

Como limpiar un virus. Como desinfectar la computadora

En la era de la informática, si bien pareciera que todo lo que nos proveen las herramientas de este campo son beneficios para hacernos más fácil la vida, lo cierto es que existen en torno a ello serios inconvenientes, que pueden perjudicar nuestros equipos e incluso generar perjuicios graves en nuestra vida cotidiana, por supuesto que estamos hablando de virus.

Sin lugar a dudas, los virus informáticos son el origen de estos problemas, que en ocasiones puede convertirse en una simple molestia cada vez que utilizamos nuestras computadoras y dispositivos informáticos, pero que en algunos casos pueden transformarse en una verdadera amenaza, como sucede por ejemplo con los virus relacionados a las actividades phishing.



En definitiva, el poder disfrutar de internet y de las computadoras también conlleva sus riesgos, por lo que si deseamos seguir pudiendo disfrutar de todas las ventajas que nos brinda la tecnología, es sumamente importante que estemos alertas para poder proteger nuestra información personal, utilizando para ello programas antivirus y de detección de malware.

Eliminar el virus Recycler

No obstante, en ocasiones más allá de que implementemos un método de seguridad informática confiable con un antivirus potente y fiable, puede llegar a suceder que nuestra computadora y nuestros dispositivos sean atacados por algún tipo de malware, como es el caso del conocido virus “Recycler”, al que seguramente en algún momento de nuestra vida deberemos enfrentar. En este caso, lo importante es poder actuar con rapidez para eliminar el virus.



A partir de este punto te contamos cuáles son los alcances y el método de propagación que posee el virus Recycler, y te brindamos las herramientas adecuadas para que puedas eliminar el virus Recycler sin mayores inconvenientes.

Qué es el virus Recycler

Como mencionamos, uno de los virus más frecuentes y comunes que en algún momento de nuestra vida deberemos enfrentar es el llamado virus Recycler, el cual por lo general se transmite a través de dispositivos extraíbles, tales como pendrives, tarjetas de memoria, discos ópticos u otros dispositivos portátiles.



El procedimiento por el cual el virus Recycler logra infectar nuestra computadora es realmente sencillo, ya que consiste en que cuando conectamos por ejemplo un pendrive infectado a nuestra PC, el virus entra en la misma a través de la función de ejecución automática, que en el sistema operativo Windows se inicializa a través del archivo autorun.inf, es decir que se aprovecha de la función “Autorun” que poseen las unidades USB.

A partir de que la computadora se infecta, el virus comienza a crear archivos y carpetas ocultos por lotes, los cuales son creados en cada una de las unidades en el sistema. Una de las carpetas que crea el virus Recycler precisamente lleva por nombre “Recycler” en la raíz de cada unidad USB y del disco duro, y se trata de una carpeta de sistema, la cual utiliza el virus para mantener los archivos borrados.

Cabe destacar que la carpeta Recycler por lo general se mantiene oculta para nosotros, por lo que para detectarla debemos utilizar la opción de poder ver archivos y carpetas ocultos, de lo contrario se esconde de nuestra vista.



De todas formas, si en algún momento encontramos en nuestra computadora algún archivo ejecutable, como por ejemplo RECYCLER.exe, tenemos que tener en cuenta que es el principal indicio de que nuestra PC y nuestras unidades USB han sido infectadas con el virus Recycler, por lo que debemos llevar adelante lo más pronto posible el método para eliminar el virus Recycler.

