Universidad Autónoma de Chiriquí

Facultada de Economía

Licenciatura en Gestión de Tecnología de Información

Asignatura: Seguridad Informática **Código: PROG 431**

Código de Asignatura: 23674 **Fecha: 17-octubre-2024**

Profesor: Andrés Miranda C.

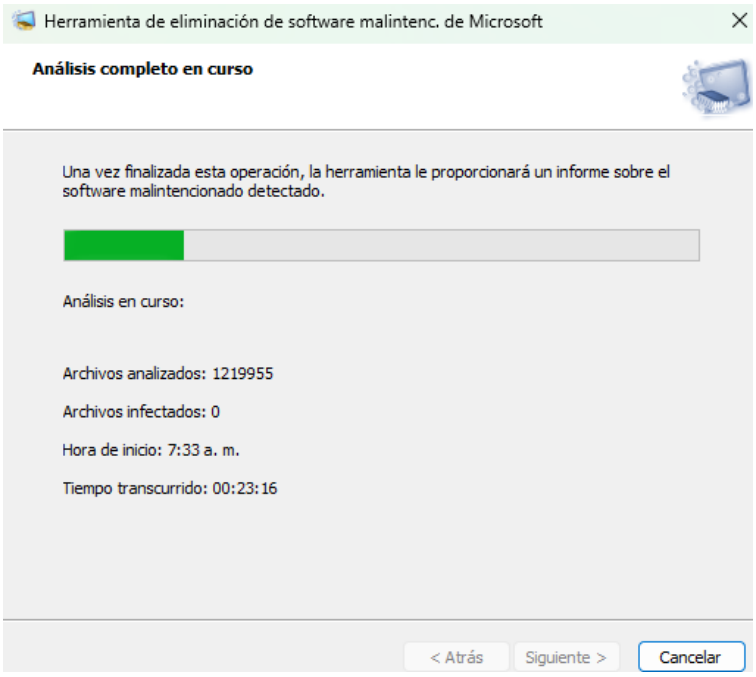
Laboratorio No. 1

Fecha de entrega y sustentación: 17- octubre-2024 **Valor Total: 100 pts.**

Herramientas:

MRT: (Malicious Software Removal Tool – MSRT) – Herramienta de eliminación de Software Malintencionado: La herramienta gratuita de Microsoft que elimina el malware y protege nuestro sistema Windows.

MRT, conocida como Microsoft Malicious Software Removal Tool, es una herramienta gratuita proporcionada por Microsoft a los usuarios de Windows. Su objetivo principal es eliminar el software malintencionado que pueda estar presente en el sistema operativo. Aunque ha estado disponible desde 2005, recientemente ha ganado popularidad entre los usuarios. Al ser gratuita, muchos creen que brinda una protección adecuada sin la necesidad de invertir en una solución antivirus, pero es importante analizar sus ventajas y desventajas para evaluar su eficacia.

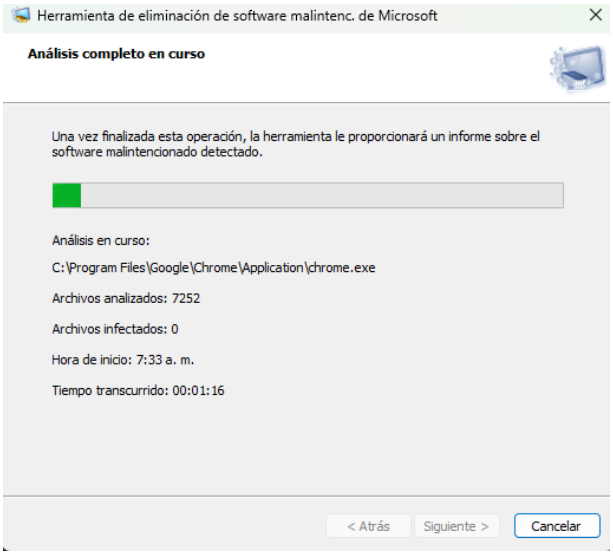


Ventajas de MRT:

Gratuito: No se requiere ningún pago adicional para acceder a esta herramienta. Actualizaciones regulares: Microsoft lanza actualizaciones mensuales para mantener el software actualizado y efectivo.
Desarrollado por Microsoft: Al ser creado por el mismo fabricante del sistema operativo, se espera que MRT funcione sin problemas y sea compatible con Windows, lo que brinda una sensación de confianza.

