UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

LOS SISTEMAS OPERATIVO COMERCIALES Y OPENSOURCE SOBRE EVITAR LAS AMENAZAS EN LA CIBERSEGURIDAD PARA LOS USUARIOS

ESTUDIANTE:

JOSTIN OVIDIO MORALES CADENA

TUTOR:

ING. CARLOS ALFREDO CEVALLOS MONAR

AÑO 2022

RESUMEN

En el presente estudio comparativo de "LOS SISTEMAS OPERATIVOS COMERCIALES Y OPENSOURCE SOBRE EVITAR LAS AMENAZAS EN LA CIBERSEGURIDAD PARA LOS USUARIOS" se explicará a detalle los percances que se han ido dando a través de los años con la seguridad en los sistemas informáticos debido a que se registran un sin números de casos que han perpetrado la integridad, confidencialidad y la seguridad del usuario u organización. Por lo que expondré dos sistemas operativos (comercial y opensource) de los cuales se ira describiendo sus características para la ciberseguridad, ya que el usuario al no conocer hasta que limite las herramientas de seguridad informática lo mantendrán a salvo, ante las amenazas y vulnerabilidades de la World Wibe Web, por lo cual se va a determinar qué sistema operativo es el más adecuado para evitar que el usuario sea perjudicado. También se recomendará algunos TIPS en cuanto se navegue en la internet, por consecuente se informará sobre los tipos de malware que pueden ser empleados para infectar el computador y así concientizar al usuario para no cometer imprudencia en su seguridad informática. Y por último se concluirá con un análisis comparativo entre ambos sistemas para evaluar cuál de los dos sistemas operativo tiene un nivel más alto de herramientas de ciberseguridad para los malware, Spoofing, DDOS, Sniffing, entre otros tipos de ataque.

Palabras Claves: Sistemas Operativos comerciales y OpenSource, Ciberseguridad, Malware, Amenazas y Vulnerabilidades.

ABSTRACT

In this comparative study of "COMMERCIAL OPERATING SYSTEMS AND OPENSOURCE ON AVOIDING CYBERSECURITY THREATS FOR USERS" the mishaps that have occurred over the years with security in computer systems will be explained in detail because a number of cases are recorded that have perpetrated the integrity, confidentiality and security of the user or organization. Therefore, I will expose two operating systems (commercial and open source) of which I will describe their characteristics for cybersecurity, since the user, not knowing until he limits the computer security tools, will keep him safe, in the face of threats and vulnerabilities of the World Wibe Web, for which it will determine which operating system is the most appropriate to prevent the user from being harmed. Some TIPS will also be recommended as soon as you browse the Internet, therefore, you will be informed about the types of malware that can be used to infect the computer and thus make the user aware so as not to commit recklessness in their computer security. And finally, it will conclude with a comparative analysis between both systems to evaluate which of the two operating systems has a higher level of cybersecurity tools for malware, Spoofing, DDOS, Sniffing, among other types of attack.

KEY WORDS: Commercial and OpenSource Operating Systems, Cybersecurity, Malware, Threats and Vulnerabilities.

INDICE

PLANTEAMIENTO DEL PROBLEMA

Desde años atrás, los usuarios se han visto envueltos en constantes peligros en amenazas cibernéticas, las cuales pueden afectar a gran medida su bienestar personal, académico o institucional. Los llamados ataques cibernéticos son una prueba clara de lo que se habla, ya que pueden llegar a ser perjudicial para la persona porque al ser conductas maliciosas pueden provocar la perdida de dinero, robo de información personal; es por esto que la ciberseguridad es un punto vital para los usuarios ya que ayuda a prevenir, detectar y responder a estos ataques los cuales podrían afectar a las personas, organizaciones o incluso a naciones enteras.

Aunque a veces pareciera que fuera una pérdida de tiempo realizar ciertas actualizaciones en ocasiones puede ser de vital importancia, ya que estas no solo sirven para habilitar una nueva interfaz, drivers, controladores, sino que además también estas actualizaciones nos incluyen soluciones a errores o a su vez incluyen parches de seguridad, ya que estos errores puede ser una oportunidad para los ciberdelincuentes.

Por lo que dentro del mercado mundial existen dos tipos de sistemas operativos más utilizados por la sociedad; el sistema operativo comercial y el sistema operativo OpenSource; cada uno tiene sus propias características y especialidades en correspondencia al uso y a la seguridad del usuario, por ende, se tomara de modelo al sistema operativo comercial Windows 11 creado por la empresa Microsoft y el sistema operativo OpenSource Parrot Security OS.

De esta manera los sistemas operativos comerciales y OpenSource son susceptibles a vulnerabilidades y amenazas ante algún fallo en la seguridad ya que, al navegar por la web, instalar algún programa o aplicaciones proveniente de internet es un riesgo que toma el usuario debido a que existe la posibilidad de ser infectado por un virus, malware, gusanos o spyware sin percatarse.

Es por eso que este trabajo tiene como finalidad establecer comparaciones entre el sistema operativo Comercial Windows 11 y del sistema operativo OpenSource Parrot Security OS, teniendo en cuenta las actualizaciones dadas entre dichos sistemas, y de esta manera poder analizar qué tan seguro será nuestra navegación con el sistema operativo Comercial Windows 11 y del sistema operativo OpenSource Parrot Security OS, por eso mediante este estudio se responderá la siguiente pregunta: "¿Qué tan vulnerable puede ser el sistema operativo Comercial Windows 11 y del sistema operativo OpenSource Parrot Security OS ante las posibles amenazas cibernéticas que presentan los usuarios a medida que navegan en la internet?"

JUSTIFICACION

Conforme van pasando los años, el mundo está en constante desarrollo y va generando nuevas tecnologías por el bien y la evolución de la sociedad, a su vez esto genera también factores en los cuales se deben tener cierto grado de seguridad informática como puede ser el caso en los sistemas operativo, por lo que la sociedad debe estar debidamente capacitada sobre las posibles amenazas que conllevan a asegurar la información personal, institucional, empresarial o gubernamental; de ese modo evitara los ataques y amenazas de ciberdelincuentes en sus sistemas operativos.