Daños del Virus Recycler

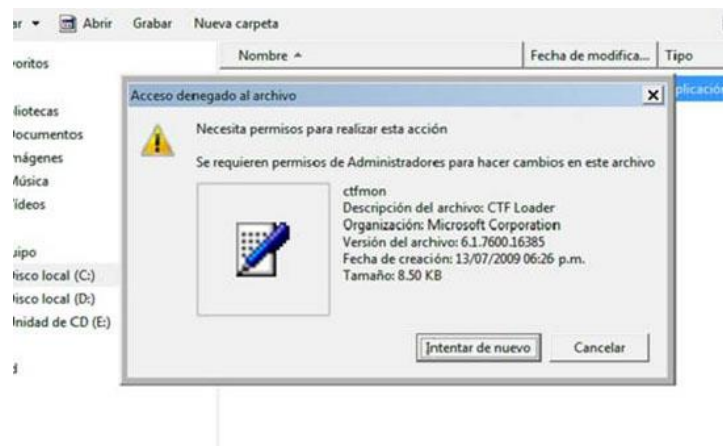
Como ya dijimos, cuando una computadora es infectada por el virus Recycler, este malware creará archivos ocultos, con lo cual el virus pueden reescribir los archivos de registro. Además, una de las más importantes amenazas que presenta el virus Recycler consiste en que puede conectarse a internet y desde allí descargar en nuestra PC sin permiso programas maliciosos que son utilizados por hackers para robar nuestra información personal.

De esta forma los ciberdelincuentes pueden acceder a nuestros nombres de usuarios y contraseñas, datos bancarios y de tarjetas de crédito, y así robarnos dinero o bien robarnos nuestra identidad para cometer todo tipo de actividades ilegales o criminales sin que quizás lo sepamos.



Una de las características más destacables del virus Recycler consiste en que debido a su conformación suele ser muy difícil de detectar antes de que produzca daños importantes, ya que si bien existen programas antivirus que son capaces de identificar el virus, lo cierto es que por lo general los programas antivirus no pueden eliminar el virus del sistema.

Por ello se considera que el virus Recycler es un tipo de malware muy difícil de eliminar, ya que tenemos en cuenta que una vez que entró en contacto con nuestra computadora y unidades USB logra afectar a un volumen muy importante de archivos que están dentro del sistema, y además de ello también infecta el registro de los archivos.

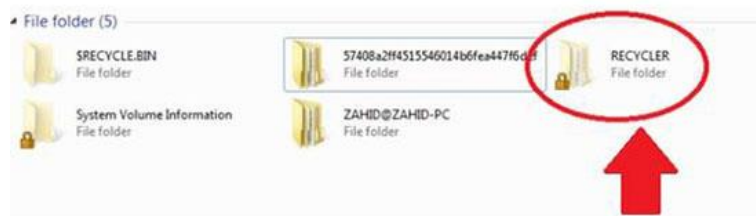


No obstante, es posible eliminar el virus Recycler de forma manual, pero debemos tener en cuenta que para ello es necesario realizar una serie de cambios en el registro, por lo cual se recomienda antes de iniciar la eliminación del virus Recycler llevar a cabo una copia de seguridad de todo el contenido de nuestra PC antes de iniciar el procedimiento, como así también una copia de seguridad de nuestro sistema actual.

Eliminar el virus Recycler

Cuando notemos que el programa antivirus que tenemos instalado en nuestra computadora, más allá de encontrarse actualizado, no puede eliminar el virus Recycler, entonces debemos

proceder a la eliminación manual del mismo, para lo cual debemos llevar a cabo los siguientes pasos.



Paso 1

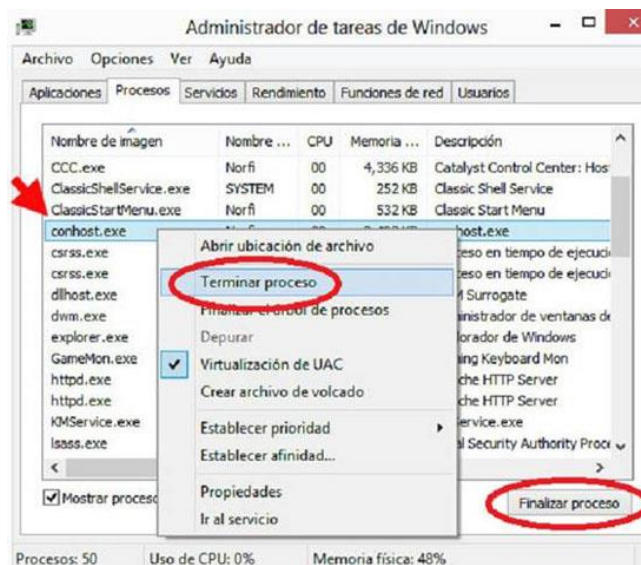
Lo primero que debemos hacer es reiniciar nuestra PC y al hacerlo debemos entrar en el Modo Seguro de Windows, para lo cual en la primera pantalla de inicio debemos pulsar la tecla F8, luego de lo cual podremos seleccionar ingresar en el Modo Seguro.

