**5.4.1. Busca información sobre diferentes herramientas que permitan bloquear spyware u otro código malicioso en nuestro equipo.**

Malwarebytes Anti-Malware

Malwarebytes Anti-Malware (MBAM) es un antiespías gratuito. Malwarebytes Anti-Malware es capaz de detectar y erradicar programas espía, falsos antivirus y todo tipo demalware y spyware no detectado por los antivirus tradicionales.

Para usarlo, elige un análisis(rápido, completo o de memorias USB) y haz clic en Analizar; Malwarebytes Anti-Malware escaneará el equipo en busca de rastros de malware. Si no puede eliminarlos, lo intenta tras reiniciar el equipo. Su herramientaFileASSASSIN sirve precisamente para eso.

La versión gratuita de Malwarebytes Anti-Malware incluye unacuarentena de archivos, actualizaciones gratuitas y una lista de ignorados, pero carece de protección en tiempo real, programador de tareas y bloqueo de páginas, características que se obtienen trascomprar una licencia.

Malwarebytes Anti-Malware es quizá el mejor antiespías en circulación, e incluso sin protección en tiempo real constituye un formidable compañero para cualquier antivirus.

SuperAntiSpyware

Los virus no son los únicos programas peligrosos para tu equipo. Los programas espía constituyen una molestia igual de importante, una amenaza que no todos los antivirus tradicionales son capaces de afrontar.

SuperAntiSpyware detecta y elimina todo tipo de spyware, desde troyanos y adware hasta dialers y cookies sospechosas. Analiza la memoria, el registro y las unidades que elijas en busca de software malicioso.

Los análisis de SuperAntiSpyware son rápidos y fiables. Los elementos que quieres examinar en un segundo momento se almacenan en cuarentena, mientras que los demás serán eliminados sin demora.

La versión gratuita de SuperAntiSpyware, aún conservando la misma potencia de la Pro, tiene algunas limitaciones importantes, como la falta de actualizaciones automáticas y de protección en tiempo-real. Es el mismo camino que han seguido otros programas, pero no llega a dañar la validez de SuperAntiSpyware, un antiespías excelente.

**5.4.2. Busca la explicación de cada uno de los malware vistos arriba. Una pregunta del examen será definir algunos de ellos.**

**Adware**

Un programa de clase adware (software publicitario) es cualquier programa que automáticamente muestra u ofrece publicidad no deseada o engañosa, ya sea incrustada en una página web mediante gráficos, carteles, ventanas flotantes, o durante la instalación de algún programa al usuario, con el fin de generar lucro a sus autores.

**Bloqueador o Adblocker**

Un 'adblocker' es un programa o extensión que se instala en cualquier navegador con apenas unos clics, de tal manera que pueda hacerlo todo el mundo y que no requiera un gran trabajo para nadie, se tengan o no conocimientos en informática.

**Bomba Lógica**

Una bomba lógica es una parte de un código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.

**Virus Joke**

Un virus joke (en español: "virus de broma"), comúnmente llamados con el anglicismo jokes son programas ejecutados de manera similar a las acciones de un virus informático en un ordenador. Su objetivo no es atacar, sino gastar una broma a los usuarios, haciéndoles creer que están infectados por un virus y que se están poniendo de manifiesto sus efectos. Aunque su actividad llega a ser molesta, no producen realmente efectos dañinos.

**Bulo o Hoax**

Los hoaxes o bulos informáticos pueden abarcar una amplia gama de temas: advertencias sobre virus informáticos o supuestos riesgos para la salud, historias de terror, teorías de conspiración, peticiones de donaciones para enfermos graves y muchos más.

**Capturador de pulsaciones o Keylogger**

Un keylogger es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado. Este malware se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note.

**Clicker**

Es una técnica maliciosa para engañar a usuarios de Internet con el fin de que revelen información confidencial o tomar control de su ordenador cuando hacen clic en páginas web aparentemente inocentes o en su propio equipo.

**Criptovirus o Ransomware**

Un ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

**Downloader**

El término descarga se utiliza frecuentemente para la obtención de contenido a través de una conexión a Internet, donde un servidor remoto recibe los datos que son accedidos por los clientes a través de aplicaciones específicas, tales como navegadores.

**Espía o Spyware**

El programa espía (en inglés spyware) es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

**Exploit**

Es un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio.

**Herramienta de fraude**

La detección automática de fraude es el proceso de descubrir fraude utilizando máquinas, comúnmente computadoras con software diseñado específicamente para esto.