Este estudio de caso irá direccionado para todas aquellas personas o entidades las cuales llevan sus actividades mediante el sistema operativo Comercial Windows 11 y del sistema operativo OpenSource Parrot Security OS, ya que de esta manera se les brindara la mayor información posible acerca de los ciberdelitos y que herramienta nos ayudará a evitarlos y prevenirlos.

Durante este trabajo se estará recabando información útil de distintos autores la cual va a permitir tener una mejor visión de la problemática en cuestión, y poder de esta manera brindar un trabajo el cual sea preciso y conciso.

OBJETIVOS DEL ESTUDIO

OBJETIVO GENERAL

- Elaborar un análisis comparativo de la seguridad del sistema operativo Comercial y del sistema operativo OpenSource entorno a la ciber amenazas.

OBJETIVOS ESPECIFICOS

- Conceptualizar las amenazas y vulnerabilidades de la ciberseguridad
- Analizar las herramientas de seguridad de los sistemas operativos ante las amenazas
- Evaluar la efectividad de ambos sistemas operativos en relación a las amenazas o vulnerabilidades

LINEA DE INVESTIGACION

Durante este estudio de caso lo que se buscara es determinar características de los sistemas operativos comercial y del sistema operativo OpenSource para esta manera poder detallar de una manera más acertada las diferencia entre los mismos y así poder realizar un análisis sobre los cambios realizados en estas mejoras.

El trabajo se estará realizando siguiendo directrices determinadas en la línea de investigación de “Sistemas de información y comunicación, emprendimiento e innovación” lo cual comprende las “Redes y tecnologías inteligentes de software y hardware”, además de esto durante todo este trabajo se estará utilizando una técnica de investigación documentada o bibliográfica.

MARCO CONCEPTUAL

SISTEMAS OPERATIVOS

En la actualidad los sistemas operativos son de mayor relevancia debido a los avances tecnológicos y el desarrollo de nuevos lenguajes de programación que han permitido a la sociedad nuevas tendencias a los funcionamientos de la informática, sin mencionar que al pasar los años se dan importantes actualizaciones en los servicios para los usuarios ya que las grandes empresas que manejan dichas cambios en los sistemas operativos se enfocan en favorecer en los requerimientos de la sociedad, determinando el uso de nuevas herramientas comerciales como son los mismos sistemas operativos.

Dentro del mercado existen dos tipos de sistemas operativos como los comerciales y los sistemas operativos OpenSource. En donde los sistemas operativos consisten en un software que organiza de forma sistemática los servicios y utilidades del usuario en una computadora, por ese motivo es necesario tener un conocimiento base sobre estos dos sistemas operativos; y los más utilizados son Windows, Linux, DOS, MAC, entre otros; por lo que hablaremos específicamente de dos sistemas operativos, el primero Windows para el sistema comercial y para el sistema OpenSource Parrot Security os:

Windows: De los más populares que existen, inicialmente se trató de un conjunto de distribuciones o entornos operativos gráficos, cuyo rol era brindar a otros sistemas operativos más antiguos como el MS-DOS una representación visual de soporte y de otras herramientas de software. Se publicó por primera vez en 1985 y desde entonces se ha actualizado a nuevas versiones.

Parrot Security os: Está basado en Debian el cual es una distribución de Linux que desempeña en actividades de seguridades informática como son los casos de análisis forenses, proteger y garantizar la red, y también trata sobre la

ciberseguridad, todas estas actividades y más puede realizar el Parrot Security os. (GCFGLOBAL, 2018)

Por consecuente, los sistemas operativos permiten el uso de otros programas que servirán de apoyo para su debido funcionamiento, por eso hay ciertos programas que pueden ser instalado y otros no por la seguridad y el bienestar de la máquina. También influye la interfaz gráfica, los gestores, las instrucciones del ordenador y las funciones y directrices dadas por el usuario.

Todo el contenido dentro de un sistema operativo es de vital importancia para su funcionamiento para el debido proceso en su administración de recursos, intercomunicación entre el usuario, aplicaciones, programas y el mismo sistema para tener una adecuada interacción con los usuarios para un manejo favorable en su entorno, ser eficaz en el correcto funcionamiento de los programas y aplicaciones, y mejorar constantemente por medio de actualizaciones brindadas por la empresa. Por último, es necesario conocer el entorno que caracteriza los sistemas operativos comerciales y OpenSource.

SISTEMA OPERATIVOS COMERCIALES

Dentro del área de los sistemas comerciales se conoce que estos están ambientados para la comercialización ya que al ser un software de tipo privado se necesita una licencia de paga para ser instalado en una máquina, así mismo contiene diversos programas o aplicaciones comerciales que para ser usado se debe realizar un pago en su licencia como por ejemplo el paquete office.

El autor Hershel Gonzales nos mencionan que:

> En informática un sistema operativo comercial es aquel que lo produce alguna compañía y está compañía cobra dinero por el producto, su

> distribución o soporte. Es decir, es aquel que genera dinero para la empresa que lo desarrolló a través de la venta del sistema operativo o soporte. (GONZALES, 2021)

Para el autor (Glez, 2018)"Fueron creados por empresas para su uso comercial. Tales empresas son sus propietarias y cobrar por utilizarlo y distribuirlo y aquellos que lo diseñaron y crearon ocultan su código original para evitar que se altere."

Tomando como punto de referencia de ambos autores, nos dice que un sistema operativo comercial es creado por compañías con la finalidad de distribuir su producto y servicio a los usuarios con un soporte de ayuda en caso de tener problemas técnicos, claro está que todos estos servicios tendrán un costo a pagar por parte del usuario para obtener dichos beneficios otorgados por los empleados de la empresa.

De esta forma se puede decir que todo sistema operativo comercial son aquellos sistemas de pago para poder ser usado y tener sus beneficios como es el soporte técnico, que es sencillo de manejar.

SISTEMA OPERATIVO WINDOWS 11

La empresa Microsoft es la creadora del famoso sistema operativo Windows por lo que el desarrollo de su última versión que es el Windows 11 está bajo su propiedad, esta última versión ha tenido mejora en su rendimiento y su usabilidad es sencilla, además hubo varios campos importantes como lo es en la parte del hardware, en su interfaz, en su seguridad, en su almacenamiento en las nubes y entre otras cosas.