Paso 2

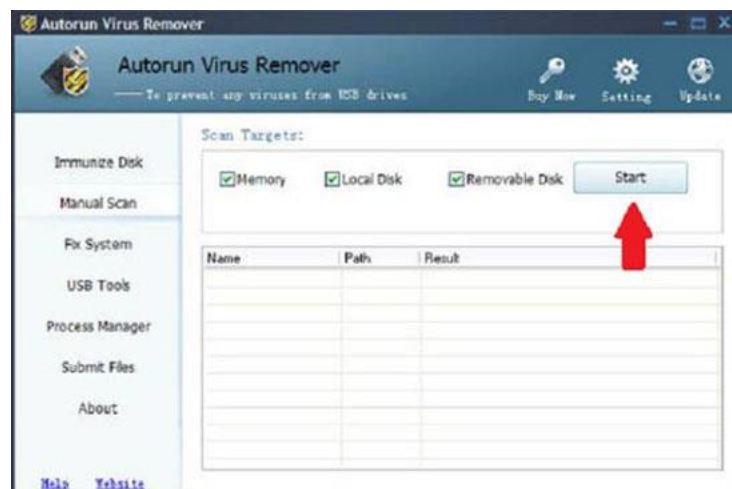
Una vez en el escritorio de la PC, siempre en Modo Seguro, ejecutamos el Administrador de Tareas, lo cual podemos hacer pulsando las teclas Ctrl + Alt + Supr, y eligiendo la opción “Administrador de Tareas”.

Paso 3

En la pestaña de “Procesos” del Administrador de Tareas debemos buscar el proceso “RECYCLER.exe” y finalizar este proceso.



Paso 4



Paso 1

Ejecutamos Autorun Virus Remove y pulsamos el botón “Start” para que inicie el escaneo del sistema.

Paso 2

El programa nos informará si existe el virus Recycler y nos preguntará si deseamos eliminarlo, lo cual deberemos aceptar.

Cabe destacar que puede llegar a suceder que el virus Recycler bloquee a Autorun Virus Remove, por lo cual se recomienda poder a funcionar esta herramienta luego de ingresar al sistema en Modo Seguro.



Además de poder eliminar el virus Recycler de nuestra PC, con Autorun Virus Remove también podemos eliminar el virus Recycler de nuestras unidades USB infectadas.

Como eliminar virus con Avast Antivirus

Seguramente muchos de nuestros lectores se sorprenderán con la siguiente declaración, pero ni siquiera el mejor antivirus del mercado es capaz de mantener nuestra computadora totalmente libre de peligros, sean en forma de virus como de malware y otros tipos de amenazas. Claro está que no debemos alarmarnos ni entrar en pánico, ya que para compensar los problemas, los desarrolladores de este tipo de software recomiendan analizar el sistema cada 15 días.

