UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

MAYO - SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS COMPARATIVO ENTRE SOFTWARE LIBRE Y SOFTWARE LICENCIADO ENFOCADO EN LA SEGURIDAD INFORMÁTICA

ESTUDIANTE:

MANUEL VENTURA BAYAS MOREJÓN

TUTOR:

ING. FABIÁN ALCOSER CANTUÑA

AÑO 2023

INDICE

INDICE DE TABLA

INDICE DE GRAFICO

RESUMEN

El presente caso de estudio se orienta en el análisis comparativo entre software libre y software licenciado enfocado en la seguridad informática. El propósito de este estudio es comparar y analizar los software libre y licenciado, identificando las ventajas, desventajas y características de cada programa logrando así brindar una guía para la toma de decisiones en la elección del software apropiado para cada empresa u organización. La elección entre software libre y licenciado enfocado en la seguridad informática es fundamental, debe basarse en el contexto y las necesidades individuales de cada empresa u organización. El software libre ofrece flexibilidad y economía, pero requiere de recursos técnicos y puede tener falta de soporte formal mientras que el software licenciado ofrece soporte y cumplimiento normativo, pero implica costos por su licencia. Es importante conocer sobre la seguridad informática y los riesgos que conlleva no tener un software seguro que proteja los datos de una organización. Caso contrario, si no se dispone de un programa seguro, todos estos datos pueden ser robados por usuarios maliciosos que quieran afectar y robarse la información.

Palabras clave: Seguridad, estabilidad, capacidad, software libre y software licenciado.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad el desarrollo tecnológico y el auge del internet logran hacer que se ofrezcan una gama de servicios por parte de instituciones, tales como: transacciones financieras, inventarios, consultas médicas, sistemas de ventas, servicios de correo electrónico, repositorios, portales bancarios y académicos, entre otros. Lo que permite tener acceso completo a datos que a su vez viajan por diferentes redes públicas que se pueden acceder desde cualquier lugar o dispositivo.

No obstante, la seguridad es un pilar fundamental al momento de afrontar tareas que se realizan en sistemas informáticos debido a que son las únicas medidas que pueden garantizar que estas se realicen con una serie de garantías que se dan por sentado en el mundo físico, el problema al usar los servicios tecnológicos e informáticos, es que no se tienen los cuidados necesarios por parte del cliente, los usuarios confían en las empresas y esperan que no exista ningún problema, para ingresar a los sistemas debe existir un control de acceso, por ello hoy en día los usuarios están protegidos y pueden denunciar las situaciones de abusos con sus datos, en cada país existen leyes sobre la privacidad de la información.

La seguridad informática ha surgido como una necesidad, debido a los intensos cambios en el sector productivo, a la manera en cómo vive la sociedad mundial gracias a la transformación digital, por este motivo, la información se ha convertido en uno de los activos principales de las empresas e individuos, para mantener sus datos resguardados, deben invertir en este tipo de seguridad para salvaguardar los sistemas frente a los ataques malintencionados de hackers y otros riesgos relacionados con las vulnerabilidades que pueden presentar los software. A través de estos defectos los intrusos pueden entrar en los sistemas, por lo que se requiere de soluciones que aporten, entre otros, modelos de autenticación.

Es por ello que en este ámbito es esencial contar con un software confiable que permita proteger tanto la información como los sistemas de posibles amenazas o ataques cibernéticos, en este aspecto, existen dos opciones tipos de software que pueden prevenirlo: el software libre y el software licenciado, ambos tienen sus propias ventajas como sus características, pero también plantean desafíos y consideraciones relevantes en términos de seguridad, por ello en el presente caso de estudio, se realizará un análisis comparativo exhaustivo enfocado a la seguridad que permita evaluar y contrastar tanto las ventajas como las desventajas de cada software**.**

A partir de todo lo antes mencionado nos lleva a plantearnos la siguiente interrogante, ¿Cómo un análisis comparativo entre software libre y software licenciado enfocado en la seguridad informática, nos permitirá identificar el tipo de programa correcto que una organización necesita?

JUSTIFICACIÓN

En la actualidad la seguridad informática es una preocupación constante en nuestro entorno tecnológico. Con el aumento de amenazas cibernéticas sofisticadas, es necesario contar con soluciones de software confiables que protejan la información de los sistemas de posibles ataques o vulnerabilidades. En este contexto, existen dos enfoques principales para adquirir software: el software libre y el software licenciado.

Al realizar un análisis comparativo entre el software libre y el software licenciado en el ámbito de la seguridad informática radica en la necesidad de facilitar a los usuarios y organizaciones una evaluación integral y objetiva de estas opciones para tomar decisiones informadas en la selección de software.

El software libre es conocido por su naturaleza de código abierto, lo que significa que el código fuente está disponible para su examen y modificación. Esto brinda una mayor transparencia y permite a los usuarios verificar la implementación de las medidas de seguridad, identificar posibles vulnerabilidades y corregirlas de forma personalizada.

En cuanto al software licenciado se basa en acuerdos legales y ofrece una serie de beneficios en términos de seguridad informática, los proveedores de software licenciado suelen ofrecer un nivel más alto de soporte y mantenimiento, lo cual incluye actualizaciones de seguridad regulares y asistencia técnica especializada.

Esta investigación brindará información relevante sobre la seguridad informática a través del software libre y licenciado, detallando sus características, ventajas y desventajas. Esto permitirá a los usuarios y organizaciones comprender mejor las implicaciones de seguridad para poder tomar decisiones informadas al momento de seleccionar el software más adecuado para proteger sus sistemas y datos.

Entre los principales beneficiarios están: la comunidad de desarrolladores, las empresas y entidades gubernamentales, los investigadores junto con universidades públicas o privadas que requieran de los servicios de estas herramientas tecnológicas.

En el presente caso de estudio se tomará en cuenta los siguientes softwares:

Software Libres:

Kali Linux, Nmap, Metasploit Framework, Wireshark y OpenVAS.

Software Licenciados:

Nessus, Cisco ASA, McAfee, BitLocker y Core Impact.

OBJETIVOS

OBJETIVO GENERAL

- Realizar un análisis comparativo entre software libre y software licenciado enfocado en la seguridad informática.

OBJETIVOS ESPECÍFICOS:

- Investigar de manera teórica y fundamentada los conceptos de software libre y licenciado, orientado a la seguridad informática.
- Identificar los diferentes softwares utilizados para la seguridad informática, evaluando sus características, eficacia y eficiencia.
- Detallar de manera precisa las principales características, ventajas y desventajas para determinar que software se adapta mejor a los diferentes tipos de empresas.

LÍNEA DE INVESTIGACIÓN

El presente caso de estudio se enfoca en la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, sostenida por la sublínea de investigación de redes y tecnologías inteligentes de software y hardware.

Se determinó realizar una comparación de la eficacia y eficiencia de los tipos de software libres y licenciados enfocados en la seguridad informática, con la finalidad de determinar cuál de ellos es el más seguro y confiable.

ARTICULACIÓN DEL TEMA

Aplicación de tecnologías de información y comunicación en el sector público y privado con supervisión docente.