Desventajas de MRT:

Limitaciones de funcionalidad: MRT se centra principalmente en la eliminación de malware y puede carecer de funciones avanzadas que ofrecen las soluciones antivirus completas.
No es un reemplazo completo para un antivirus: Aunque MRT proporciona cierta protección, no garantiza una defensa completa contra todas las amenazas de seguridad. Dependencia de las actualizaciones de Microsoft: La eficacia de MRT depende de las actualizaciones periódicas de Microsoft, lo que puede generar una brecha de protección hasta que se lancen las actualizaciones.

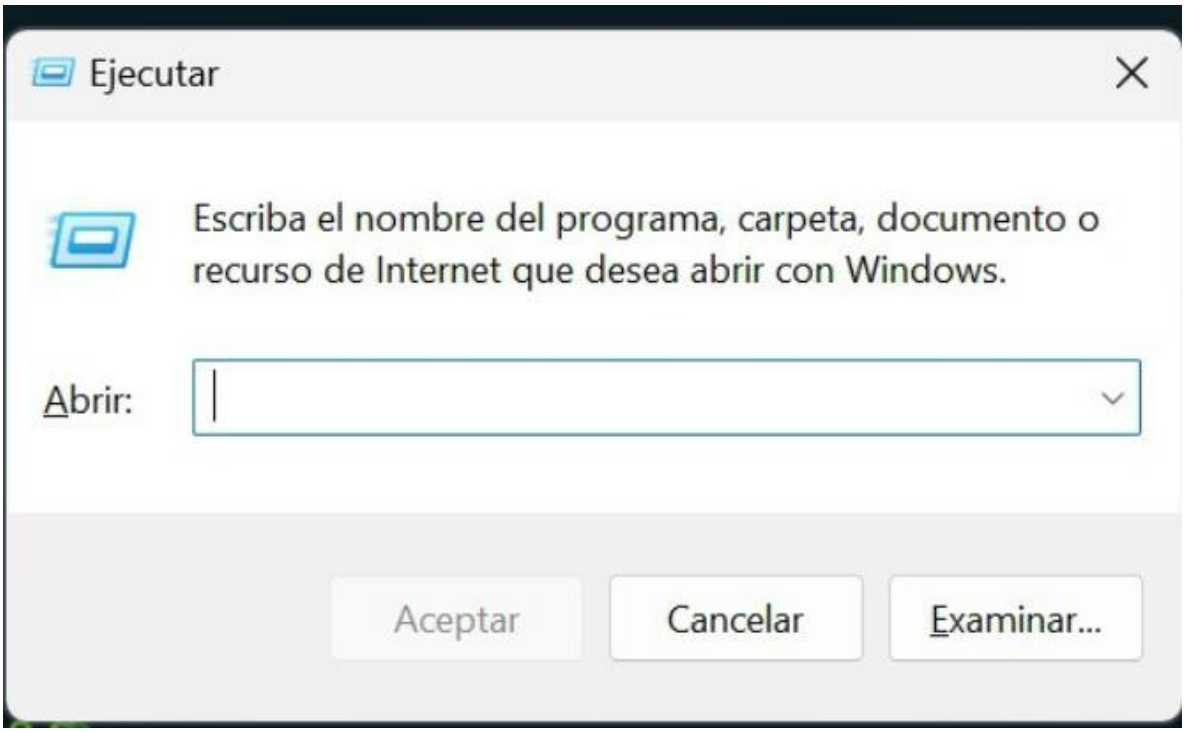


Cómo usar MRT

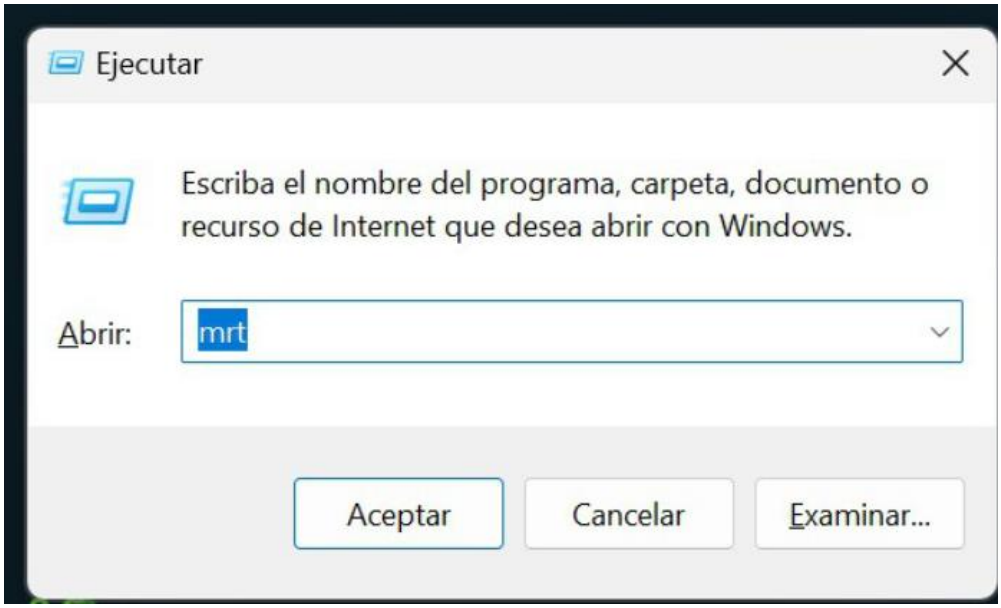
La utilización de MRT es bastante sencilla. Si estás utilizando una versión reciente de Windows, probablemente ya esté preinstalada en tu sistema. Sin embargo, también puedes descargarla