**Instalador o Drooper**

Un dropper es un tipo de troyano y son tan distintos que pertenecen a su propia raza. Su propósito de firma es instalar otro malware una vez que están presentes en un sistema. De hecho, se denominan trojan-dropper porque colocan malware y componentes de malware en un sistema comprometido.

**Stealer**

Es el nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, tal como su nombre de acceso a sitios web, contraseña o número de tarjeta de crédito.

**Dialer**

Un dialer es un programa que marca un número de teléfono de tarificación especial usando el módem, estos NTA son números cuyo coste es superior al de una llamada nacional.

**Puerta trasera o Backdoor**

Es una secuencia especial o un término trasero dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autenticación) para acceder al sistema.

**Rootkit**

Un rootkit es un conjunto de software que permite un acceso de privilegio continuo a un ordenador pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

**Secuestrador del navegador o Browser Hijacker**

Se trata de un secuestrador del navegador que una vez dentro del sistema empieza a realizar ciertas actividades maliciosas, como la modificación de la configuración del navegador o ralentizar drásticamente el sistema.

**5.4.3. Busca información sobre 5 ejemplos reales y muy peligrosos de malware. Primero pon la definición del tipo de malware y después haz una ficha con el nombre, nombre de archivo y método de propagación e infección y mecanismo de reparación.**

Phishing

El Phishing es uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta. Este malware utiliza técnicas basadas en ingeniería social, haciéndose pasar por una entidad de confianza en una aparente comunicación oficial electrónica: correo electrónico, mensajería instantánea, redes sociales o incluso utilizando también llamadas telefónicas.

Virus informático

Un virus informático es un “programa introducido subrepticiamente en la memoria de una computadora que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada”.

Spyware

Es un programa espía que recopila la información sobre los hábitos y el historial de información, así como información personal, de un ordenador para después transmitirla a una entidad externa sin que el usuario tenga conocimiento de este acto.

Troyano

A este tipo de malware también lo conocemos como “caballo de Troya”, actúa camuflándose como software legítimo para intentar acceder a los sistemas de los usuarios. Su manera de actuar, normalmente consiste en que algún tipo de ingeniería social engaña a los usuarios para que carguen y ejecuten los troyanos en sus sistemas operativos. Una vez que los troyanos han sido ejecutados e instalados en el sistema, permiten a los cibercriminales espiar al usuario, robar sus datos confidenciales y obtener acceso a través de una puerta trasera (backdoor) a su sistema, esto permite la administración remota de dicho sistema a un usuario no autorizado.