El presente caso de estudio tiene relación con las prácticas preprofesionales, en este proceso se puede conocer profundamente los conceptos, ventajas, desventajas, tanto de los softwares libres como licenciados, ya que en el lugar donde se realizaron las prácticas se manejaban diferentes tipos de estas herramientas tecnológicas. Gracias a esto surgió la inquietud de conocer qué tipo de software es mejor para las empresas, si el libre o el licenciado.

MARCO CONCEPTUAL

Seguridad Informática

Sisti (2020), detalla que, "la seguridad informática es el proceso de prevención, y detección de acceso y eventual uso malicioso a sistemas informáticos por parte de terceros, anónimos e incluso a veces personas pertenecientes a la misma organización", la protección de los sistemas informáticos no debe ser subestimada porque es imprescindible para el desarrollo de las operaciones de toda empresa, porque la utilización maliciosa de estos sistemas privados y de los recursos internos puede acarrear desastrosas consecuencias en todas las áreas de una organización.

Por ello se debe evitar todo tipo de fuga y pérdida de información confidencial o la corrupción de los datos por terceros adoptando mecanismos de seguridad correspondientes mediante herramientas o softwares que esten dirigidos al análisis constante y a la ejecución proactiva para detectar vulnerabilidades de todo tipo, ya que es fundamental mantener siempre segura e intacta la información privada de una organización.

Software

Cevallos (2019), en su portafolio virtual detalla que, "un software como tal es un conjunto de instrucciones lógicas que permiten al usuario interactuar con el computador a través de una interfaz, conocida comúnmente como programas de computador y van desde un editor de texto hasta aplicaciones de gestión".

En aspectos de seguridad informática el software es una herramienta que está diseñada para proteger los ordenadores ante cualquier riesgo o peligro informático que abarcan una gran variedad de ataques, desde virus o malware, hasta pérdida de datos o accesos ilegítimos.

Ramirez (2022), explica que, "un software de seguridad informática es un programa que

tiene la función de proteger la privacidad de los datos que se encuentran dentro de un sistema informático". Así pues, esta solución de seguridad informática garantiza la protección de datos y ayuda a las empresas a protegerse ante posibles ataques informáticos.

Existen diferentes tipos de software, que varían en función de sus especificaciones técnicas y funciones, en el presente caso de estudio se abarcará sobre software por su tipo de licencia, las licencias de software son un elemento clave, puesto que establecen los términos que permiten el uso correcto del mismo, de este tipo de software existen 2 tipos que son: software libre y software licenciado o propietario.

Software Libre

El software libre es normalmente identificado como un software gratuito que tiene como característica, no contar con derechos de autor, permitiendo que se pueda copiar o editar su código fuente y distribuirlo poniéndolo a disposición del resto de usuarios de internet sin ninguna limitación.

Según Stallman (2020) "el software libre hace referencia a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software, especialmente a cuatro clases de libertad para los usuarios de software" (p.152).

Estas libertades son:

Libertad 0: Es la libertad para ejecutar un programa con cualquier propósito.

Libertad 1: Es la libertad para analizar el funcionamiento del programa y adaptarlo a necesidades propias, tener acceso al código fuente es la condición indispensable para hacerlo.

Libertad 2: Esta libertad es la que permite redistribuir copias del programa a cualquier persona u organización.

Libertad 3: Se refiere a la libertad para mejorar el programa y luego publicarlo para el

bien de toda la comunidad.

Un programa es un software libre solamente si otorga a los usuarios todas estas libertades de manera adecuada, de lo contrario no puede considerarse libre (Stallman, 2020). En el ámbito de la seguridad informática por lo general se piensa que el software libre al ser de código abierto es menos seguro que un programa cuyo código fuente sólo conocen sus creadores y desarrolladores, pero es una percepción errónea.

Torres (2018) explica que, "tener el código accesible para todo el mundo, no significa necesariamente que el vecino de enfrente pueda explotarlo para instalar una puerta trasera, ya que para explotar cualquier vulnerabilidad o agregar algún código malicioso es necesario tener habilidades necesarias".

A pesar de que no existen programas invulnerables, el software libre es más seguro que el privativo en términos generales, porque al tener el código público permite a la comunidad de desarrolladores encuentre y repare cualquier tipo de vulnerabilidad que se presente, el apoyo de las comunidades de desarrollo de software en la seguridad informática es bastante conocido en sectores que dependen especialmente de ella, como el bancario, en una entrevista Eneko Astigarraga, presidente de ESLE (Asociación de Empresas de Software Libre de Euskadi), dijo que, "los grandes bancos también utilizan el software libre precisamente por seguridad, porque hay miles de desarrolladores mirando la plataforma y es más fácil detectar los problemas".

Ventajas del Software Libre

De acuerdo a lo establecido en Structuralia (2023), las ventajas del software libre son:

- **Accesibilidad**: Este software es accesible para todo tipo de personas o empresas.
- **Personalización**: Al tener el código abierto, puede ser adaptado y personalizado a las necesidades de cada proyecto.

- **Colaboración**: Fomenta la colaboración y el trabajo en equipo, lo que puede resultar en una mejora de la calidad del software y en su evolución continua.
- **Reducción de costes**: al ser un software gratuito permite reducir los costes de licencias.
- **Seguridad:** El software libre permite controles de seguridad independientes que ayudan a cerrar los agujeros de seguridad más rápido.
- **Permite la independencia tecnológica:** Al no depender de los fabricantes de software, los mismos usuarios pueden decidir si es necesario realizar migraciones o actualizaciones del sistema, sin tener que esperar decisiones del fabricante.

Desventajas del software libre

El software libre no está exento de desventajas, entre ellas están las siguientes:

- **Falta de garantías:** Dado que no hay pago de derechos de autor, este software suele usarse bajo completa responsabilidad del usuario, por lo que a menudo es preferido por quienes poseen un conocimiento técnico en sistemas informáticos.
- **El usuario debe tener nociones de programación.** La administración del sistema recae mucho en la automatización de tareas y esto se logra utilizando, en muchas ocasiones, lenguajes de programación (perl, python, shell, etc).
- **Problemas de seguridad y estabilidad:** Al no contar con una empresa que garantice la calidad del software, genera problemas de seguridad y estabilidad en algunos casos.

Febrero (2021), explica que, “el software libre tiene otro tipo de riesgos, lo cual no significa que sea inseguro, existen posibilidades que tenga funcionalidades no deseadas en el software, por lo que es imprescindible configurarlo con los requerimientos y permisos específicos que se necesitan”.

Softwares Libres enfocados en seguridad informática

Kali Linux

Keepcoding (2023), detalla que este software está basado en Debian GNU/Linux y fue desarrollado por la compañía de ciberseguridad Offensive Security. Kali es un sistema operativo de código abierto y se diferencia de otras distribuciones de sistemas operativos en cuanto a que reúne más de 600 programas para hacking ético, que se encuentran preinstalados en el sistema.

Este software se utiliza principalmente en la seguridad informática y en pruebas de penetración para evaluar la seguridad de los sistemas informáticos.

Altube (2021), explica que, "este software es bastante potente y con multitud de usos avanzados para que un administrador pueda aprovecharla en totalidad", se caracteriza por:

- Ser gratuito, no tiene coste y puede usarse tanto personal como profesionalmente.
- Cuenta con un soporte eficiente, en varios lenguajes y muy bien atendido.
- No hace falta instalarlo para ser usado, ya que tiene un modo live que permite utilizarlo desde dispositivos portátiles en casi cualquier sistema.
- Está desarrollado en un entorno seguro, dando garantías sobre de datos y fallos.