Los requisitos mínimos del Windows 11 son los siguientes:

- Tener un procesador CPU de 1GHz (2 o más núcleos)

- Con una memoria de 4 GB RAM
- Un almacenamiento de 64 GB
- Una tarjeta gráfica que sea compatible con DirectX 12 / WDDM 2.x
- Una pantalla de 9 pulgadas con resolución de 720p
- Un firmware del sistema UEFI compatible con Arranque seguro
- Con un módulo de plataforma segura
- Con conexión a Internet

HERRAMIENTAS DE CIBERSEGURIDAD

El **Windows Defender** se incluye en Windows 11 como parte del mismo sistema, está integrado con el sistema y, como el resto de soluciones instaladas, se adelantan a la introducción de malware, lo detecta y en su caso lo elimina gracias a sus capacidades proactivas. Pero también el usuario puede usarlo para escanear activamente en busca de malware tanto las unidades de almacenamiento interno como las externas conectadas. En este práctico básico, repasamos un uso que no difiere del resto de antivirus gratuitos.

Plutón es un procesador dedicado solamente a la seguridad e incrustado. Esto es, un TPM directamente en el procesador que almacena las claves de cifrados para proteger información. Además, el firmware de Plutón será controlado por las propias actualizaciones de Windows.

Con **Config Lock**, no habrá ninguna ventana de oportunidad entre el momento de cambio de algún valor de seguridad perpetrado por el usuario y la aplicación de la política de seguridad impuesta por la administración.

Personal Data Encryption se trata de cifrar los archivos, con una capa de cifrado invisible también para el usuario. Pero este no tendrá que recordar ni ejecutar nada para

descifrar su información, sino que al hacer login con Hello en Windows, podrá acceder a sus datos sin problemas.

Si el usuario desactiva algún sistema de seguridad, inmediatamente volverá al estado predeterminado.

SISTEMA OPERATIVO OPENSOURCE

Se denomina OpenSource a los sistemas que permiten el total acceso a su código de programación, con el objetivo de facilitar modificaciones por parte de programadores externos que no fueron parte de la creación de dicho software.

Como se había mencionado anteriormente, otro de los beneficios del OpenSource, es que da la total libertad que el usuario (no solamente programadores) puedan copiar, modificar o distribuir un software libre sin tener en contra una acción legal.

Y de acuerdo el autor Daniel Gonzales Piñero menciona que:

> Miles de personas, especialmente desarrolladores de software (profesionales o amateurs), se han adherido a esta forma de pensar, creando una comunidad virtual de ámbito mundial. Así pues, este grupo de personas dedican habitualmente su tiempo libre a desarrollar nuevas aplicaciones y compartir con la comunidad las ya creadas, de forma que en grupo puedan mejorarlas y añadirles características, convirtiéndolas en muchas ocasiones en proyectos de magnitudes ni siquiera soñadas por el desarrollador original. (Piñero, 2019)

De acuerdo a lo que citó, el autor Piñero nos menciona que gracias al trabajo colaborativo de los desarrolladores de software y de personas que crearon una comunidad virtual donde se publican incontables foros sobre problemas, soluciones, actualizaciones, modificaciones y personalización del sistema; gracias a esto, se puede obtener diversas respuestas a sin números de inconvenientes que puedan suscitar en un sistema operativo OpenSource.

SISTEMA OPERATIVO PARROT SECURITY OS

Es una distribución de Linux que está basada en Debian cuyo desarrollador es Frozenbox Team, y ha sido elaborada para el campo de la ciberseguridad, análisis forense, pentesting, entre otras cosas

Se puede recalcar que el sistema operativo Parrot Security OS nos ofrece variedad de herramientas que pueden ser utilizadas para la ciberseguridad y análisis forense, y también incluye la opción de desarrollar tus propios programas y proteger tu privacidad mientras navegas por la red.

Security Edition

Esta edición está diseñada para proporcionar un conjunto completo de herramientas para realizar todo tipo de pruebas de penetración. También permite usarla para la mitigación de ataques, investigación de seguridad, análisis forense y evaluación de vulnerabilidades.

La edición Security también cuenta con todo lo necesario para realizar pruebas de informática forense y navegación web anónima. Además, todo lo que no viene instalado de serie se puede bajar desde los repositorios oficiales sin problemas.

Home Edition

Esta edición se ha diseñado para uso diario y está enfocada a usuarios que busquen un sistema operativo más ligero y rápido en vez de uno tan avanzado y completo como la edición Security. Es una edición perfecta tanto para dar los primeros pasos dentro de ella como para estudiantes y programadores.

Esta edición incluye programas para chatear en privado con personas, cifrar documentos y navegar por Internet de forma anónima.

Requisitos mínimos y recomendados

Dependiendo de la edición que elijamos, los requisitos que debemos cumplir serán casi los mismos ya que para usar Parrot Security OS, es recomendable tener lo siguiente:

- Procesador Quad-Core de 64 bits.
- 8 GB de memoria RAM.
- 128 GB de espacio de almacenamiento SSD.

HERRAMIENTAS DE CIBERSEGURIDAD

Aquí podríamos escribir durante horas sobre todas las aplicaciones con las que cuenta Parrot OS. En nuestro caso vamos a destacar solo las que son más utilizadas en general de esta distribución.

- **OnionShare.** Utilidad de código abierto para compartir archivos de forma segura y anónima a través de TOR.
- **AnonSurf.** Sirve para mantener el anonimato, pasando por TOR u otros sistemas que lo mantienen y garantizan, sin necesidad de un navegador en especial. También anonimiza protocolos de comunicación como P2P, haciendo la comunicación mucho más segura.