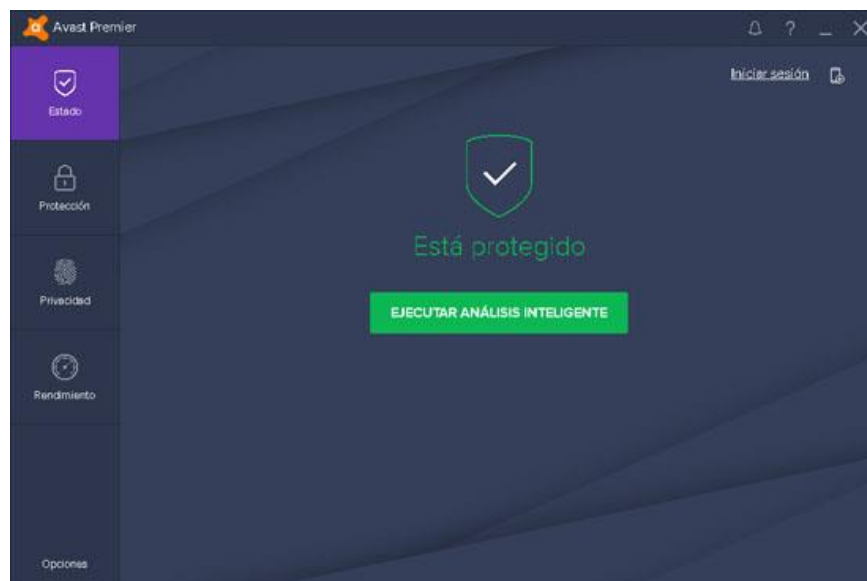
Una recomendación un poco extraña y que no soluciona nada, ya que una vez que un virus ha entrado en nuestro sistema se podría decir que el antivirus ha fallado, y por lo tanto nuestros datos y documentos han sido vulnerados.

Sin embargo, si el virus que el software antivirus no detuvo es solamente una amenaza de esas que sólo se limitan a cambiar algunos parámetros de nuestra computadora como la página de inicio de nuestro navegador favorito, todavía podemos quitarlo y prevenir que sea la puerta de entrada a otras cosas. En el caso de que seamos usuarios de Avast! Antivirus, y sospechemos que este ha dejado pasar alguna amenaza, en este artículo encontraremos los

pasos necesarios para limpiarla y dejar todo en las mismas condiciones que antes, en forma sencilla y rápida.



Avast! es uno de los mejores antivirus del mercado, eso se puede comprobar fácilmente observando la cantidad de copias que se descargan desde los sitios que las albergan mes a mes. Esto no es por capricho o moda, es simplemente debido a que es un antivirus eficaz y que ofrece muchas y muy importantes herramientas para prevenir y eliminar virus de nuestra computadora.



Eliminar un virus de nuestra computadora utilizando Avast! Antivirus

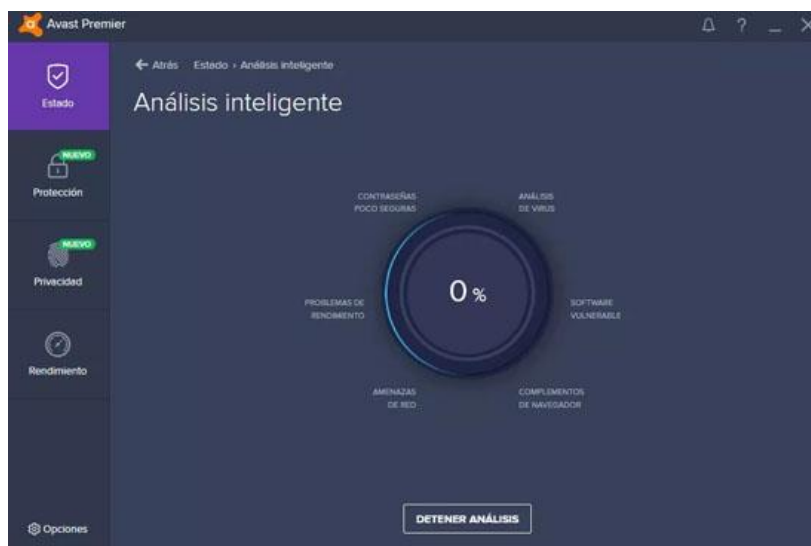
Cabe destacar que este procedimiento es válido para ambas versiones del producto, la gratuita y la paga.

Paso 1

Lo primero que tenemos que hacer para eliminar un virus es obviamente ejecutar Avast!, lo que podemos hacer pulsando sobre su icono en la bandeja de entrada ubicada junto al reloj del sistema.

Paso 2

A continuación, pulsamos sobre el mismo y en la ventana que se despliega seleccionamos la opción “Análisis” y luego “Análisis completo”.