Entre los usos que se le puede dar a este software destacan los siguientes:

- Recopilación de información
- Análisis de vulnerabilidades y aplicaciones web
- Evaluación de bases de datos
- Ataques de contraseñas y wireless
- Ingeniería inversa
- Herramientas de explotación, reporte, ingeniería social y análisis forense
- Sniffing and Spoofing

Nmap (Network Mapper - Mapeador de Redes)

Shivanandhan (2023) lo define como “un software de código abierto que se utiliza para escanear una red y sus puertos con el objetivo de obtener información importante sobre la misma para controlar y gestionar su seguridad”, este software sirve normalmente para realizar auditorías de seguridad y monitoreo de redes, ya que, permite a los administradores de red encontrar dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.

Entre los usos que se le dan a este software están:

- Mapear una red.
- Identificar servicios en ejecución
- Realizar una auditoría de seguridad
- Detectar sistemas operativos

Abrie (2022), explica que, las principales características de este software son:

- Reconocimiento rápido y oportuno de todos los dispositivos, incluidos servidores, enrutadores, DNS, entre otros en redes únicas o múltiples.
- Encontrar información sobre el sistema operativo que se ejecuta en dispositivos, proporcionando información detallada de las versiones del sistema operativo, lo que facilita la planificación de enfoques adicionales durante las pruebas de penetración.
- Durante una auditoría de seguridad y el escaneo de vulnerabilidades, sirve para atacar sistemas usando scripts existentes del motor de scripting de Nmap.
- Tiene una interfaz gráfica de usuario llamada Zenmap, la cual ayuda a desarrollar mapeos visuales de una red para una mejor usabilidad y generación de informes.

Metasploit Framework

Frias (2021), define este software como, “una herramienta de código abierto que permite a profesionales de la ciberseguridad desarrollar y ejecutar módulos (usualmente exploits) para aprovechar una vulnerabilidad y hacer de esta explotación algo completamente sencillo en la mayoría de los casos”.

Metasploit permite a los probadores de penetración (Pentesters) implementar escenarios de piratería en el mundo real para mantenerse al día con las técnicas avanzadas de los piratas informáticos y evitar posibles violaciones de datos, también ayuda a la automatización de tareas involucradas en el proceso de prueba de penetración, debido a que gran parte del código básico de estos comandos se almacena en sus bibliotecas.

Este software cuenta con herramientas que pueden utilizarse para realizar todas las etapas de las pruebas de penetración, que incluyen:

- Recopilación de información
- Enumeración
- Obtener acceso
- Escalada de privilegios
- Mantener el acceso
- Cubrimiento de pistas

Wireshark

Argüello (2023), detalla que, “Wireshark es un analizador de protocolos utilizado para realizar el análisis, captura de paquetes de datos a un nivel microscópico y solucionar problemas en redes de comunicaciones cuenta con todas las características estándares de un analizador de protocolos”.

Este software para un ingeniero de redes, es similar a un microscopio para un biólogo, debido a que permite ‘escuchar’ una red en vivo (después de establecer una conexión a ella) y capturar e inspeccionar paquetes sobre la marcha, también es utilizado para:

- Identificar amenazas de seguridad y actividad maliciosa en una red
- Observar el tráfico de la red para depurar redes complejas
- Filtrar el tráfico según protocolos, puertos y otros parámetros
- Aplicar reglas de coloración a la lista de paquetes para un mejor análisis
- Exportar los datos capturados a XML, CSV o archivo de texto sin formato.

OpenVAS (Open Vulnerability Assessment System – Sistema Abierto de Evaluación de Vulnerabilidades)

Barquero (2022), explica que, “es una herramienta gratuita de evaluación de vulnerabilidades completo, que sus características incluyen, verificación de autenticación, autenticación cero, ajuste de rendimiento para escaneo a gran escala, un poderoso lenguaje de programación interno que le permite verificar cualquier tipo de agujeros de seguridad y una amplia variedad de protocolos industriales y de internet de alto y bajo nivel, las características clave con las que cuenta OpenVAS son:

- Compatibilidad con el protocolo SSL, con HTTP y HTTPS
- Permite hacer escaneos programados y proporciona informes claros y completos
- Ayuda a reiniciar o detener los escaneos en cualquier momento
- Multiplataforma
- Permite escanear varias computadoras simultáneamente
- Ayuda a gestionar usuarios desde el panel de control

Software Licenciado

Fernandez (2019), explica que, se entiende como "software licenciado aquél que se distribuye en forma de binarios, sin código fuente, por parte de una compañía que licencia dicho software para un uso concreto, con un coste determinado".

Este software normalmente llamado software propietario o privativo se caracteriza por tener su código fuente no disponible o el acceso a éste se encuentre restringido ya que tiene acceso solamente fabricante, sus usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo (con o sin modificaciones), puesto que requieren autorización.

Ventajas del software Licenciado

Martinez (2023), en su sitio web detalla que, el software licenciado presenta una serie de ventajas que lo hacen atractivo para empresas y usuarios que buscan un alto nivel de calidad, soporte técnico y seguridad, entre las principales ventajas están:

- **Soporte técnico y actualizaciones:** Este software cuenta con un soporte técnico que ofrece ayuda y solución a problemas que puedan surgir en el uso del software.
- **Seguridad y garantía:** Es testados por miles de usuarios, por lo que su margen de error es casi inexistente, lo que se conoce como garantía de calidad.
- **Innovación:** Las empresas que desarrollan software licenciado suelen invertir en investigación y desarrollo, para ofrecer programas más avanzados y sofisticados.
- **Facilidad de uso:** Cuenta con una interfaz de usuario más intuitiva y fácil de usar, lo que lo hace más accesible para los usuarios sin experiencia técnica.
- **Personalización:** Ofrece herramientas de personalización que permite a los usuarios adaptar el software a necesidades específicas.

Desventajas del software licenciado

Este software también tiene algunas desventajas entre las que se destacan las siguientes:

- **Soporte técnico ineficiente.** A pesar de que el soporte técnico es señalado como una ventaja, la eficiencia que presenta muchas veces deja mucho que desear, debido a que tarda demasiado tiempo en ofrecer una respuesta satisfactoria.
- **Cursos de aprendizaje costosos**. Es difícil aprender a utilizar eficientemente el software sin haber asistido a costosos cursos de capacitación.
- **Secreto del código fuente.** El funcionamiento de este software es un secreto que guarda celosamente la compañía que lo produce.
- **Ilegalidad de copias sin licencia:** Es ilegal realizar copias de este software sin antes haber contratado las licencias necesarias.
- **Necesidad de confiar totalmente en el fabricante:** Los usuarios que adquieren este software dependen 100% de la empresa creadora.

Softwares Licenciados enfocados en seguridad informática

Nessus

Sepulveda (2023), explica que, "es un software que permite escanear de vulnerabilidades de red, es decir, una herramienta de seguridad que busca debilidades en los sistemas informáticos y redes", es fundamental para cualquier organización que busque mejorar la seguridad y proteger su información de posibles amenazas, ya que tiene la capacidad de escanear redes y sistemas informáticos en busca de vulnerabilidades, permitiendo identificar los riesgos y tomar medidas para corregirlos.