- **I2P.** También es utilizado para el anonimato y permite acceder a los servidores de la DarkNet.
- **Electrum Bitcoin Wallet** sirve como una cartera electrónica que utiliza servidores distribuidos para mantenerse en el anonimato y permite guardar y transferir Bitcoins de forma segura.
- **Ricochet.** Utiliza cadenas especificas con mensajes cifrados de extremo a extremo debido a que es un chat seguro y en anonimato.
- **Crunch.** Es un creador de diccionarios para ataques de contraseña, el cual genera un sin número de listas de contraseñas hasta poder encontrar la correcta permutación.
- **CUPP. -** es un generador de diccionarios avanzado para usuarios que permite la creación de perfiles de contraseñas personalizadas.
- **Bleachbit.** Es un limpiador de espacio en disco duro, que elimina archivos de registro inútiles, el historial de internet, cookies y archivos temporales, entre otros.
- **Macchanger.** Sirve para evitar el filtrado de información de la dirección de los enrutadores por medio del cambio de la MAC.
- **OpenVas.** es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad. (Velasco, 2022)

CIBERSEGURIDAD

Los sistemas informáticos dieron un cambio total en el vivir de las personas, ya que por medio de estos sistemas pueden acceder a sin números de sitios en donde cada acción lo lleve a un lugar en específico que ira en constante cambio, y según el autor (Alonso García, 2020) “la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día”.

Tras aquello cabe resaltar que estar navegando en la red es un arma de doble filo ya que al haber usuarios que realizas sus actividades cotidianas en la World Wide Web sin perjudicar a otros usuarios, así mismo existen usuarios que realizan actividades ilícitas con las herramientas cibernéticas, por lo que a pesar de que hay seguridad en cada sistema operativo, existe la posibilidad de que los ciberdelincuentes desarrollen nuevos métodos y técnicas para amenazar y vulnerar los sistemas de seguridad.

Por otra parte, el Autor (Alvarado, 2019) que citó a ISACA menciona que la ciberseguridad es la “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”, tras lo mencionado es por ese motivo que la ciberseguridad está conformado por un conjunto de herramientas para salvaguardar la información de los usuarios y de una organización.

FUNCIONES DE LA CIBERSEGURIDAD

Las principales funciones de la ciberseguridad son: Identificación, protección, detección, respuesta y recuperación.

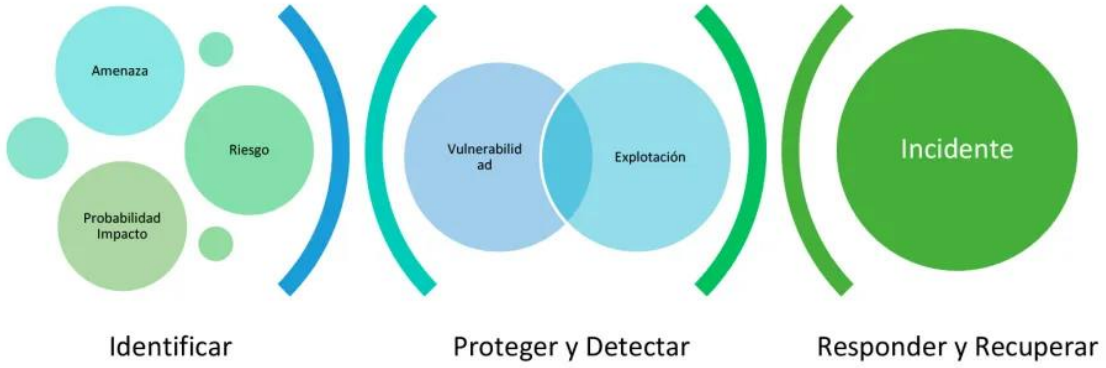


Imagen 1. Gabriel Lis y Jeimy Poveda (31 de abril de 2022.) Funciones Básicas de la Ciberseguridad [Imagen]. Recuperado de https://news.itsmf.es/.

De acuerdo al autor (Moreno, 2022) "Es importante recordar que para dar respuesta a los riesgos que se han identificado, y cuyo nivel no es aceptable por la misma, disponemos de diferentes marcos de control y medidas que nos pueden ayudar en esta respuesta."

Cada función de la ciberseguridad tiene un propósito en el cual deben cumplir ciertas indicaciones de seguridad para luego realizar una rigurosa evaluación de probabilidad de riesgos tras algún peligro informático e intentar solucionarlo o evitarlo.

El primero de estas funciones es el de Identificación, que su rol conlleva a identificar, evaluar y analizar las posibles amenazas de las actividades del usuario u organización; es decir, esta función tiene como fin recabar toda información de entrada y así saber que se debe proteger y como proteger el sistema ante las amenazas informáticas.

La segunda función es la Protección, se llevará a cabo con la recopilación de información proporcionada por el proceso de identificación de amenazas y riesgo, por lo que una vez identificado los peligro se puede plantear medidas de seguridad para disminuir los riesgos y amenazas, como por ejemplo utilizar un antimalware.

En la Tercera función es la Detección, el cual dará apoyo a la función de Protección ya que cada vez existen un sin número de amenazas a veces es difícil proteger el sistema con un solo tipo de mecanismo de seguridad, por ello es considerable tener otros mecanismos de detección de amenazas y ataques.

La cuarta función es la Respuesta, en donde se hace referencia que nuestro equipo está bajo un ataque o ya fue infectado, por lo que tendrá como objetivo recabar todas las actividades realizadas en las últimas horas para descubrir el incidente de vulnerabilidad en la seguridad del sistema.

La última es la recuperación en donde ya luego de que la máquina haya sido infectada, se procederá a buscar la forma de recuperar lo perdido, infectado o borrado del ataque, por lo que una de las formas es el proceso de restauración de copa de seguridad para así devolverlo a su estado original antes del ataque de seguridad.

CIBERAMENAZAS

Las amenazas a las que se enfrenta la ciberseguridad son tres:

- El delito cibernético incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.
- Los ciberataques a menudo involucran la recopilación de información con fines políticos.
- El ciberterrorismo tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor. (Lab, 2022)

Además, se mencionará los métodos más utilizados para las amenazas que ponen en riesgo la ciberseguridad.

El Malware es el más conocido por los cibercriminales ya que permite interrumpir o dañar el equipo del consumidor y es realizado por medio de un correo electrónico en donde se adjunta un archivo, por aplicaciones, suscripciones gratuitas, entre otros; con el fin de acceder a datos de un usuario, empresa u organización.

Con el pasar de los años se han ido creando variantes de malware en donde cada uno tiene su propio objetivo de ataque; algunas de estas variantes son: Virus, Troyanos, Spyware, Ransomware, Botnets, Adware.