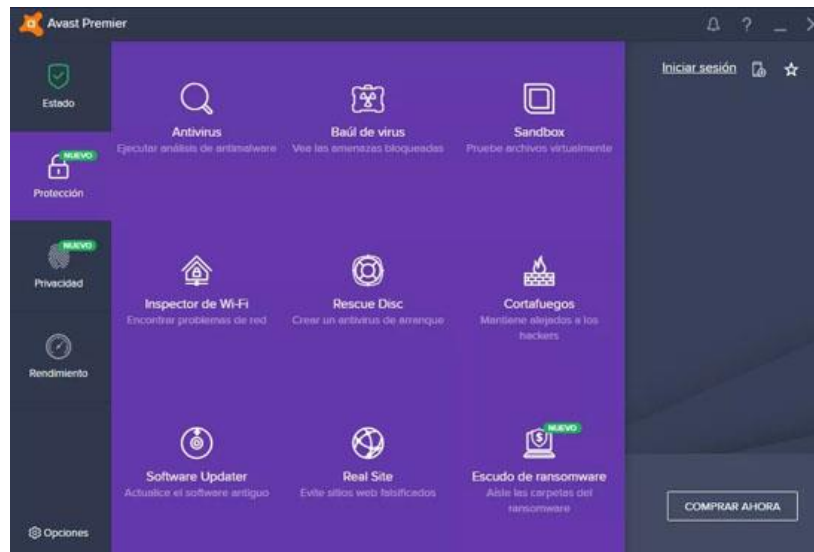
Paso 3

Luego, nos toca esperar a que el sistema termine de realizar la tarea, es decir que la barra llegue hasta el 100%.

Paso 4

En el caso de que la cantidad mostrada en “Archivos Infectados” sea igual a cero, quiere decir que no tenemos virus. Ahora si esta cantidad supera este número, significa que nuestra PC está infectada con virus, y tendremos que pulsar sobre el botón “Mostrar resultados” ubicado a la derecha para obtener más detalles e instrucciones para su eliminación.

En este punto, encontraremos 4 opciones, de las cuales deberemos seleccionar una. Sin embargo, lo más recomendable es dejar que Avast! Antivirus realice la acción predeterminada, es decir, “Mover al baúl”.



Reparar: Este ítem es para intentar reparar el archivo infectado. Sin embargo casi nunca lo logra.

Mover al baúl: Aceptando esta acción, Avast! moverá los archivos infectados a una especie de baúl diseñado para contenerlos. Esto es muy útil en el caso de que los archivos que hayan sido infectados con virus sean importantes y los queramos almacenar sin problemas para un mejor análisis por parte de un especialista.



Eliminar: esta opción eliminará de forma segura los archivos infectados con virus. No debe ser usada si queremos preservar los mismos para un análisis posterior.

No hacer nada: Como su nombre lo indica, no realiza ninguna acción, algo muy peligroso tratándose de archivos infectados con virus.

Herramientas e instrucciones para eliminar los virus de tu computadora

Debido a que Windows es el sistema operativo más popular del mundo, [los desarrolladores de malware obviamente tiene una especial predilección por crear malware y virus](#) para esta plataforma, y lamentablemente como resultado de estas prácticas existen miles de programas malintencionados y virus acechándonos y listos para espiarnos, destruir nuestra información o simplemente robarnos.