Este software se caracteriza por:

- Brindar la capacidad de identificar amenazas y responder eficazmente.

- Presentar los paneles de mando de manera más detallada con el fin de ayudar a los clientes a fortalecer las redes contra las amenazas cibernéticas.
- Ayuda a reducir el tiempo y costo de seguridad en la exploración y asegurar a los clientes con el cumplimiento de seguridad.
- Escalabilidad a ciertos de miles de sistemas
- La interfaz gráfica de usuario (GUI) muestra resultados en tiempo real
- Brinda una interfaz unificada para el analizador
- Los análisis se ejecutan en el servidor, sin importar que se lo desconecte

Las organizaciones normalmente lo emplean para los siguientes usos:

- Escaneo de red y aplicaciones web.
- Auditoría de cumplimiento.
- Penetration testing.
- Evaluación de proveedores.

Cisco Adaptive Security Appliance (ASA)

El software Cisco ASA es el núcleo del sistema operativo en el que se basa la familia Cisco ASA. Proporciona funciones de firewall de clase empresarial para los dispositivos ASA en una variedad de formatos: dispositivos autónomos, módulos blade y virtuales.

Padilla (2023) detalla que, el software ASA se integra además con otras tecnologías esenciales de seguridad a fin de ofrecer soluciones completas que satisfacen en todo momento las necesidades de seguridad en constante evolución, se caracteriza por:

- Ofrecer funciones integradas de IPS, VPN, y Comunicaciones Unificadas
- Ayudar a las organizaciones a aumentar su capacidad y mejorar su rendimiento a través de formación de clústeres.

- Ofrecer aplicaciones de alta disponibilidad y gran capacidad de recuperación
- Facilitar el routing dinámico y VPN entre sitios en función del contexto

McAfee

De la Mora (2023), explica en su estudio sobre herramientas de ciberseguridad que este software ofrece soluciones, servicios proactivos y comprobados que ayudan a asegurar sistemas y redes en todo el mundo, protege a consumidores y empresas de todos los tamaños frente a todo tipo de amenazas, también cuenta con soluciones que están diseñadas para trabajar juntas e integrar las funciones de antimalware, antispyware y antivirus con las de una administración de la seguridad que ofrece visibilidad y análisis en tiempo real, las características que destacan de este software son:

- Protección identidad, antivirus y navegación web
- Firewall personal
- Protección contra ransomware
- Filtros de correo no deseado
- Seguridad en la red doméstica y seguridad móvil
- Análisis de vulnerabilidades
- Actualizaciones automáticas e informes de seguridad

BitLocker

Vega, (2021), detalla que, “Bitlocker es un software de cifrado que introdujo Microsoft para proteger los datos de sus usuarios, se integra a la perfección con el sistema operativo y evita que los piratas informáticos y los ciberdelincuentes roben o vean los datos almacenados en el disco”.

Este software permite almacenar la clave que actúa como llave para acceder a los datos

de cinco maneras posibles: En una cuenta Microsoft, en una copia impresa, en una unidad de memoria USB, en una cuenta de Azure Active Directory y en posesión del administrador del sistema.

Entre las principales características de BitLocker se destacan las siguientes:

- **Facilidad de uso:** presenta una protección transparente para el usuario y en caso de que ocurra algún error o bloqueo del sistema se pueden recuperar los archivos.
- **Eliminación y reciclaje de equipos:** Hace que el contenido de los datos sea inaccesible eliminando las claves necesarias para obtener acceso al disco/s.
- **Independencia de cifrado entre las cuentas de usuarios:** el cifrado que se realiza con BitLocker no va a depender de las cuentas de usuario, ya que cuando el administrador lo habilita, cada cuenta de usuario en el equipo tiene sus propios archivos de cifrado.
- **Implantación empresarial:** Este software ofrece una solución para proteger los datos de forma fácil y eficaz pudiéndose implantar de forma centralizada a través del Directory Active o de forma local en cada uno de los equipos.

Core Impact.

Alvarado (2018), explica que este software es una solución de pruebas de penetración muy completa que permite replicar ataques de múltiples etapas que apuntan a sistemas, dispositivos y aplicaciones. Mediante una biblioteca estable y actualizada de exploits de grado comercial, Core Impact revela cómo las cadenas de vulnerabilidades abren rutas a los sistemas y activos críticos para la misión de la organización.

Está diseñado para equipos de seguridad en diversos sectores, como: atención médica, servicios financieros, comercio minorista, educación, sector gubernamental, entre otros.

Permite testear los distintos vectores tal como lo haría un hacker, los principales vectores

de ataque que esta herramienta puede testear son:

Redes:

- Identifica las vulnerabilidades reales y los prioriza de acuerdo a su riesgo real.
- Identifica y explota sistemas operativos, vulnerabilidades de servicio de aplicación / test IPS, IDS y otras defensas. Respecto a wifi, permite descubrir, crackear y unir redes encriptadas por WEP, WPA-PSK and WPA2-PSK

Estaciones de trabajo de empleados

- Provee un mecanismo efectivo para las campañas internas de concientización del empleado
- Reduce los riesgos corporativos que involucran los ataques client-side (Aurora)
- Testea consumidores finales contra ataques phishing y spear phishing

Aplicaciones web/internet

- Testea todos los TOP10 OWASP 2010 (por ejemplo, ataques similares al Caso González quien fue condenado por violación a los Heartland Payment Systems, robo de más de 40 millones de números de tarjetas de crédito)
- Permite intrusiones de tipo Cross-site Scripting, Remote File Inclusion y ataques SQL Injection.

Combinación de distintos vectores de ataque

- Pivotea entre redes, estaciones de trabajo y las aplicaciones web para revelar caminos de exposición a los sistemas backend y a datos tal como si lo hiciera un atacante.

MARCO METODOLÓGICO

Para el desarrollo de este caso de estudio se utilizó el tipo de investigación descriptivo-comparativo con el objetivo de identificar las características y diferencias que posee cada software, en términos de capacidad, rendimiento y funcionalidad.

Se utilizó el método cuantitativo y cualitativo, con el fin de recolectar información, donde los datos serán tabulados y analizados estadísticamente para obtener una visión más óptima y centralizada en el uso de software libre y licenciado.

Para la recolección de opiniones y criterios, se tomó una población de 40 estudiantes pertenecientes a la carrera de sistemas de información para poder analizar las respuestas referentes al rendimiento y uso de software libre como licenciado, por otro lado, se toma una muestra de 3 personas de carácter profesional en el área de ingeniería en sistemas, en dónde se implementaron las técnicas de la entrevista y encuesta.

RESULTADOS

Luego de haber realizado las entrevistas a 3 profesionales en el área de ingeniería informática se ha logrado obtener los siguientes resultados.

1. **¿Cuál es su experiencia en el uso de software libre y licenciado en el ámbito de la seguridad informática?**

Con la información proporcionada de los 3 entrevistados se llegó a concluir que su experiencia es buena en el uso de los dos tipos de software tanto libre como licenciado y si tienen conocimientos de los mismos.