A continuación, detallaremos algunas de las variantes de malware:

- El virus es un programa capaz de expandirse por todo el sistema, el cual tiene la finalidad de infectar con códigos maliciosos los archivos del computador.
- Para (Muñoz, 2021) los Troyanos "Se trata de un programa malicioso que se hace pasar por algo legítimo o inofensivo para intentar acceder a la computadora o dispositivo móvil de la víctima y realizar distintos tipos de acciones maliciosas."
- Los Spyware tiene la finalidad de registrar todos los movimientos del usuario para luego usar dicha información.

También existen ataques de Inyecciones de código SQL, que consiste en aprovechar las vulnerabilidades de las bases de datos mediante la inserción de un código malicioso para tomar el control y robar los datos de una base de datos.

Por otra parte, están los Phishing y de acuerdo a lo que nos menciona el autor (Rivero, 2019) "se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS."

Por consecuente también existen los ataques que interceptan la comunicación entre usuarios para robar los datos y/o información, pueden ocurrir mediante una red Wi-Fi no segura; estos tipos de ataque se los denominan como “Man-in-the-middle”

De acuerdo a (FERNÁNDEZ, 2022) “es cuando un grupo de personas o automatismos atacan a un servidor u ordenador desde muchos equipos a la vez. Este flujo masivo de datos hace que los recursos del servidor colapsen y deje de funcionar.”

VULNERABILIDADES DE LA CIBERSEGURIDAD

Las vulnerabilidades en la ciberseguridad suceden cuando el atacante puede obtener la integridad, confidencialidad, control y acceso a los datos del sistema o aplicación.

Y con el respaldo del autor (Castillo, 2020) menciona que “Estas vulnerabilidades son producto de fallos producidos por el mal diseño de un software, sin embargo, una vulnerabilidad también puede ser producto de las limitaciones propias de la tecnología para la que fue diseñado.”

Tras lo mencionado, se puede decir que las vulnerabilidades son problemas de seguridad que persiste en un sistema, ocasionando que el usuario sea expuesto por los hackers o ciberdelincuentes poniendo en riesgo la confidencialidad e integridad de sus datos.

MARCO METODOLOGICO

En el presente caso de estudio se empleó la metodología cualitativa debido a que permite conocer la perspectiva de especialistas o profesionales con respecto a la experiencia y su conocimiento en relación al caso de estudio.

De lo cual también se empleó el método bibliográfico, en donde se recopilo información de casos de estudios, investigaciones, libros, revistas y artículos científicos publicados por anteriores autores, para luego ser llevado a un proceso de análisis, síntesis, deducción y obtener un nuevo conocimiento para dar con una conclusión.

La técnica que se utilizo fue la entrevista debido a que es una forma de recopilar información sobre el tema estudiado, ya que el entrevistado nos dará una opinión de acuerdo a su experiencia y conocimiento de la ciberseguridad; por lo cual se aplicó un cuestionario de preguntas abiertas con el objetivo de profundizar el tema y encontrar detalles importantes que no han sido considerado para la investigación.

RESULTADOS

WINDOWS 11	Ventajas de ciberseguridad	Desventajas de ciberseguridad
HERRAMIENTAS DE CIBERSEGURIDAD	• Las actualizaciones consumen pocos recursos. • Protección en tiempo real de la nube • Analiza cada archivo del dispositivo tanto carpetas internas e información externa. • Notifica los problemas de manera rápida. • Realiza análisis periódicos del sistema • Detecta amenazas de phishing, de malware, de spyware, de virus. • Maneja un Firewall. • Brinda un reporte del sistema. • Seguridad del hardware. • Controles parentales.	• En ocasiones el análisis de todos los archivos ralentiza el sistema. • La detección de malware es un poco superficial. • El informe de estado del sistema de PC es básico (y no incluye optimización del rendimiento ni limpieza del sistema) • Carece de una red privada virtual (VPN) • Carece de protección contra el robo de identidad • Carece de monitorización de la dark web • Carece de protección antirrobo de identidad • Carece de protección de webcam y micrófono • Pocas herramientas de optimización del sistema • Carece de gestor de contraseñas

De acuerdo al cuadro de las ventajas que tiene Windows 11 con respecto a la ciberseguridad, tiene una herramienta básica pero eficiente que le permite analizar los archivos del computador mientras está verificando que no exista alguna amenaza y en

caso de existir, notifica inmediatamente al usuario que se ha encontrado un potencial problema que podría afectar al sistema, por lo cual procederá a bloquearlo y aislarlo para su eliminación, por consecuente nunca dejara de analizar y proteger al usuario ya que trabaja en tiempo real en conjunto al firewall y análisis periódicos del sistema, pero aun así, también existe las contras de Windows defender, debido a que a pesar que contiene varios parámetros para proteger el sistema ante las amenazas de terceros, también carecen de ciertas medidas de seguridad como es el control de protección en sus dispositivos de audio y video, lo que provocaría que un hacker o un tercero grabe lo que este proyectando el computador o la laptop en tiempo real sin que el perjudicado se dé cuenta; también no tiene suficientes herramientas para realizar profundos análisis al sistema para ser identificados y resolverlo, como es el caso de ataques de los ataques de denegación de servicios.

Parrot Security OS	**Ventajas de ciberseguridad**	**Desventajas de ciberseguridad**
HERRAMIENTAS DE CIBERSEGURIDAD	• Privacidad y criptografía • Recopilación de inteligencia • Asesoría de vulnerabilidades • Análisis de aplicaciones web • Análisis de BBDD • Control de accesos • Herramientas de gestión WIFI • Testeo de fuerza de redes WIFI • Sniffers / Spoofers • Herramientas forenses digitales • Ingeniería inversa • Herramientas de gestión de informes	• Ninguna desventaja en relación a la ciberseguridad

	• Aircrack-ng testea la seguridad inalámbrica. • Nmap escaneo de puertos y analizar la seguridad de redes. • owas-zap permite encontrar vulnerabilidades en aplicaciones web. • Wireshark analiza paquetes y protocolo en redes	

Mientras en el cuadro de ventajas del sistema operativo Parrot Security OS contiene muchas herramientas de ciberseguridad que permiten mantener protegido el sistema operativo ante los ataques cibernéticos, dichas herramientas constan de seguridades en las redes al momento de navegar por la World Wide Web, enmascaramiento de la IP el cual permitirá no ser rastreado fácilmente y ser víctima de ciberacoso como es el ejemplo de los doxers que son personas que tienen la finalidad de revelar la información personal de otro individuo sin su consentimiento hacia el público, esto sucede con frecuencia en mediana y grandes empresas. También consta con asesoría de vulnerabilidad, es decir que son personas o grupo o comunidad que brinda un servicio de ayuda sobre alguna problemática de vulnerabilidad; por otra parte, la protección de documentación será sumamente asegurada ya que existe una herramienta que permite usar la criptografía para que el documento sea confidencial y autentico, además para abrirlos, solo tendrán la autorización de las personas que estén autorizadas y conozcan la correspondiente clave.