desde la página oficial de Microsoft. Para acceder a ella, simplemente busca la herramienta «MRT» en el sistema y ejecútala. También puedes ejecutarla a través de la PowerShell, CMD o la ventana de ejecutar.

Una vez abierta la herramienta, haz clic en «Siguiente» y elige el tipo de escaneo que deseas realizar. Hay 3 tipos de escaneo disponibles:

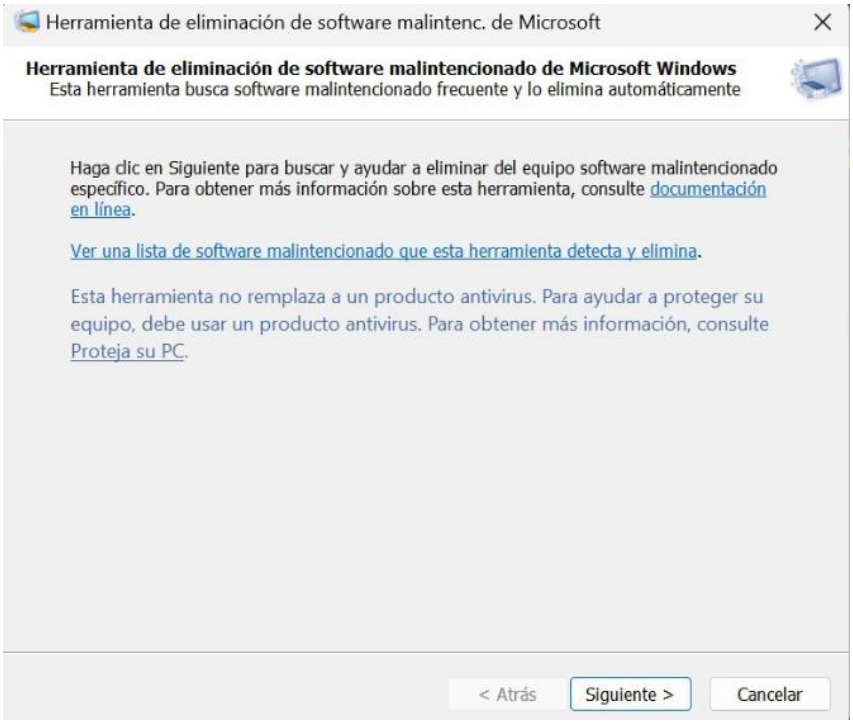
- **Análisis rápido**: Un análisis rápido de la memoria y los archivos del sistema que pueden estar infectados con mayor frecuencia. Si se detecta un virus o un troyano, la herramienta ofrecerá realizar un análisis completo;
- **Análisis completo:** Un análisis completo del dispositivo (puede llevar varias horas dependiendo de la cantidad de archivos en un disco);
- **Escaneo personalizado:** En este modo puede especificar una carpeta para escanear.