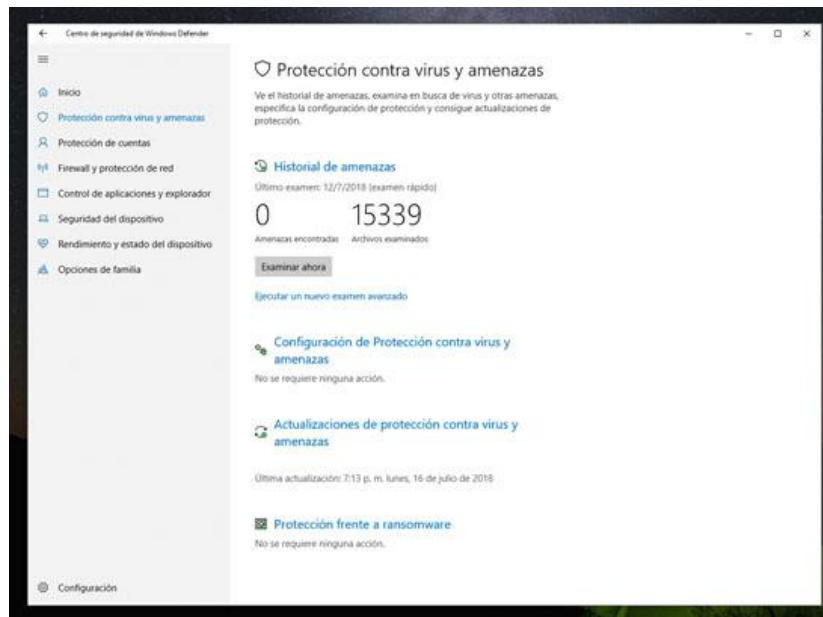
A partir de este punto conoceremos los procedimientos y las herramientas necesarias como para comenzar a comprender su funcionamiento y aprender a cuidarnos y deshacernos de todo tipo de virus.

Contrariamente a los que los muchos creen, Windows es un sistema bastante seguro, quienes lo hacen inseguro son sus propios usuarios por ignorancia o por descuido. Muchas veces por no tomar los recaudos mínimos necesarios, como la instalación de un buen antivirus para protegernos, podemos terminar con una computadora completamente infectada de virus, sin que el sistema operativo de Microsoft tenga la culpa.



Básicamente, un malware puede tomar cualquier forma: virus, adware, spyware, ransomware, scareware, BOT, Backdoor, exploits, rootkit, dialer, troyanos, gusanos y muchos tipos más, pero en cualquiera de esas formas es potencialmente dañino, y su único objetivo es el de infectarnos.

Generalmente, los medios mediante los cuales se propagan este tipo de programas son a través de archivos adjuntos en mensajes de correo electrónico o por mensajes de mensajería instantánea, pero también cabe la posibilidad, sobre todo si no tenemos un buen antivirus instalado, de infectarnos al navegar por sitios web peligrosos. En este punto debemos tener cuidado, ya que algunos portales, aun teniendo una buena reputación, pueden intentar infectarnos con algún tipo de malware.



Si no tomamos los resguardos necesarios, podremos descargar a nuestra computadora sin saberlo, a con nuestro consentimiento, lo que es peor, elementos que pueden ayudar a instalar un virus en ella. También muy peligrosa es la actitud que tienen muchos usuarios de no comprobar la existencia de virus en unidades de almacenamiento extraíbles como pendrives, tarjetas de memoria o discos externos, confiando en que provienen de una fuente segura como un amigo, pero quizás nuestro amigo no esté al tanto de lo que sucede en su computadora.

Otros casos de los que debemos sospechar son las tarjetas de felicitación, archivos de audio y vídeo o programas piratas, ya que en su interior se puede esconder fácilmente una amenaza para nuestra seguridad.

Principales síntomas de infección por malware

Algunos síntomas característicos que nos pueden indicar que nuestra computadora está en peligro son:

El cambio de la página de inicio o de búsqueda por defecto en nuestro navegador favorito