DISCUSION DE RESULTADOS

Tras el proceso de investigación se pudo obtener información relevante sobre cuáles son las amenazas y vulnerabilidades que persisten en la actualidad para perjudicar al usuario, y además se pudo recabar información sobre las herramientas que utilizan para proteger de manera eficaz y segura el sistema.

Como se pudo observar en los cuadros de ambos sistemas operativos, cada uno tienen sus medidas de seguridad que implementan parámetros para denegar e impedir que terceros accedan a la información del computador, que manipulen los servicios de administración, que inclusive bloquean posibles riesgos de ataques por parte de malware y otros métodos utilizados por los hackers.

Por lo cual a partir de las investigaciones anteriormente realizadas de amenazas y vulnerabilidades con relación a las herramientas de seguridad del sistema operativo Windows 11 y del sistema operativo Parrot Security OS, se puede determinar que ambos cumplen con su objetivo de proteger al usuario ante los invasores que buscan perpetrar la integridad, confidencialidad y seguridad de la persona.

A pesar de que ambos cumplen su objetivo, uno está por encima del otro debido a que el sistema operativo Parrot Security OS está inmerso en complacer al usuario a sentirse realmente seguro, ya que como se pudo observar en los cuadros, este contiene muchas más herramientas que protegen varios campos del sistema como son: la seguridad de la red, la criptografía, realizar análisis forense en la propia máquina, poder escanear los puertos de red que estén abierto de la maquina y muchos demás beneficios que aporta tener el sistema operativo Parrot Security OS; en cambio a pesar de que Windows también contiene sus propias herramientas de seguridad, sigue estando por detrás ya que al ser un antivirus con opciones de seguridades básicas, no podrá ser capaz de proteger el ordenador de otros tipos de amenazas; por ejemplo hay ocasiones que nosotros

descargamos varios archivos por la internet en páginas no tan seguras de las cuales pueden contener amenazas más complejas que por lo usual no podrían manejarlo, ya que al no tener más opciones de seguridad, este será vulnerable, como es el caso en conectarse a otra red externa (no del hogar), este no consta con medidas para proteger nuestra privacidad.

CONCLUSIONES

El presente estudio de caso ha logrado determinar los conceptos básicos de las amenazas y vulnerabilidades que existen en el campo de la ciberseguridad, que han sido aportes fundamentales de varios autores para informar a los usuarios los riesgos que existen al navegar por la internet, así mismo se ha podido identificar las herramientas de seguridad que tienen estos dos sistemas operativos al momento de contrarrestar los ataques cibernéticos.

Algunas herramientas de seguridades en el sistema operativo de Windows serán de mucha ayuda para los usuarios como es el caso de Windows Defender debido a que, al ser un antivirus básico permite realizar un análisis constante del sistema, protegiéndolo en tiempo real ante las amenazas de phishing, de spyware, de virus entre otros tipos de ataques y la persona puede solicitar el reporte del análisis del sistema. Mientras que el sistema operativo Parrot Security OS, creado exclusivamente para la seguridad informática, por lo tanto, ofrece a sus usuarios un completo ecosistema de pruebas de penetración, evaluación y análisis de vulnerabilidades, incluyendo herramientas que permiten el análisis de sistemas forenses, la preservación del anonimato, así como la practica con la criptografía y el cifrado; medidas de seguridad que Windows defender no proporciona, por lo que si el usuario busca un sistema que le garantice su seguridad ante las amenazas y vulnerabilidades, este es el indicado ya que como se había mencionado antes y se pudo observar en el cuadro de Parrot Security OS esta más apto para ser la defensa total de peligros cibernéticos usando la herramienta Macchanger que consiste en evitar que se filtre la MAC del router y permanecer en el anonimato.

Gracias a las investigaciones realizadas y los cuadros comparativos de los sistemas operativos mencionados, se puede denotar la efectividad del Parrot Security OS, ya que garantiza la protección de ataque cibernéticos, no solo por la amplia lista de

opciones de seguridad que cuenta, sino que también abarca seguridad en redes, seguridad antimalware, escaneo de vulnerabilidades en redes y puertos, eliminación de archivos temporales y de dudosa procedencia, entre otras herramientas que permitirán al usuario sentirse seguro y protegido.

Cabe recalcar que, a pesar de que el Parrot Security OS está por encima del Windows 11 en relación a ciberseguridad; el entorno del Windows 11 es más agradable y sus actualizaciones de parches son más fáciles de instalar.

RECOMENDACIONES

En la actualidad con el crecimiento de la tecnología y el uso del internet en nuestra cotidianidad es necesario tomar ciertas medidas de prevención al momento de usar un dispositivo con acceso a internet, por lo que, recomiendo que antes de adquirir o usar un computador, se realice una pequeña investigación sobre la seguridad que ofrece el sistema operativo instalado en casos de ciberataques, ya que al tener desconocimiento sobre las capacidades que tienen nuestros ordenadores en enfrentar los ataques de los hackers que son personas especializadas en realizar estas actividades con fines delictivos o maliciosos, nos volvemos vulnerables al navegar por la World Wide Web por lo que es mejor prevenir dichos riesgos.

Se sugiere a los usuarios utilizar el sistema operativo Parrot Security OS porque cuenta con la preparación y las estrategias necesarias de ciberseguridad para evitar accesos no autorizados en permisos administrativos y en redes, así como evitar filtraciones de información, deshabilitar servicios innecesarios, monitoreo del estado de tráfico de red, generador de diccionario para perfiles de contraseñas, entre demás medidas

de seguridad, ya que es común manejar un flujo de información importante y confidencial en el diario vivir, y necesitamos protegerla.