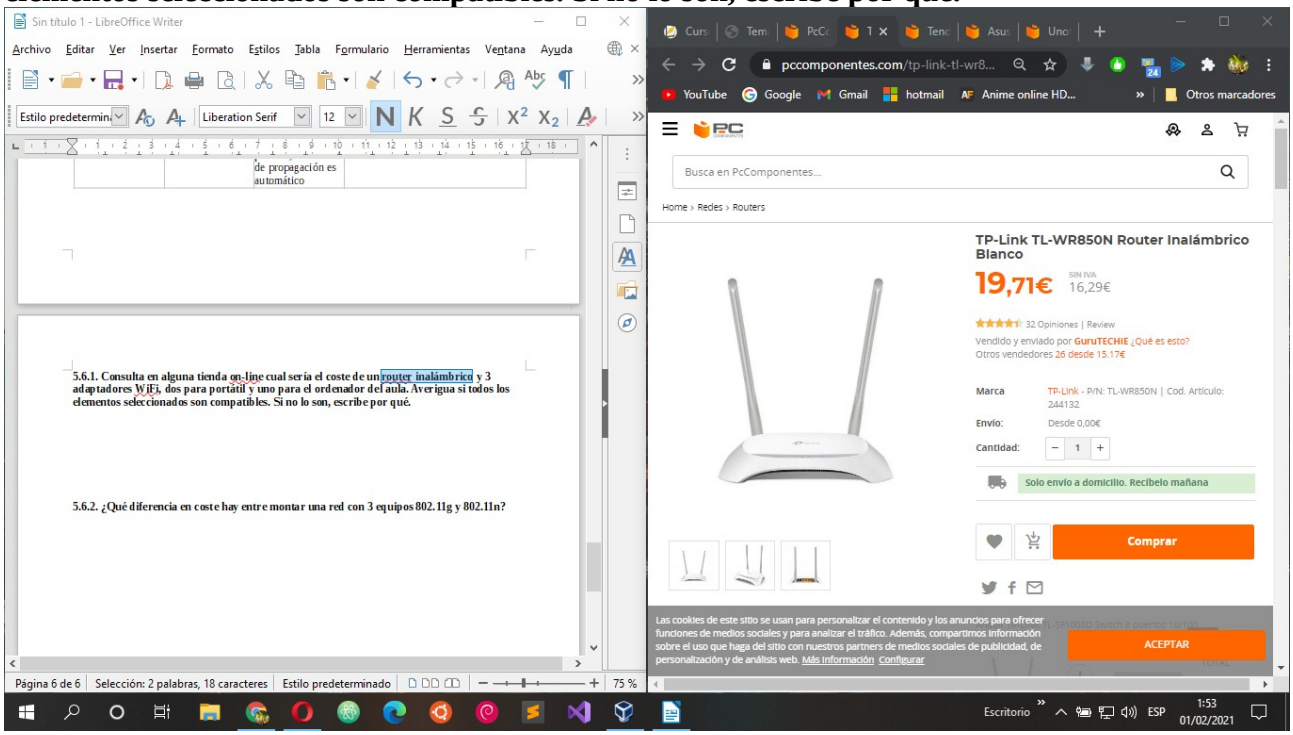
Gusano

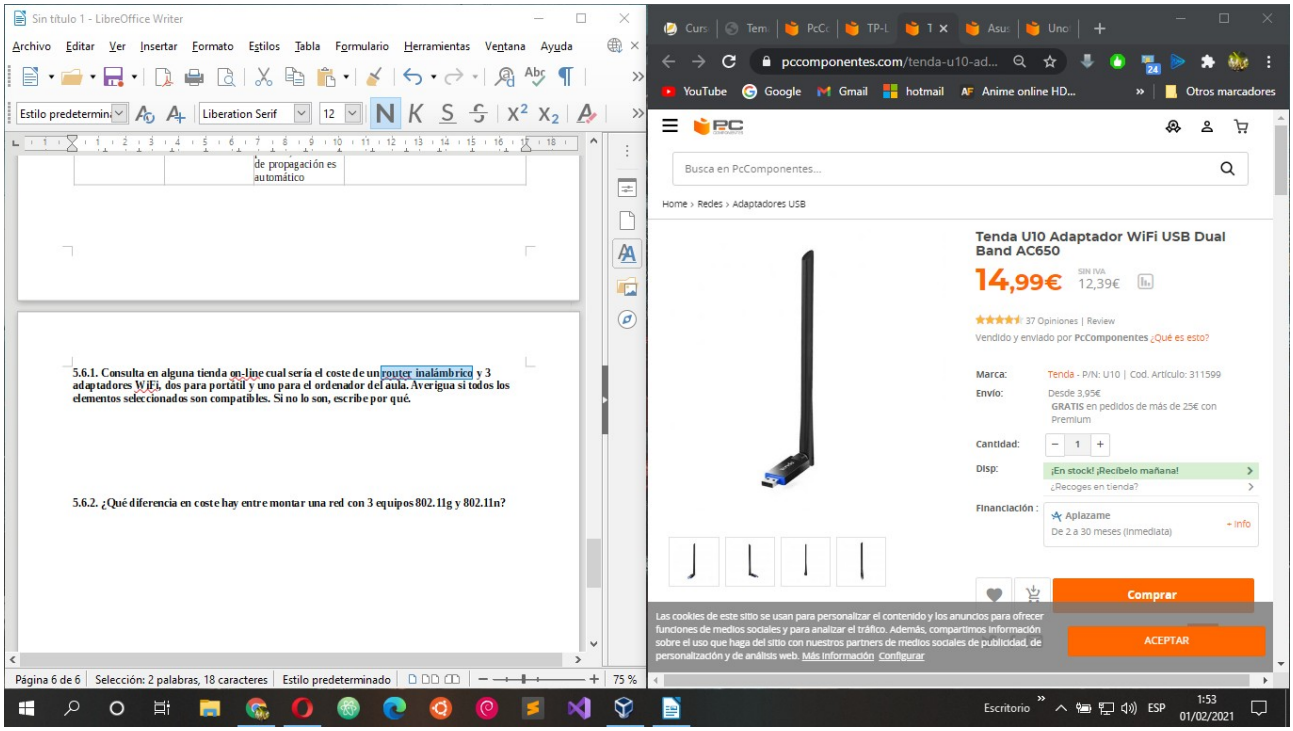
Un gusano informático es un malware que se multiplica para propagarse a otros sistemas mediante una red informática. Para acceder a un sistema utiliza las brechas de seguridad de éste. Los gusanos casi siempre realizan una acción perjudicial en la red, por mínima que sea, como por ejemplo consumir ancho de banda, mientras que los virus casi siempre corrompen o modifican archivos en una computadora de destino.