Aparición de barras de herramientas en el navegador que no hemos instalado

Una cantidad excesiva de ventanas emergentes durante la navegación

Equipo lento

Excesivo uso de memoria o de la CPU

Notificaciones extrañas en la bandeja del sistema

Transferencias a Internet o actividad de transferencia de datos inusuales

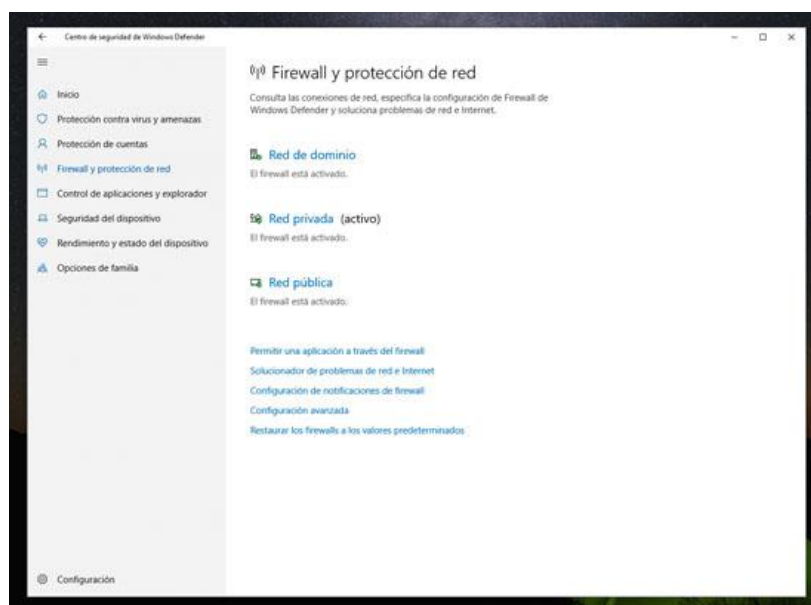
Software de seguridad o cortafuegos desactivado

Funciones de Windows deshabilitadas.

Programas nuevos que no hemos instalado

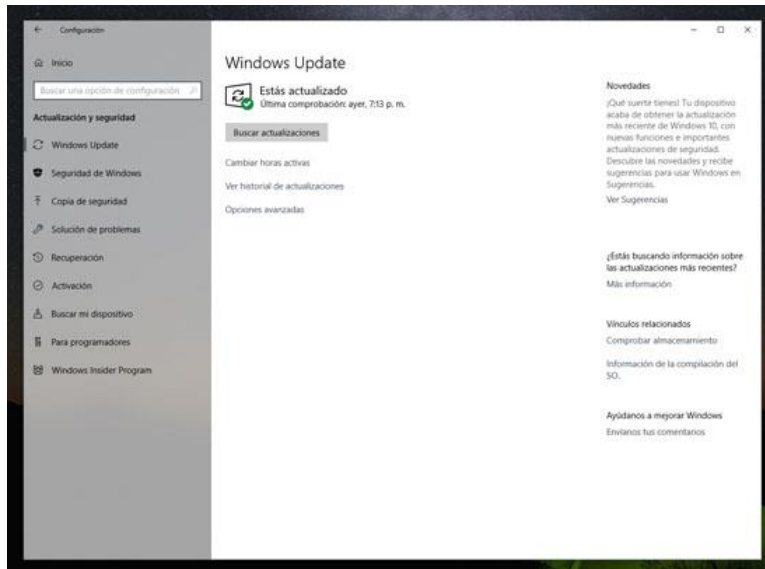
Manual del principiante para la eliminación de malware

A partir de Windows Vista, Microsoft introdujo muchas opciones de seguridad en el sistema operativo, las que han sido mejoradas en las versiones 7 y 8 de Windows. Pero a pesar de ello, todavía podemos resultar infectados con algún tipo de malware, pero afortunadamente hay una gran cantidad de soluciones y herramientas disponibles para estos casos.



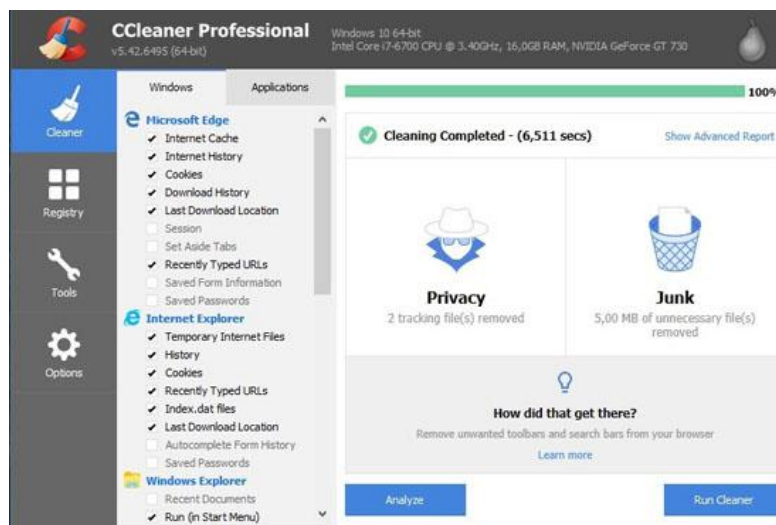
Pero antes de empezar acción alguna, lo mejor es salvaguardar nuestros datos realizando copias de seguridad de los mismos para evitar cualquier problema que pudiera surgir de estos procedimientos.