2. **¿Cuáles son las principales diferencias entre el software libre y el software licenciado en el ámbito de la seguridad informática?**

Se puede llegar a la conclusión que la principal diferencia del software libre es en la libertad que posee su código porque es abierto y permite que los usuarios desarrolladores puedan editarlo mientras que el software licenciado tiene limitaciones ya que depende del pago y uso de una licencia.

3. **En el ámbito de la seguridad informática ¿Cuáles son las ventajas al utilizar software libre en comparación con software licenciado?**

Se puede llegar a la conclusión que la ventaja de usar software libre es que permite personalizarlo logrando así que el usuario logre visualizar las ventajas y características que posee.

4. **¿Cuáles son las principales preocupaciones o desafíos que se presentan al utilizar software libre en comparación con el software licenciado?**

Se puede llegar a la conclusión que la principal preocupación es el mal uso que le pueden dar a este software libre porque por ser de código abierto puede existir un robo de datos mediante actualizaciones del software.

5. **¿Ha notado alguna tendencia reciente en el uso de software libre o licenciado en la comunidad de seguridad informática?**

Se puede llegar a la conclusión que las tendencias están enfocadas en la inteligencia artificial para simular ataques, en su comunidad de desarrolladores activos los cuales pueden corregir errores y finalmente en el interés de sus usuarios porque no tiene costo alguno.

6. **¿Qué recomendaciones daría para mejorar la seguridad informática en entornos de software libre y licenciado?**

Se puede llegar a la conclusión que recomiendan usar el software libre en caso de decidirse cuál elegir, también recomiendan mantener actualizados sus repositorios para detectar a tiempo alguna amenaza en caso de existir.

De las encuestas realizadas a los estudiantes de la carrera de sistemas de información se obtienen los siguientes resultados:

1. **¿Tiene experiencia en el uso de software de seguridad informática?**

OPCIONES	FRECUENCIA	PORCENTAJE
Si	38	95%
No	2	5%
TOTAL	40	100%

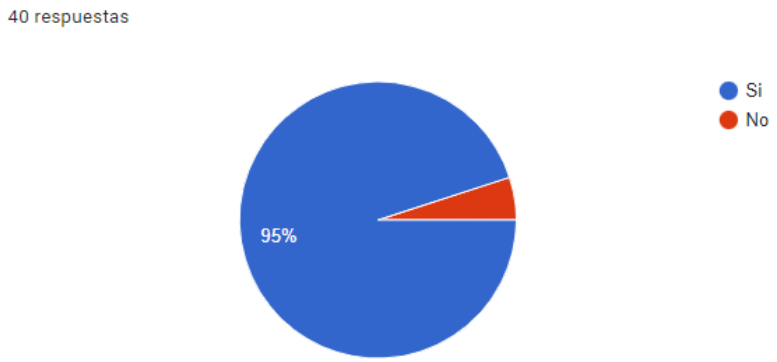

Gráfico 1 Uso de software de seguridad informática

Análisis e interpretación de resultados

Del 100% de la población encuestada se puede concluir que el 95% si tienen experiencia en el uso de software de seguridad informática mientras que solo el 5% no tiene experiencia. Por lo tanto, podemos concluir que si tienen experiencia en el manejo del software de seguridad informática.

2. **¿Qué tipo de software utiliza con mayor frecuencia en sus actividades relacionadas con la seguridad informática?**

OPCIONES	FRECUENCIA	PORCENTAJE
Software libre	19	47,5%
Software licenciado	7	17,5%
Ambos	12	30%
Ninguno	2	5%
TOTAL	40	100%

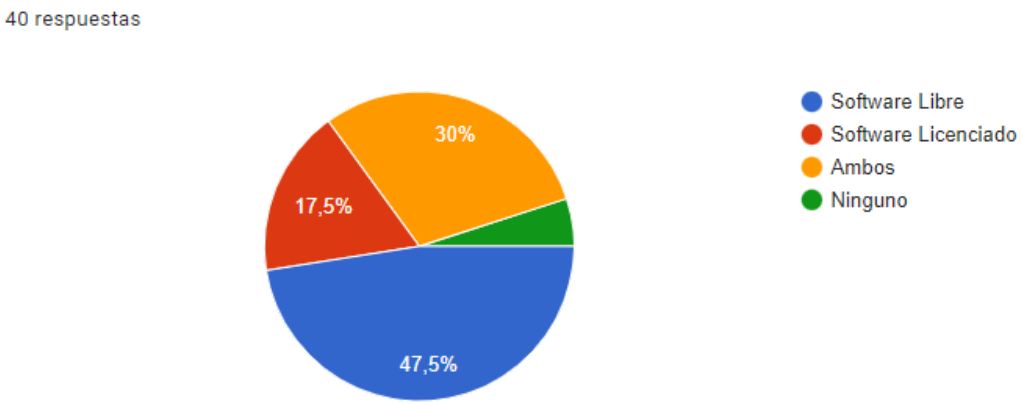

Gráfico 2 Software utilizado con mayor frecuencia

Análisis e interpretación de resultados

Del 100% de la población encuestada, el 47,5% respondió que utilizan software libre en sus actividades relacionadas con la seguridad informática, el 30% utilizan ambos software tanto libre como licenciado, el 17,5% utiliza el software licenciado y solamente el 5% no utiliza ninguno. En conclusión, los datos reflejados en la encuesta indica que los estudiantes utilizan ambos software con mayor frecuencia en sus actividades.

3. ¿Qué tipo de software considera que es más eficaz en la detección de vulnerabilidades y amenazas informáticas?

OPCIONES	FRECUENCIA	PORCENTAJE
Software libre	6	15,0%
Software licenciado	27	67,5%
Ambos	7	17,5%
Ninguno	0	0%
TOTAL	40	100%

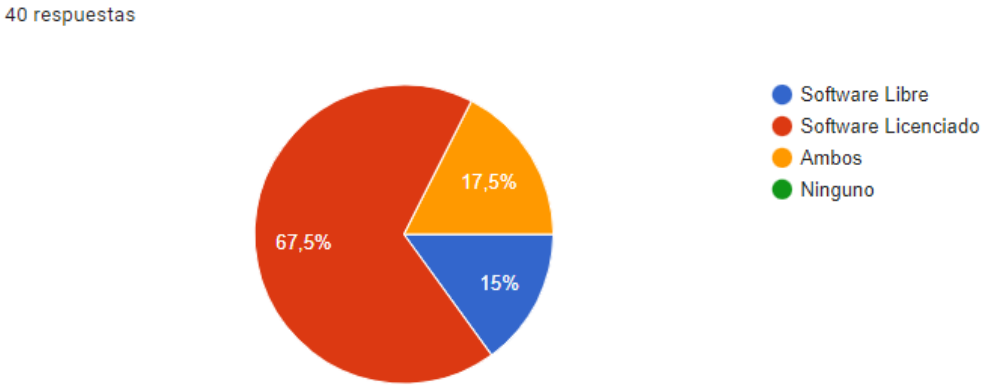

Gráfico 3 Software más eficaz en detección de vulnerabilidades

Análisis e interpretación de resultados

Del 100% de la población encuestada el 67,5% considera que el software licenciado es el más eficaz en la detección de vulnerabilidades y amenazas informáticas, el 17,5% considera que ambos software son los más eficaces y solamente el 15% considera que el software libre es el más eficaz. Por ende, se puede indicar que la mayoría de los estudiantes consideran al software licenciado como el más eficaz en detectar vulnerabilidades.