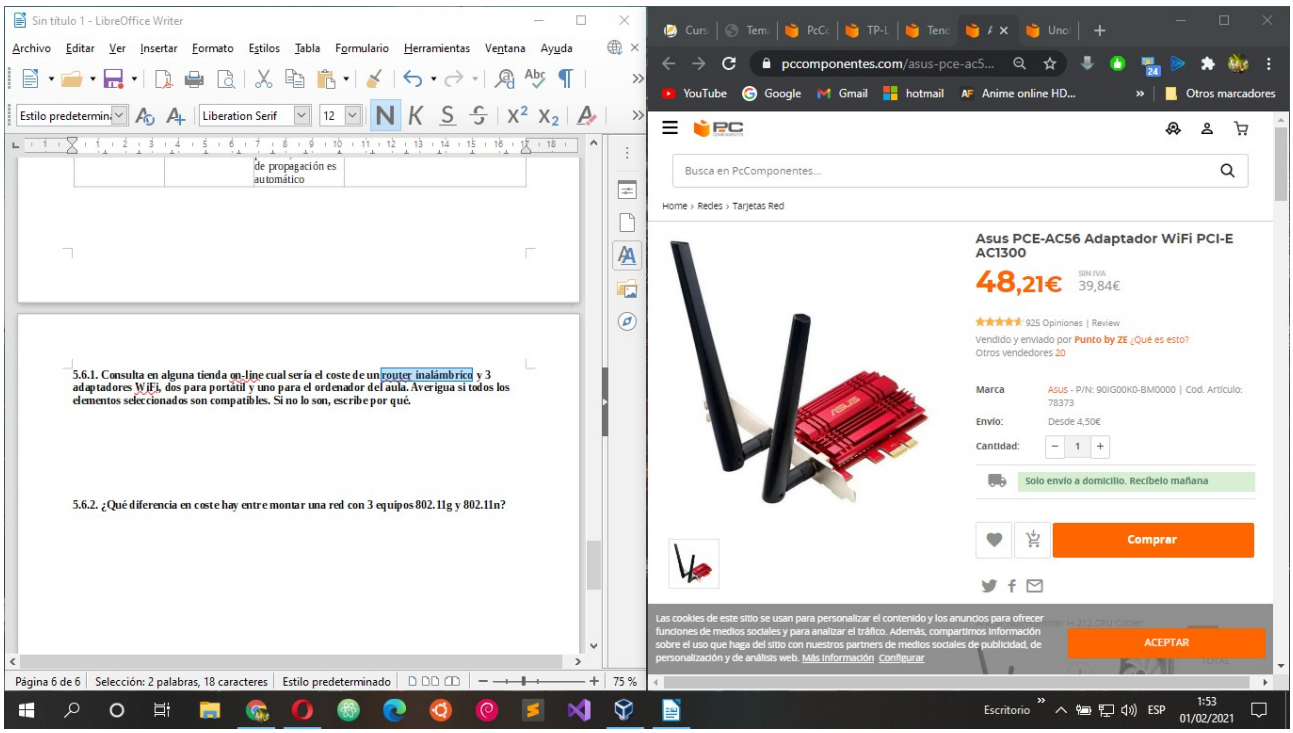
| **Nombre** | **Archivo** | **método** | **mecanismo** |
|---|---|---|---|
| Spyware | archivos que no deberían existir | las claves de registro del sistema utilizadas y modificadas por el ‘malware’ cada vez que el ordenador se pone en marcha | tienes que comprobar los servicios para asegurarte que está todo correctamente. Un truco para que el análisis no se te haga eterno es activar la casilla que oculta todos los servicios de Microsoft e ir mirando los de terceras empresas. Presta especial atención a lo que provenga de 'Desconocido' y a aquellos |