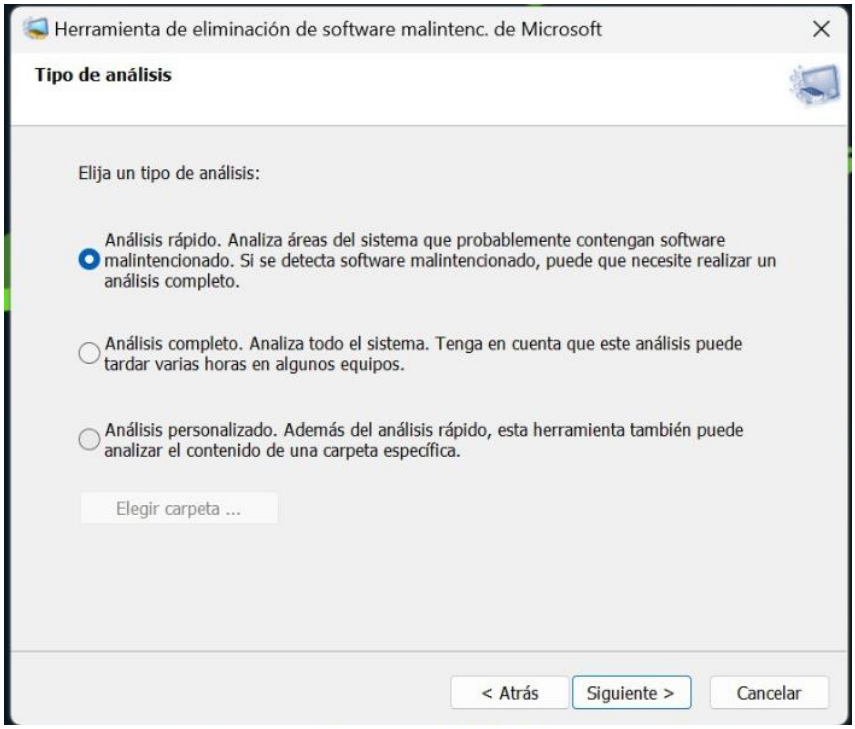
Lo primero que tienes que hacer es **pulsar a la vez las teclas *Windows + R*** de tu ordenador. Esto abrirá la ventana *Ejecutar*, donde puedes lanzar directamente programas en Windows.



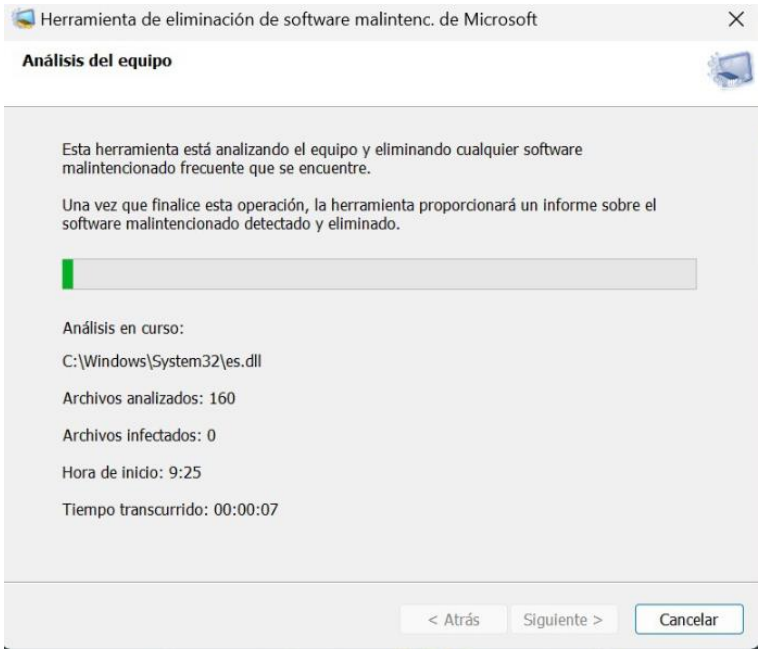
En esta ventana, tienes que escribir mrt y pulsar en Aceptar. mrt, solo esas tres letras, que sirve para lanzar el programa de eliminación de malware. Cuando lo haga, Windows te preguntará si quieres permitir que la aplicación haga cambios en el equipo, y en esta ventana tienes que pulsar que Sí.



Esto abrirá una aplicación llamada Herramienta de eliminación de software malintencionado de Microsoft. En ella, tienes una presentación en la que se te explica que buscará malware. En esta primera pantalla pulsa en Siguiente para continuar.