Otra cosa que tenemos que comprobar que nuestro Windows se encuentre al día con todas las actualizaciones de seguridad instaladas.



1. Limpieza de la basura

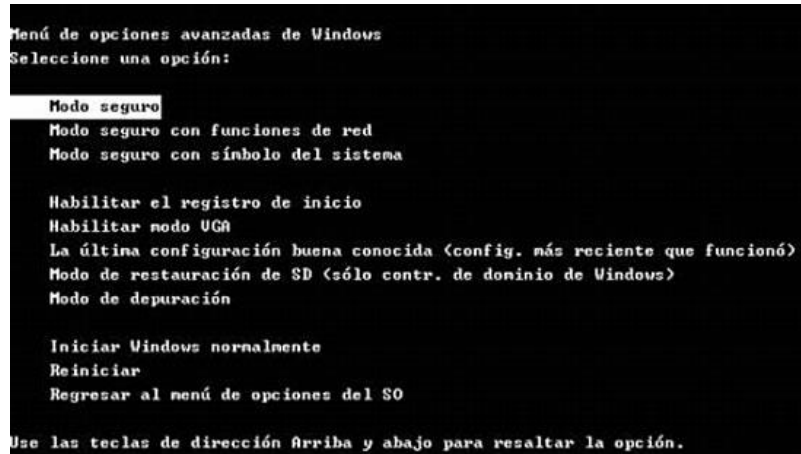
Para sanear y eliminar cualquier tipo de archivos temporales y restos de aplicaciones, nada mejor que CCleaner, una herramienta gratuita que es capaz de realizar este trabajo con escasa participación nuestra. CCleaner limpiará nuestra PC de su basura, incluyendo los mencionados archivos temporales, cookies, cookies de Flash y caché de Java, además de cualquier otra cosa que ocupe espacio inútilmente en la PC. Otro beneficio que se obtiene de la utilización de CCleaner en este punto es que reducirá el tiempo de exploración para otras aplicaciones que necesitaremos para llevar a cabo la tarea.



2. Actualización y utilización de un antivirus

Una de las principales herramientas a usar en la búsqueda y eliminación de malware es el antivirus, y por lo tanto debemos mantenerlo actualizado. En este caso, uno de los mejores antivirus disponibles es Avast!

Una vez actualizado, ejecutamos un análisis completo del equipo, en lo posible en el modo seguro de Windows, ya que este es una de las maneras más sencillas para el antivirus para detectar cualquier amenaza. Para entrar en el modo seguro de Windows, mientras la computadora se inicia, mantenemos presionada la tecla F8.



En el caso de que el antivirus encuentre alguna amenaza, comenzaremos con la tarea de removerla. Si el antivirus no puede eliminar el virus del archivo infectado, utilizaremos algún programa gratuito para eliminar el archivo infectado en el próximo reinicio de la PC. Una vez que Windows se inicie, volveremos a usar CCleaner para eliminar las claves en el registro del sistema y cualquier resto que haya quedado.

Escaneo de archivos dudosos con antivirus en línea

Si nuestro antivirus no detecta un archivo como un virus, pero tenemos sospechas de que puede serlo, lo mejor es intentar despejarse la duda utilizando los servicios de algún antivirus en línea. Algunos de los mejores servicios de este tipo son Panda Activescan, ESET o VirusTotal.

En líneas generales, los procedimientos que acabamos de realizar tienen una efectividad del 100 por ciento, lo único que tenemos que hacer es seguir al pie de la letra las instrucciones para lograr el éxito esperado.