4. **¿Cuáles son las ventajas más importantes del software libre en seguridad informática?**

OPCIONES	FRECUENCIA	PORCENTAJE
Costo cero	10	25%
Comunidad de desarrollo activa	13	32,5%
Transparencia del código fuente	8	20%
Personalización	7	17,5%
Flexibilidad de licencia	2	5%
TOTAL	40	100%

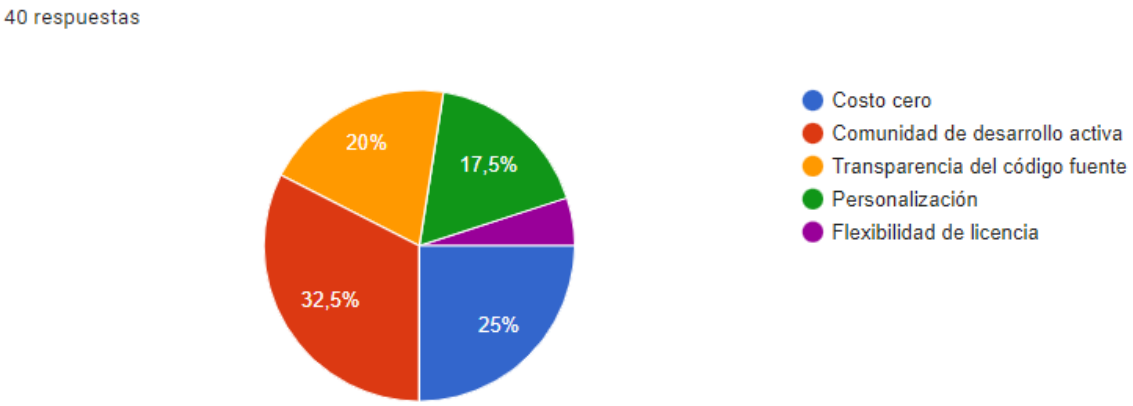

Gráfico 4 Ventajas más importantes del software libre

Análisis e interpretación de resultados

Del 100% de la población encuestada el 32,5% respondió que la comunidad de desarrollo activa es una de las ventajas más importantes del software libre, un 25% respondió el costo cero, el 20% respondió la transparencia de código fuente, el 17,5% considera que la personalización es una de las ventajas más importantes del software libre en seguridad informática y solamente un 5% optó por la flexibilidad de licencia. Por consiguiente, se concluye que, los datos reflejados indican que los estudiantes se inclinan más por la elección de 3 tipos de ventajas los cuales son costo cero, comunidad de desarrollo activa y transparencia del código fuente.

5. ¿Cuáles son las ventajas más importantes del software licenciado en seguridad informática?

OPCIONES	FRECUENCIA	PORCENTAJE
Soporte técnico garantizado	16	40%
Actualizaciones regulares y parches de seguridad	14	35,0%
Amplia variedad de características	10	25%
Cumplimiento normativo	0	0%
Integración de otros productos	0	0%
TOTAL	40	100%

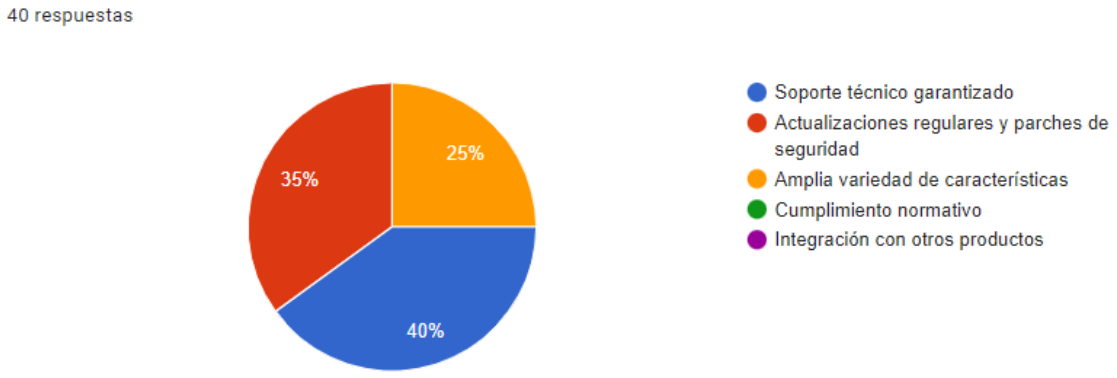

Gráfico 5 Ventajas más importante del software licenciado

Análisis e interpretación de resultados

Del 100% de la población encuestada el 40% considera que el soporte técnico garantizado es una de las ventajas más importantes del software licenciado, el 35% respondió las actualizaciones regulares y parches de seguridad y el otro 25% respondió una amplia variedad de

características como una de las ventajas más importantes. De esta manera, se determina que los estudiantes consideran más importantes al soporte técnico garantizado como ventaja del software licenciado al igual que la amplia variedad de características y actualizaciones regulares.

DISCUSIÓN DE RESULTADOS

Una vez obtenidos datos relevantes para el presente caso de estudio se proceden a realizar el análisis y síntesis de las siguientes tablas:

Software	Escalabilidad		Flexibilidad		Rendimiento		Capacidad		Estabilidad	
	Tamaño de red	Eficiencia en el uso de recursos	Tareas de seguridad de red	Variedad de herramientas	Velocidad de escaneo	Eficiencia en el uso de recursos	Funciones	Datos	Confiabilidad	Resistencia a fallos
Kali Linux	9	9	10	10	9	9	10	10	10	9
Nmap	9	9	9	9	9	9	9	8	9	9
Metasploit Framework	8	8	9	9	8	8	9	9	7	8
Wireshark	9	9	10	10	9	9	10	10	9	9
OpenVas	9	9	10	10	9	9	10	10	10	9

Tabla 1 Características de Software Libre *Autor: Manuel Bayas*

De acuerdo a esta tabla donde se menciona las características de los software libres a comparar en donde detalla su escalabilidad, flexibilidad, rendimiento, capacidad y estabilidad, cada uno de estos puntos se encuentran calificados en una escala del 1 al 10, donde todos los software descritos en la tabla comparativa cuentan con una buena calificación en cada una de sus características. Podemos concluir que estos software son eficientes en las funciones que cumplen cada uno.

Software	Escalabilidad		Flexibilidad		Rendimiento		Capacidad		Estabilidad	
	Facilidad de expansión	Soporte Multiplataforma	Personalización de políticas	Integración de terceros	Tiempo de respuesta	Impacto en recursos	Funcionalidades avanzadas	Gestión de incidentes	Disponibilidad	Actualizaciones y parches
Nessus	8	8	8	7	8	7	8	8	8	8
Cisco ASA	9	9	8	8	9	9	9	9	9	9
McAfee	8	9	9	9	8	8	8	8	9	9
Bitlocker	2	2	4	5	9	7	8	6	9	9
Core Impact	9	8	9	9	9	9	9	9	9	9

Tabla 2: Características Software Licenciado *Autor: Manuel Bayas*

De acuerdo a la tabla 2 donde se menciona las características de los software licenciados en lo que respecta a su escalabilidad, flexibilidad, rendimiento, capacidad y estabilidad, cada uno de estos puntos se encuentran calificados en una escala del 1 al 10, en donde cada programa cumple porque destacan con una alta calificación en cada una de sus características a excepción del software Bitlocker que obtiene una baja calificación en su escalabilidad y flexibilidad. Por lo tanto, se concluye que el software menos eficiente es Bitlocker debido al bajo rendimiento en sus funciones lo cual hace que su calificación sea baja.