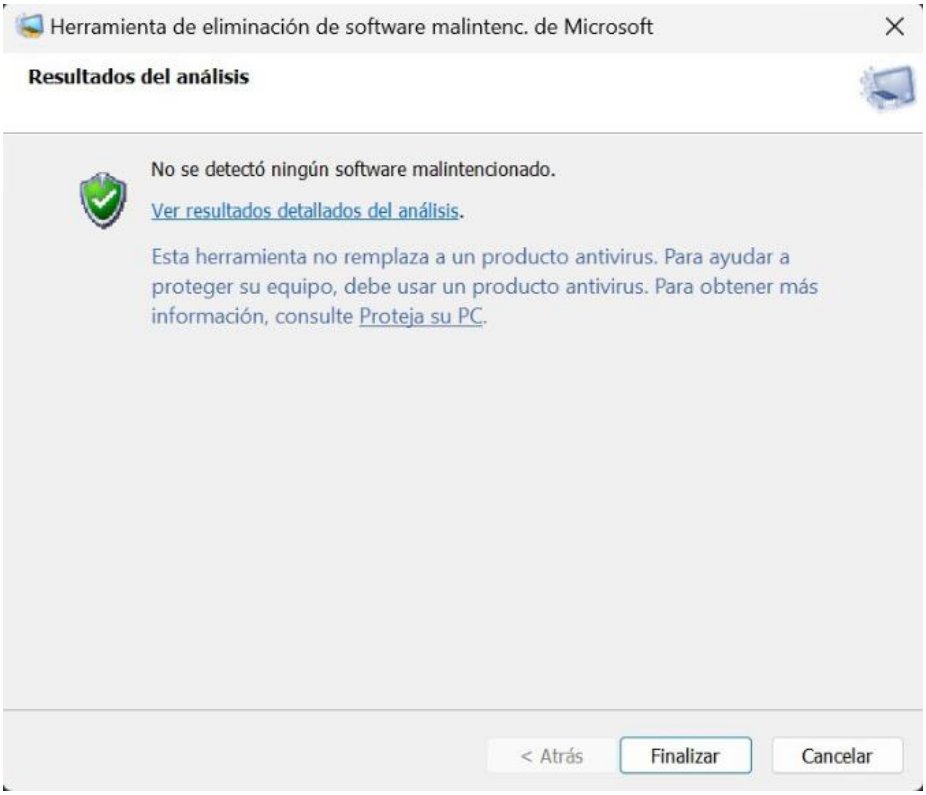


Irás a la pantalla donde tienes que elegir el tipo de análisis que quieres realizar en el ordenador. Puede ser rápido, completo buscando en todos los rincones del ordenador, o personalizado para elegir carpetas específicas que quieras analizar.

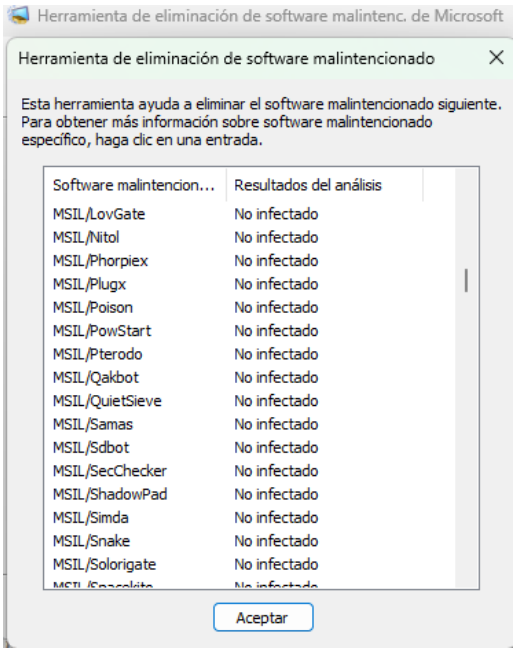


Y tras elegir el tipo de análisis que quieres realizar, el programa pasará a buscar malware y virus en tu ordenador. Este proceso puede tardar desde unos pocos minutos hasta más de una hora dependiendo del tipo de análisis que hayas

elegido y del tamaño de los discos duros o la cantidad de elementos que tengas en ellos.



Y cuando termine el análisis, el programa te dirá si ha encontrado algún software malintencionado o no. En el caso de que no haya nada, podrás finalizar la aplicación. Y si ha encontrado algo, entonces te dará la opción de borrarlo de tu ordenador. En este caso que se realizó el análisis no se encontraron archivos infectados ni software malintencionado por lo tanto la Pc está libre de riesgo de ataque malintencionado el análisis debe de hacerse periódicamente para mantener el sistema libre de software malintencionado.



En conclusión, la Herramienta de Eliminación de Software Malintencionado de Microsoft (MRT) es una solución eficaz y accesible para la eliminación de malware en sistemas Windows. Al ser una herramienta gratuita y de fácil acceso, proporciona una capa de protección básica que, aunque no reemplaza una solución antivirus completa, es útil para complementar las defensas del sistema. Sus actualizaciones periódicas y su desarrollo por Microsoft garantizan una compatibilidad óptima y una experiencia de usuario confiable.