Cabe recalcar, que no todos los usuarios necesitan un alto nivel de ciberseguridad, ya que va en función de las actividades que realizan o de las empresas que lo usan.

REFERENCIAS

Alonso García, J. (2020). *Derecho penal y redes sociales.* Madrid: Aranzadi.

Alvarado, A. R. (MAYO de 2019). *www.researchgate.net.* Obtenido de https://www.researchgate.net/publication/338518716_INTRODUCCION_A_LA_CIBERSEGURIDAD

Castillo, R. (2 de Diciembre de 2020). *Tecnología + Informática.* Obtenido de https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

FERNÁNDEZ, Y. (24 de Enero de 2022). *XATAKA BASICS.* Obtenido de https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte

GCFGLOBAL. (2018). *SISTEMAS OPERATIVOS PARA EL COMPUTADOR*. Obtenido de https://edu.gcfglobal.org/es/informatica-basica/sistemas-operativos-para-el-computador/1/

Glez, A. G. (2018). *iesvillalbahervastecnologia.files.wordpress.com.* Obtenido de https://iesvillalbahervastecnologia.files.wordpress.com/2018/10/sistemas-operativos.pdf

GONZALES, H. (8 de AGOSTO de 2021). *herschelgonzalez.com*. Obtenido de https://herschelgonzalez.com/que-es-un-sistema-operativo-comercial/

Lab, A. K. (2022). *Kaspersky* . Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Moreno, M. Á. (30 de Marzo de 2022). *Information Technology Service Management PARA TI.* Obtenido de https://news.itsmf.es/las-funciones-basicas-de-la-ciberseguridad/

Muñoz, F. (14 de Mayo de 2021). *Welivesecurity.com.* Obtenido de https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/

Piñero, :. D. (19 de Enero de 2019). *www.cs.upc.edu.* Obtenido de https://www.cs.upc.edu/~tonis/daniel_gonzalez_pinyero.pdf

Rivero, M. (23 de Diciembre de 2019). *InfoSpaware.* Obtenido de https://www.infospyware.com/articulos/que-es-el-phishing/

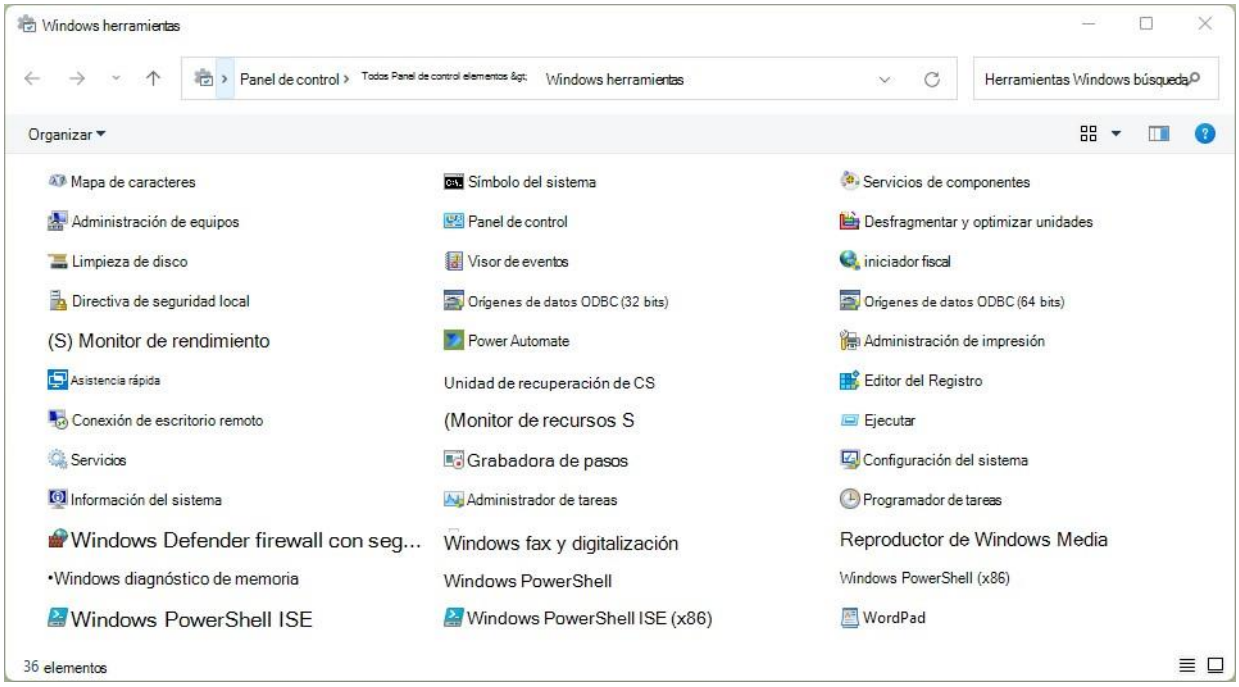
Velasco, R. (20 de abril de 2022). *softzone.* Obtenido de https://www.softzone.es/linux/distros/parrot-os/

Monterrubio-Hernández, E. (2019). Sistema Operativo. Con-Ciencia Serrana Boletín Científico De La Escuela Preparatoria Ixtlahuaco, 1(1). Recuperado a partir de https://repository.uaeh.edu.mx/revistas/index.php/ixtlahuaco/article/view/3672

