Una Guía Para Limpiar Su PC Infectado Y Prevenir Futuras Infecciones

Una Guía Para Limpiar Su PC Infectado Y Prevenir Futuras Infecciones

La amenaza puede provenir de su navegador de Internet, los pop-ups, e-mails, el software que utiliza, etc. Estos virus existen con la finalidad de robar datos, pero existe un impacto negativo para su PC, con el tiempo éste no podrá utilizarse.



Si estás cansado de tratar con ellos, y quieres encontrar un procedimiento estándar que puede seguir para erradicar adecuadamente estos virus, esta es la guía para que necesitas. Aquí hay 6 pasos para Limpiar Su PC infectada, y evitar infecciones futuras para su PC .

1. Use La Función De Restaurar Sistema De Windows

Este es el método más sencillo para restaurar su PC a un estado optimo antes de infectarse. La restauración del sistema devolverá la configuración del equipo a su estado anterior (basado en un estado) sin ningún cambio en los archivos en su ordenador, siempre y cuando la función **Restaurar sistema** no este desactivada.

Esto es lo que debes hacer:

lestore your computer to	o the state it was in before the se	elected event
low do I choose a restore po	nt?	
urrent time zone: GMT+5:30		
Date and Time	Description	Туре
7/18/2012 10:28:25 PM	Windows Update	Critical Update
Show more restore points		Scan for affected programs

- 1. Abra el menú Inicio> Haga clic en Todos los programas.
- 2. A continuación, vaya a Accesorios> Herramientas del sistema y haga clic en Restaurar sistema.
- 3. Una vez que se abre el programa, haga clic en «Restaurar mi equipo a un estado anterior«.
- Seleccione la fecha en el calendario antes de que se infectó el PC y haga clic en Siguiente.
- 5. Se le presentará con más información sobre la

restauración del sistema, una vez leído haga clic en Siguiente para reiniciar el ordenador.

6. Después de que el proceso de restauración está terminado, el equipo **regresará a su estado normal**.

Nota: Los usuarios de <u>Windows</u> 8 pueden abrir **Restaurar** sistema mediante la función de búsqueda de Metro. Buscar Sistema, a continuación, haga clic en Sistema> Protección del sistema> Restaurar sistema.

¿Tienes tu **PC como nuevo**? Bueno. Ahora es el momento de dar un par de pasos más para asegurarse de que la infección haya desaparecido. Un virus es peligroso tras la ejecución. El hecho de que su PC ya no muestre los síntomas, no significa que el virus ya se ha ido. Todavía puede estar «viviendo» en algún lugar dentro de su PC, esperando la oportunidad de volver a surgir.

2. Deteniendo El Virus

Para **encontrar el virus**, necesita para llevar a cabo una exploración obligatoria. Sin embargo, antes de ejecutar el análisis, es necesario asegurarse de que el virus **no se está ejecutando en segundo plano**. Si es así, puede que no sea capaz de detectarlas, ya que usan algoritmos especiales para no ser detectados.



Aquí es donde se necesita una herramienta que le ayude. <u>RKill</u> es libre de usar y le puede ayudar a evitar que los virus se

ejecuten en segundo plano en cuestión de clics.

Sin embargo, algunos virus pueden impedir que programas como **RKill** se ejecute. En casos como este, intente cambiar el nombre a algo como: iExplore. Al hacer esto, usted podría «**engañar**» al virus para que piense que está ejecutando Internet Explorer en lugar del programa <u>RKill</u>.

3. Eliminado Los Virus

Una vez que se ha detenido el proceso del virus con **RKill**, descargue <u>TDSSKiller</u> y utilicelo para **escanear su PC en busca de malware**. Una vez que el escaneo termine, si hay una amenaza, puede utilizar <u>TDSSKiller</u> para reparar o eliminar los archivos. Una vez que haya terminado, reinicie su PC.



existan. Por ahora el sistema ya debe estar libre de la mayoría de los virus, pero si usted todavía quiere asegurarse de que usted ha limpiado su PC a fondo, echa un vistazo a los próximos pasos.

4. Software Adicional Para Eliminar Virus

Es hora de entrar en detalles. Usted puede utilizar software como <u>AdwCleaner</u> para eliminar <u>adware</u>, **Junkware Removal Tools** para eliminar las barras de herramientas no deseadas, y <u>Malwarebytes</u> si le parece que un poco más de <u>malware</u> todavía reside en su PC. Antes de utilizar cualquiera de las herramientas, no olvide ejecutar primero **RKill**.

	the second	antine Logs Ignole List Settings Mole I c	About alo	
			And a second second second	edi.
Scanner	t af an af a' an an th	and a second		and different second
Eelow is a li	st of malicious softw	are found on your system. Close all unnecessary applicatio	ns to ensure su	accessful threat removal.
_				
Vendor	Category	Item	Other	Action taken
Virus.4on.1346	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.Fellow	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.Jerusal	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.4on.1346	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.ARCV	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
HLLP.Birthday.	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.Guess	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.Fellow	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.Jerusal	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.4on.1346	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.ARCV	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
HLLP.Birthday.	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Virus.Guess	File	c:\\$Recycle.Bin\s-1-5-21-3649715934-24315		No action taken.
Troise Agent	File	c:\Users\Sierra\AppData\Local\Temp\.exe		No action taken.

