# Una Guía Para Limpiar Su PC Infectado Y Prevenir Futuras Infecciones

## Una Guía Para Limpiar Su PC Infectado Y Prevenir Futuras Infecciones

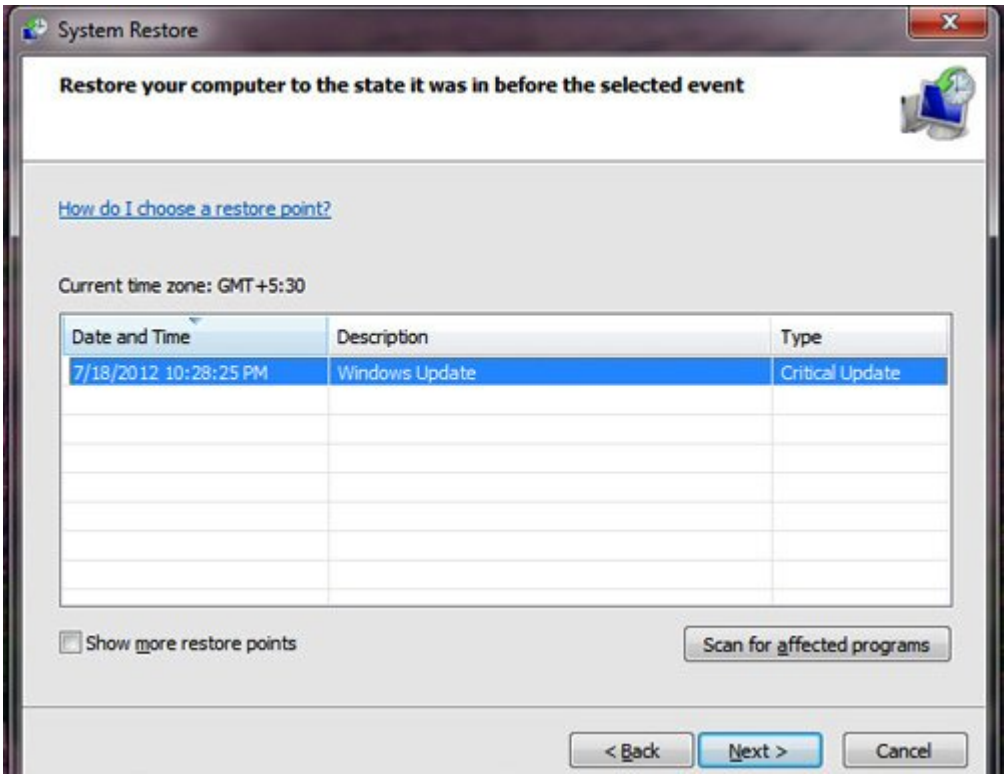
La amenaza puede provenir de su navegador de Internet, los pop-ups, e-mails, el software que utiliza, etc. Estos virus existen con la finalidad de robar datos, pero existe un impacto negativo para su PC, con el tiempo éste no podrá utilizarse.


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:




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**«.
4. 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.

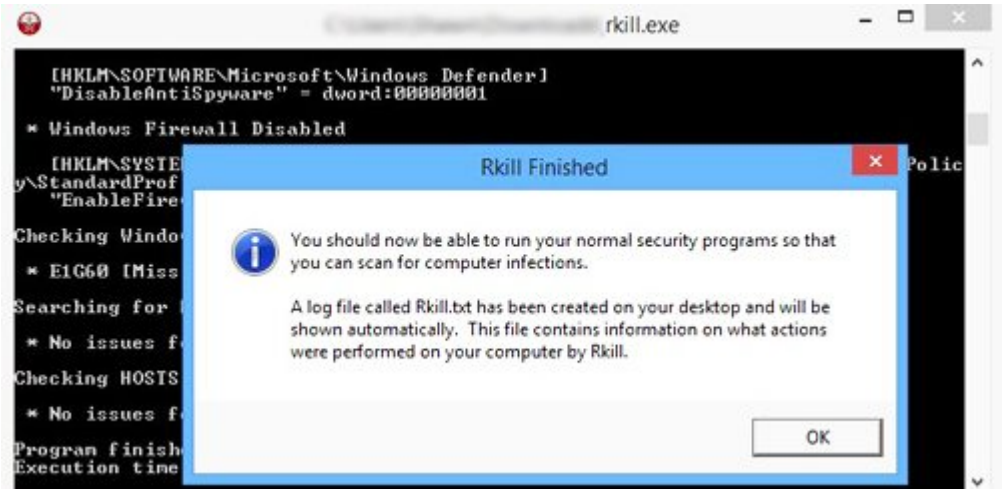
6. Después de que el proceso de restauración está terminado, el equipo **regresará a su estado normal**.

Nota: Los usuarios de **Windows 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.

