeniería de Sistemas campus Lima Este