Características	Software Libres					Software Licenciados				
	Kali Linux	Nmap	Metasploit	Wireshark	OpenVas	Nessus	Cisco ASA	McAfee	BitLocker	Core Impact
Tipo de software	Sistema operativo Linux	Herramienta de escaneo de puertos	Herramienta de explotación de vulnerabilidades	Analizador de paquetes	Sistema de gestión de vulnerabilidades	Sistema de gestión de vulnerabilidades	Firewall	Antivirus	Cifrado de disco	Herramienta de pruebas de penetración
Licencia	GNU General Public License (GPL)	GNU General Public License (GPL)	Apache License 2.0	GNU General Public License (GPL)	Apache License 2.0	Pago	Pago	Pago	Pago	Pago
Disponible en	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux
Uso principal	Seguridad informática	Seguridad informática	Seguridad informática	Seguridad informática	Seguridad informática	Evaluación de vulnerabilidades	Seguridad de redes	Protección contra malware	Protección de datos	Pruebas de penetración
Funciones principales	Amplia gama de herramientas de seguridad	Escanea puertos, descubre hosts, genera informes	Explota vulnerabilidades en sistemas informáticos	Captura y analiza el tráfico de red	Evalúa la seguridad de redes	Escanea redes y sistemas para identificar vulnerabilidades	Filtra el tráfico de red	Detecta y elimina malware	Encripta datos en un disco duro o dispositivo de almacenamiento	Simula ciberataques para evaluar la seguridad de una red
Precio	Gratuito	Gratuito	Gratuito	Gratuito	Gratuito	Desde 1.495 USD	Desde 1.995 USD	Desde 299 USD	Desde 100 USD	Desde 12.995 USD
Nivel de experiencia	Medio-alto	Medio-bajo	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

Tabla 3: Comparación de los Software Libres y Licenciados *Autor: Manuel Bayas.*

De acuerdo a la tabla 3 donde se menciona las características globales tanto de los software libre como licenciado, se puede observar que cada uno de los software mencionados en la tabla comparativa cuentan con una función en específico de los cuales los de tipo libre son gratuitos mientras que los licenciados son de paga, todos ellos tienen compatibilidad con los sistemas operativos, Windows, macOS y Linux, así como también cuentan con sus precios específicos más que todo los software licenciados porque son de paga y finalmente el nivel de experiencia para poder utilizar cada uno de estos programas es media-alta.

Finalmente podemos indicar, que todos los software comparados ofrecen una amplia gama de opciones para satisfacer las necesidades de los clientes en términos de rendimiento, flexibilidad, escalabilidad, capacidad y estabilidad lo que permite a los usuarios y empresas poder elegir la mejor opción que se adapte a sus necesidades.

CONCLUSIONES

Después de haber culminado este caso de estudio se concluye que:

El análisis comparativo entre software libre y licenciado se destaca que ambos ofrecen una gran cantidad de características y servicios, también tienen sus propias ventajas y desventajas lo cual permite que las empresas u organizaciones elijan el software que se adapte mejor a sus necesidades.

A través del análisis se concluyó que el software libre posee grandes diferencias del software licenciado, una de ellas es en la libertad que tiene su código ya que los usuarios pueden personalizarlo y editarlo a su conveniencia, cosa que el software licenciado no permite por la privacidad que tiene y por la licencia ya que es de paga y no gratuito como el software libre.

Elegir un tipo de software entre libre y licenciado depende de las necesidades que tenga una empresa u organización, considerando puntos clave como el financiamiento, migraciones de datos y tareas a cumplir para la seguridad informática. De los software libres comparados se recomienda a Kali Linux para pymes que requieran de sus servicios en seguridad informática y de los licenciados Core Impact es una buena opción por las pruebas de penetración que realiza pero tiene un alto costo.

RECOMENDACIONES

El uso de software para seguridad informática ha tomado bastante relevancia en la actualidad tanto para usuarios y organizaciones, por ello se recomienda que:

Antes de elegir un tipo de software es de vital importancia evaluar las necesidades específicas de seguridad informática de la empresa u organización ya que hay que considerar la detección de vulnerabilidades y el análisis de riesgos, antes de tomar una decisión.

Analizar aspectos clave del software como sus características, diferencias, similitudes que ofrecen para determinar que programa se adapta mejor al usuario o empresas en base a sus necesidades.

Finalmente, se recomienda considerar los costos de adquisición de un software porque es de suma importancia al momento de elegir un tipo de software para la seguridad, se debe comparar los precios de los diferentes proveedores, elegir el que sea más rentable, eficaz para su empresa u organización, se debe tomar en cuenta las habilidades y conocimientos que debe tener un usuario en caso de que adquiera un software gratuito.

REFERENCIAS

Abrie, A. (6 de mayo de 2022). *Nmap - Mapeo de redes*. Obtenido de https://www.icm.es/2022/05/06/nmap-analisis-de-puertos-y-monitorizacion-de-redes/

Altube, R. (5 de noviembre de 2021). *Caracteristicas de Kali Linux*. Obtenido de Openwebinars.net: https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Alvarado, Y. (19 de Noviembre de 2018). *Presentación de Core y sus principales productos* . Obtenido de https://docplayer.es/2801126-Presentacion-de-core-y-sus-principales-productos.html

Argüello, F. (5 de junio de 2023). *Usos de Wireshark*. Obtenido de https://www.infoteknico.com/que-es-wireshark-y-como-se-utiliza/

Barquero , A. (28 de marzo de 2022). *Estudio comparativo entre openvas y wazuh.* Obtenido de https://repositorio.upct.es/bitstream/handle/10317/11663/tfg-bar-est.pdf?sequence=1

Cevallos, K. (17 de abril de 2019). *Software y la Ingeniería del software*. Obtenido de Wordpress: https://ingsotfwarekarlacevallos.wordpress.com/category/el-software-y-la-ingenieria-de-software/

De la Mora, F. (24 de mayo de 2023). *Implementación de software McAfee.* Obtenido de http://ri.uaemex.mx/bitstream/handle/20.500.11799/138458/TRABAJO_FINAL_2023-FEBRERO_REVISORES_FINAL.pdf?sequence=1&isAllowed=y

Febrero, A. (14 de septiembre de 2021). *Software libre en ciberseguridad*. Obtenido de Segurilatam: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/software-libre-ventajas-y-vulnerabilidades_20210914.html

Fernandez, J. (3 de febrero de 2019). *Informe de seguridad de software licenciado.*

Obtenido de http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf

Frias, M. (18 de octubre de 2021). *Fundamentos de Metasploit Framework*. Obtenido de Openwebinars.net: https://openwebinars.net/blog/fundamentos-de-metasploit-framework/

Keepcoding. (6 de enero de 2023). *Que es Kali Linux*. Obtenido de https://keepcoding.io/blog/que-es-kali-linux/

Martinez, E. (3 de mayo de 2023). *software de ciberseguridad*. Obtenido de https://www.iebschool.com/blog/software-propietario-digital-business/

Padilla, L. (5 de abril de 2023). *Concepto de Cisco ASA.* Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/23851/1/CD%2013079.pdf

Ramirez, P. (5 de septiembre de 2022). *Software de seguridad, Beneficios y Funciones*. Obtenido de https://www.epitech-it.es/beneficios-funciones-software-seguridad/#:~:text=Un%20software%20de%20seguridad%20inform%C3%A1tica%20protege%20a%20los%20sistemas%20inform%C3%A1ticos,malware%20y%20ransomware%2C%20entre%20otros.