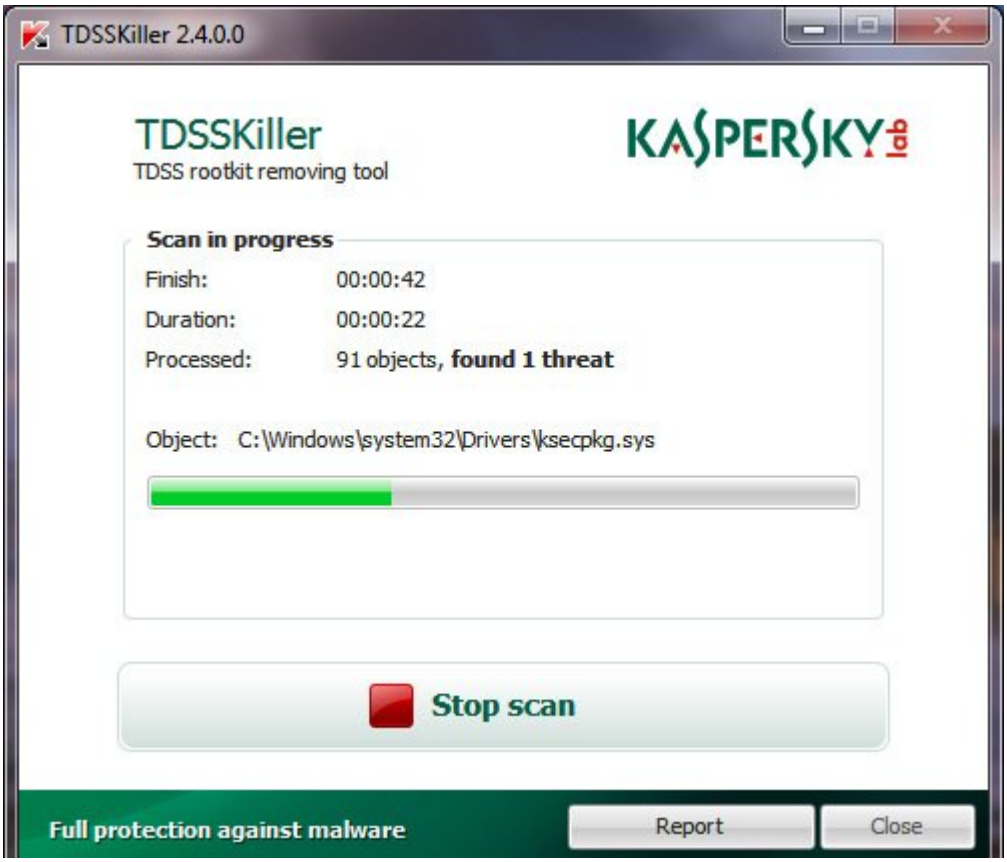



Aquí es donde se necesita una herramienta que le ayude. RKill es libre de usar y le puede ayudar a evitar que los virus se ejecuten en segundo plano en cuestión de clics.

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 RKill.

# 3. Eliminado Los Virus

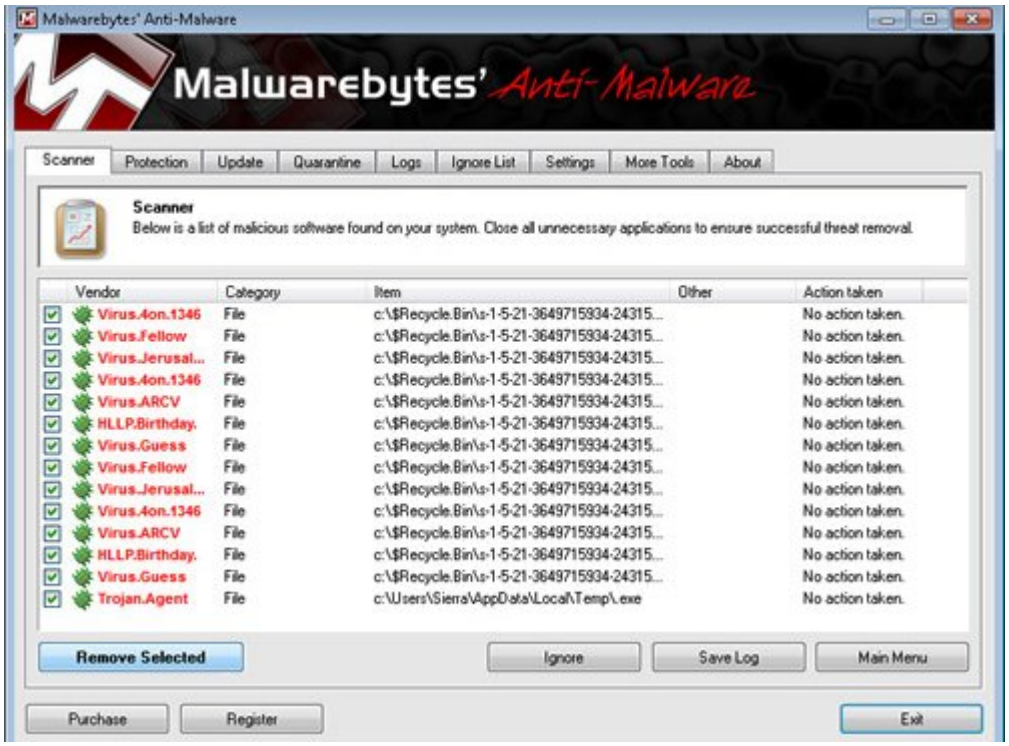
Una vez que se ha detenido el proceso del virus con **RKill**, descargue TDSSKiller y utilicelo para **escanear su PC en busca de malware**. Una vez que el escaneo termine, si hay una amenaza, puede utilizar TDSSKiller para reparar o eliminar los archivos. Una vez que haya terminado, reinicie su PC.