También, recuerde que debe actualizar la base de datos del software para obtener sus últimos cambios antes de iniciar la exploración. La razón por la que usted necesita

mantener la

actualización de ellos, se debe a que los virus vienen en muchas formas diferentes y se propagan con facilidad en toda la Web. Con una base de datos actualizada, usted tiene una mayor probabilidad de que el software detecte más tipos y versiones de los virus.

5. Proteja Su PC Con Un Firewall

Con 1 a completa limpieza del equipo, es el momento de configurar un <u>servidor</u> de <u>seguridad</u> para mayor protección. Comodo es un de programa servidor de seguridad para

	Summary	6 Firewall	+ Defense+	= □ ×
All systems are active and running.	Firewall Frewal ha	a blocked 0 intrusion(a) so far outbound connection(a) bound connection(a)	83.5% OnlineCmdLineSca 10.4% suchost.exe 6.1% firefox.exe	Safe Mode 🔘
	Defense+	has blocked § intrusion(s) so fa nrecognized file(s) observed oplication(s) currently running in t	Stop At Traffic sr the Sandbox	Safe Mode 📀
				Ja.

Windows que ayuda a **proteger su PC de las amenazas**, supervisar las conexiones y asegura sus conexiones. Descárgalo <u>aquí</u> e instalelo para proteger su PC.

De esta manera, todos los software de instalación o ejecución tendrá que pasar por la inspección de Comodo primero. Si se sospecha que hay algún problema con un software en particular, el programa lo marcara, y le preguntará si desea mantener o eliminar el software.

6 . Activar La Función Restaurar sistema

Lo ultimo que podemos hacer para prevenir futuras pérdidas importantes de datos, es la activación de la **Restauración del Sistema**. Tener un punto de restauración es conveniente porque si su PC se infecta, se puede arreglar con sólo restaurarlo a un estado anterior del sistema.

5		Turn off System Restore -
Turn off System P	Restore	Previous Setting Next Setting
 Not Configured Enabled Disabled 	Comment: Supported on:	At least Windows Server 2008 R2 or Windows 7
Options:		
		Allows you to disable System Restore. This policy setting allows you to turn off System Restore. System Restore enables users, in the event of a problem, to restore their computers to a previous state without losing personal data files. By default, System Restore is turned on for the boot volume. If you enable this policy setting, System Restore is turned off, and the System Restore Wizard cannot be accessed. The option to configure System Restore or create a restore point through System Protection is also disabled. If you disable or do not configure this policy setting, users can perform System Restore and configure System Restore settings through System Protection. Also, see the "Turn off System Restore configuration" policy setting. If the "Turn off System Restore configuration" policy

- Vaya al menú Inicio > Ejecutar. Si no puede encontrar el programa , buscar Ejecutar y haga clic en él.
- 2. En el cuadro **Ejecutar** , escriba **gpedit.msc** y pulse **Enter**
- Se le presentará con la carpeta de directivas de grupo . Haga clic en Configuración del equipo, en la parte de la izquierda.
- 4. Luego vaya a la carpeta Plantilla > Sistema Administrativo.
- 5. Busque la carpeta Restaurar sistema y haga clic en él .
- 6. Una vez dentro , ve a la parte derecha de la ventana Carpeta de directiva de grupo y haga doble clic en Desactivar Restaurar sistema.
- 7. Elija Desactivar y, a continuación , haga clic en Aceptar.
- 8. Volver a la carpeta **Restaurar sistema** y haga doble clic en **Desactivar Configuración**.
- 9. Elija No configurado. A continuación, pulse Aceptar.
- 10. Una vez hecho esto , cerca de todo y reinicie el equipo.

Conclusiones

Si desafortunadamente los pasos anteriores no han sido de gran ayuda, puedes encontrar una posible solución en <u>San Google</u>. Se preciso en las palabras que describir tu problema, ademas añade la palabra «**resuelto**«, con esto nos aseguramos de encontrar una posible solución.

Asimismo, recuerda que en la mayoría de los casos no hay una manera segura de eliminar un virus. Incluso los programas antivirus deben actualizarse regularmente para hacer su trabajo correctamente. Por otra parte , sólo podemos recurrir a los procedimientos estándar al igual que lo que se vio en esta guía para deshacerse de aquellas amenazas.

¿Que solución implementas en estos casos?