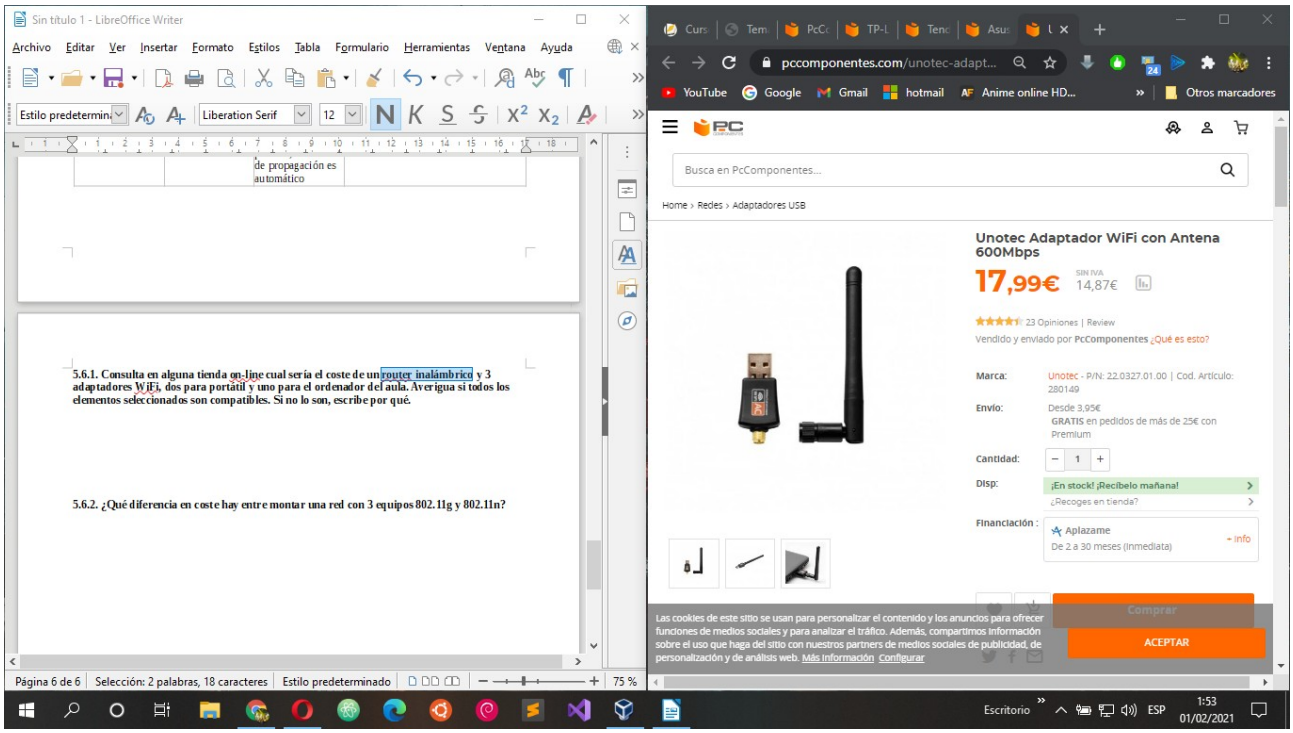
| | | | |
|---|---|---|---|
| | | | nombres que no te suenen de nada que hayas instalado manualmente. Poniendo el nombre del servicio en Google (por ejemplo: ASGT service), las páginas webs te indicarán qué es exactamente. De ser algo malicioso, basta con que desmarques su casilla para que deje de funcionar |
| Virus informático | Archivo.bat | Pragramcion de sistema bat | el antivirus que tengas instalado te servirá de barrera contra el ‘malware’, pero no siempre es así. |
| Troyano | programas | Mensajes raros y pop-ups<br>=<br>Ordenador muy lento<br>=<br>Conexión a Internet interrumpida<br>=<br>Ventanas maliciosas<br>=<br>Ficheros perdidos<br>=<br>Desactiva la protección contra virus y el cortafuegos | Para eliminarlo del sistema, el nuevo software debe ser desinstalado. Dado que algunos troyanos no aparecen en la lista de aplicaciones, la base de datos del registro del ordenador también debe ser revisada para detectar software sospechoso. Si hay un programa con un nombre inusual, la entrada para esta aplicación debe ser eliminada. Es importante señalar que el troyano tendrá instalado otro software y debe ser eliminado en consecuencia. |
| Phishing | Phish Phry | El ataque se realiza mediante comunicaciones electrónicas | Avast Free Antivirus hace mucho más que protegerlo de los virus. Nuestra detección de amenazas inteligente puede detectar y notificar los enlaces maliciosos y los archivos adjuntos infectados que a los phishers tanto les gusta emplear contra usted. Si los phishers no logran engañarlo, no podrán robarle sus datos, y estamos centrados en evitar que lo consigan. |
| Gusano | LOVE-LETTER-FOR-YOU.TXT.vbs | los gusanos tiene la capacidad a propagarse sin la ayuda de una persona, el método de propagación es automático | Instala, actualiza y ejecuta un antivirus gratuito |

**5.6.1. Consulta en alguna tienda on-line cual sería el coste de un router inalámbrico y 3 adaptadores WiFi, dos para portátil y uno para el ordenador del aula. Averigua si todos los elementos seleccionados son compatibles. Si no lo son, escribe por qué.**






Si que son compatibles.

**5.6.2. ¿Qué diferencia en coste hay entre montar una red con 3 equipos 802.11g y 802.11n?**

802.11n puede costar alrededor de 21€
802.11g puede costar alrededor de 100€