Una vez reiniciado, vuelva a ejecutar RKill. A continuación, descargue el Dr. Web CureIt! y ejecute el escáner para buscar programas maliciosos, troyanos y spyware que todavia 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 AdwCleaner para eliminar adware, **Junkware Removal Tools** para eliminar las barras de herramientas no deseadas, y Malwarebytes si le parece que un poco más de malware todavía reside en su PC. Antes de utilizar cualquiera de las herramientas, no olvide ejecutar primero **RKill**.




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.

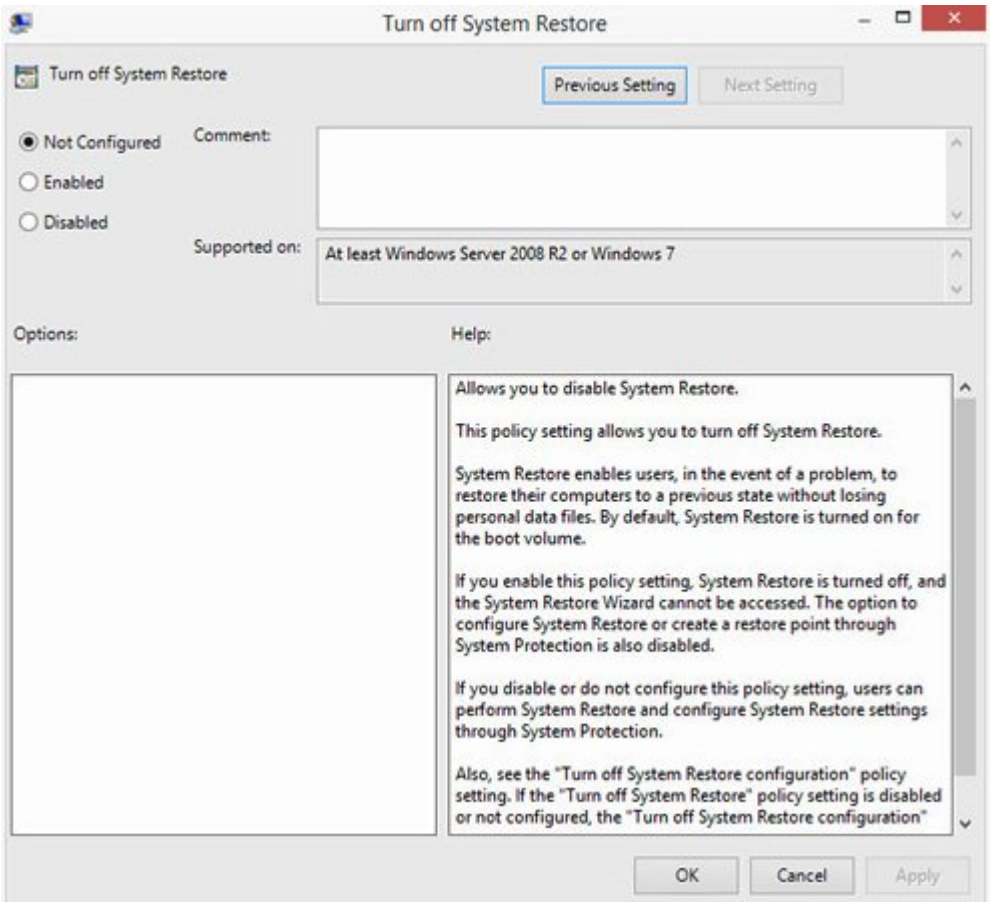
# 5. Proteja Su PC Con Un Firewall


Con la completa limpieza del equipo, es el momento de configurar un servidor de seguridad para mayor protección. Comodo es un programa de **servidor de seguridad para Windows** que ayuda a **proteger su PC de las amenazas**, supervisar las conexiones y asegura sus conexiones. Descárgalo aquí 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.




1. 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** .
3. 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 San Google. 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?