Sepulveda, M. (23 de febrero de 2023). *Utilidades de Nessus* . Obtenido de https://ciberseguridad.club/que-es-nessus-y-como-utilizarlo/

Shivanandhan, M. (23 de abril de 2023). *Guía de uso de Nmap*. Obtenido de freecodecamp.org: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Sisti , A. (1 de abril de 2020). *Seguridad Informática.* Obtenido de https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Stallman, R. (2020). La definición del software libre. *Communiars*, 153. Obtenido de https://revistascientificas.us.es/index.php/Communiars/article/view/12773/11048

Structuralia. (19 de junio de 2023). *Ventajas y Desventajas del Software Libre*. Obtenido de blog.structuralia.com: https://blog.structuralia.com/software-libre-ventajas-desventajas

Torres, G. (7 de diciembre de 2018). *Software Libre*. Obtenido de Nosturi: https://nosturi.es/2016/12/07/software-libre-seguridad/

Vega, E. (2 de marzo de 2021). *Estudio de medidas y herramientas de seguridad* . Obtenido de https://accedacris.ulpgc.es/bitstream/10553/78002/2/0771898_00000_0000.pdf

ANEXOS

Entrevista realizada a profesionales en el área de ingeniería en sistemas:

Ing. Nelly Esparza

1. **¿Cuál es su experiencia en el uso de software libre y licenciado en el ámbito de la seguridad informática?**

Cuando se utiliza software libre frecuentemente pide actualizaciones o ajustes debido a que se lanzan nuevas versiones sin mayor control al mercado, mientras que el licenciado se mantiene más estable con mayor control sobre los cambios.

2. **¿Cuáles son las principales diferencias entre el software libre y el software licenciado en el ámbito de la seguridad informática?**

Las principales diferencias entre el software libre del licenciado es que no tiene ningún costo porque es gratuito y su código está abierto al uso de todo público mientras que el otro software es privado por mantener una licencia por la cual pagar.

3. **En el ámbito de la seguridad informática ¿Cuáles son las ventajas al utilizar software libre en comparación con software licenciado?**

Las ventajas de usar software libre es que le permite al usuario poder visualizar las ventajas de utilizar programas para la seguridad y esto les puede impulsar a comprar software licenciado que se ajuste a sus necesidades.

4. **¿Cuáles son las principales preocupaciones o desafíos que se presentan al utilizar software libre en comparación con el software licenciado?**

En nuestro país por la cultura de los usuarios siempre prefieren software libre, sin embargo con el pasar del tiempo el software licenciado ha bajado los costos y eso si influye a comprar licencias por parte de los usuarios finales.

5. **¿Ha notado alguna tendencia reciente en el uso de software libre o licenciado en la comunidad de seguridad informática?**

La tendencia reciente es que el software libre cada vez tiene un mayor interés por parte de sus usuarios porque no cuenta con costos de licencia mientras que el software licenciado si posee costos por la compra de su licencia.

6. **¿Qué recomendaciones daría para mejorar la seguridad informática en entornos de software libre y licenciado?**

En el caso de ser usuario final puede probar software libre antes de decidir cuál comprar, pero en el caso de las empresas o negocios si deberían adquirir software licenciado para asegurar el soporte técnico adecuado y no dejar puertas de seguridad abiertas por usar programas gratuitos que nunca son seguros.

Ing. Omar Montecé

1. **¿Cuál es su experiencia en el uso de software libre y licenciado en el ámbito de la seguridad informática?**

Mi experiencia es positiva en ambos sistemas referentes a la seguridad informática.

2. **¿Cuáles son las principales diferencias entre el software libre y el software licenciado en el ámbito de la seguridad informática?**

Las principales diferencias que he podido encontrar sin duda alguna es la manipulación del código fuente por parte de las aplicaciones de código abierto mientras que las que son comerciales dependen mucho de el pago de las licencias para la instalación de plugins adicionales.

3. **En el ámbito de la seguridad informática ¿Cuáles son las ventajas al utilizar software libre en comparación con software licenciado?**

En el ámbito de la seguridad informática el software libre permite personalizarlo a conveniencia y además se puede establecer políticas adicionales mediante el uso de usuarios root.

4. **¿Cuáles son las principales preocupaciones o desafíos que se presentan al utilizar software libre en comparación con el software licenciado?**

Las principales preocupaciones están orientadas a las nuevas formas suplantación de datos que hacen que los software se actualicen periódicamente.

5. **¿Ha notado alguna tendencia reciente en el uso de software libre o licenciado en la comunidad de seguridad informática?**

Las nuevas tendencias están orientadas al uso de la inteligencia artificial para simular algunas situaciones referentes a los ataques.

6. **¿Qué recomendaciones daría para mejorar la seguridad informática en entornos de software libre y licenciado?**

La principal recomendación es tener actualizada su base de repositorios con lo cual podríamos estar al tanto de amenazas actuales que podrían perjudicar a los servidores de información y en lo referente a el software comercial pedir al proveedor revise constantemente los diferentes cambios existentes.

Ing. Walter Silvera

1. **¿Cuál es su experiencia en el uso de software libre y licenciado en el ámbito de la seguridad informática?**

En mi experiencia he utilizado ambos software en el campo de la seguridad que me han sido de gran ayuda siempre.

2. **¿Cuáles son las principales diferencias entre el software libre y el software licenciado en el ámbito de la seguridad informática?**

La principal diferencia entre estos software consiste en que uno brinda el acceso al código fuente para su propio uso mientras que el otro posee limitaciones ya que es un software de licencia por lo cual el usuario debe de pagar.

3. **En el ámbito de la seguridad informática ¿Cuáles son las ventajas al utilizar software libre en comparación con software licenciado?**

Una de las ventajas que posee este software es que al ser gratuito el usuario final puede personalizarlo para adaptarlo en base a sus necesidades.

4. **¿Cuáles son las principales preocupaciones o desafíos que se presentan al utilizar software libre en comparación con el software licenciado?**

Las principales preocupaciones se basan en su vulnerabilidad de seguridad porque al ser un software libre está presto a que personas externas la utilicen para alguna actividad maliciosa.

5. **¿Ha notado alguna tendencia reciente en el uso de software libre o licenciado en la comunidad de seguridad informática?**

Las nuevas tendencias que he logrado notar es que cada vez existen más comunidades de desarrollo activo los cuales pueden corregir los errores que existan en cada software.

6. **¿Qué recomendaciones daría para mejorar la seguridad informática en entornos de software libre y licenciado?**

La recomendación que daría es que deben de mantener más controles de seguridad para detectar amenazas y actualizar periódicamente cada software.