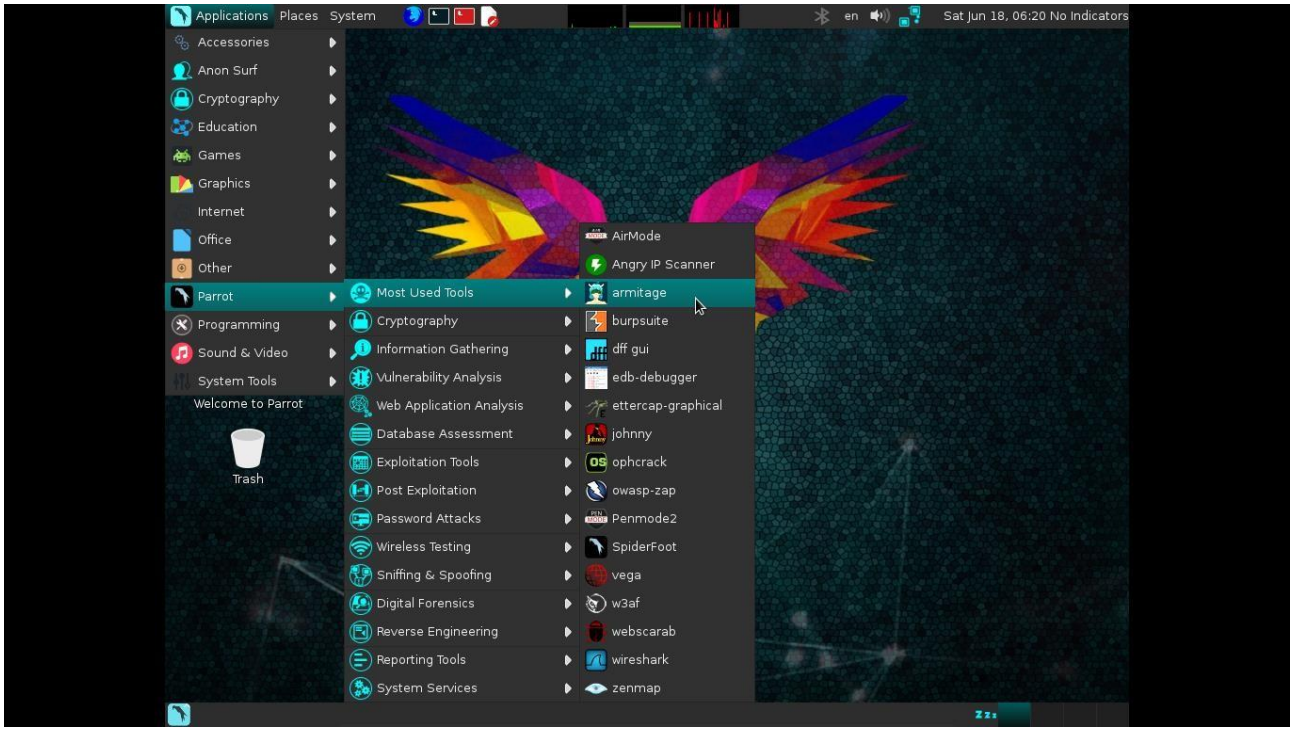
Gabriel Lis y Jeimy Poveda (31 de abril de 2022.) Funciones Básicas de la Ciberseguridad [Imagen]. Recuperado de https://news.itsmf.es/.

ANEXOS

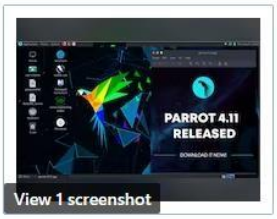
Anexox 1° Sistema Operativo Windows 11



Anexo 2° Sistema Operativo Parrot Security OS



Anexo 3° Comparaciones de sistemas operativos

+ Add Product	Parrot OS by Parrot Security VIEW PROFILE	Windows 11 by Microsoft VIEW PROFILE
Starting Price	N/A	N/A
Ratings	Overall ★ 4.0 (2) See all ratings	Overall ★ 4.3 (10) See all ratings
Best For	Not provided by vendor	Operating System for Windows users
Features	5 / 7 See all features	6 / 7 See all features
Deployment	✓ Cloud-based ✗ On-premise	✓ Cloud-based ✓ On-premise
Training Software	✓ Documentation ✗ Videos	✓ Documentation ✓ Videos
Support	✗ Email/Help Desk ✓ Knowledge Base Software ✗ Chat	✓ Email/Help Desk ✗ Knowledge Base Software ✓ Chat
Screenshots	 View 1 screenshot	 View 3 screenshots

Cumple con los requisitos	9.6 Respuestas: 14	9.1 Respuestas: 1464
Facilidad de uso	8.8 Respuestas: 14	9.1 Respuestas: 1468
Facilidad de configuración	9.0 Respuestas: 5	8.9 Respuestas: 334
Facilidad de administración	9.3 Respuestas: 5	8.7 Respuestas: 330
Calidad de soporte	8.3 Respuestas: 15	8.4 Respuestas: 1322
¿El producto ha sido un buen socio para hacer negocios?	9.3 Respuestas: 5	8.6 Respuestas: 312
Dirección del producto (% positivo)	9.2 Respuestas: 14	8.8 Respuestas: 1386

Pequeños negocios (50 emp. o menos)	62,5%	34,0%
Mercado medio (51-1000 emp.)	12,5%	32,3%
Empresa (> 1000 emp.)	25,0%	33,7%

Industria de revisores

Seguridad informática y de redes	29,2%	Tecnología de la Información y Servicios	20,9%
Tecnología de la Información y Servicios	25,0%	Software de ordenador	12,8%
Administración de educación	12,5%	Educación más alta	4,2%
Software de ordenador	12,5%	Administración de educación	3,8%
Seguridad e Investigaciones	4,2%	Seguridad informática y de redes	3,0%
Otro	16,7%	Otro	55,4%

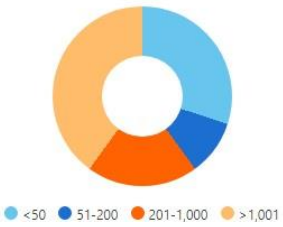
Anexo 4° Reseña de los sistemas operativos

Reseñas de Windows 11

Puntuación media

General	★ 4.3
Facilidad de uso	★ 4.5
Servicio al Cliente	★ 4.0
Características	★ 4.6
Relación calidad-precio	★ 4.4

Valoraciones por tamaño de empresa (empleados)



Buscar reseñas por puntaje

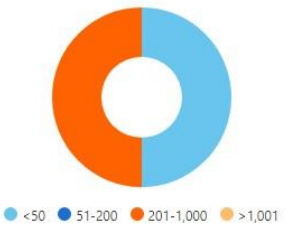
5 ★	40%
4 ★	50%
3 ★	10%

Reseñas de Parrot OS

Puntuación media

General	★ 4.0
Facilidad de uso	★ 3.0
Servicio al Cliente	★ 3.0
Características	★ 4.0
Relación calidad-precio	★ 5.0

Valoraciones por tamaño de empresa (empleados)



Buscar reseñas por puntaje

4 ★	100%