Sin embargo, su funcionalidad es limitada en comparación con programas antivirus más completos. MRT se enfoca principalmente en la eliminación de malware ya presenté en el sistema, careciendo de funciones preventivas avanzadas como la protección en tiempo real o la defensa contra una gama más amplia de amenazas cibernéticas. Además, su efectividad depende de la frecuencia y puntualidad de las actualizaciones lanzadas por Microsoft, lo que podría dejar brechas de seguridad en el sistema hasta que se implementen nuevas actualizaciones.

En definitiva, aunque MRT es una herramienta útil para detectar y eliminar malware, se recomienda realizar análisis periódicos y complementarla con una solución de seguridad más robusta para garantizar una protección integral del sistema.

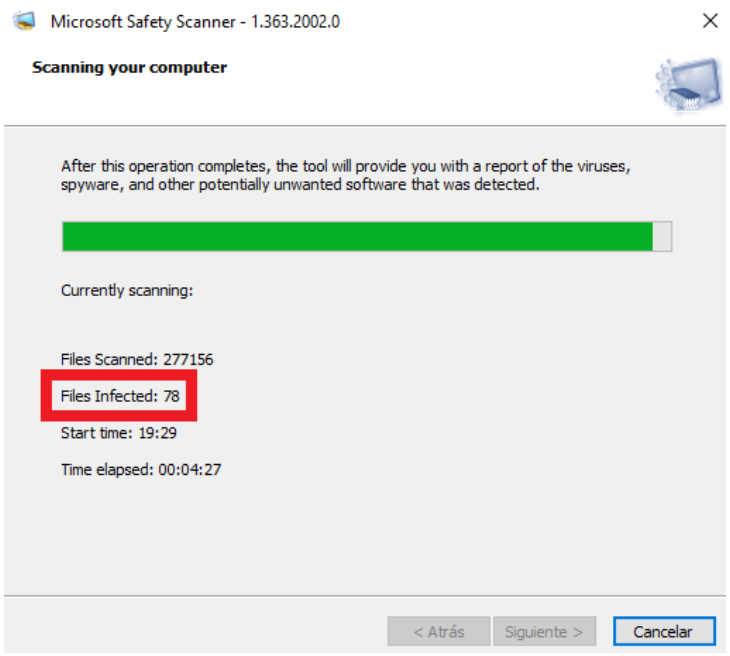
MSERT:

El Antivirus y Antimalware de Microsoft "MSERT" detecta infecciones que no resuelve.

El programa es ágil, no pesa y es muy práctico, pero, a pesar de que dice que dará un REPORT de VIRUS, se apaga sin darlo Como puede verse, detecta infecciones y, NO las RESUELVE ni da SOLUCIONES. Como mínimo debería dar un Archivo "log" para poder eliminar las infecciones manualmente.

Msert.exe es una Herramienta de Respuesta a Emergencias del Soporte de Microsoft que pertenece al Paquete de Firma del Anti-malware de Microsoft, Escáner de Seguridad de Microsoft o Protección Malware de Microsoft. Originalmente, es ejecutable es legítimo, pero a menudo causa problemas a los usuarios de Windows. Adicionalmente, puede ser afectado por malware.

El Escáner de Seguridad de Microsoft es un programa compatible con la mayoría de las versiones del sistema operativo Windows, empezando por Windows Server 2008 y finalizando con Windows 10. Esta herramienta es usada para encontrar y eliminar malware (NO LOS ELIMINA NI DA SOLUCIONES). No obstante, puede ser usada solo diez días tras su descarga.



Por ello, tras el período de 10 días, el ejecutable puede empezar a causar problemas. No obstante, los usuarios pueden eliminar msert.exe de los ordenadores ya que no es un archivo crucial de Windows. Si necesitas esta

herramienta de nuevo alguna vez, podrás descargarla. Microsoft recomienda siempre usar las últimas versiones del programa.

NOMBRE	Msert.exe
Programas relacionados	Herramienta de Respuesta a Emergencias del Soporte de Microsoft
Desarrollador	Microsoft
Sistemas Operativos	Windows OS
Versión infectada del archivo	Consume mucho CPU, causa anuncios, instala programas sin el conocimiento de los usuarios, etc.
Modos de comprobar el archivo	Una comprobación completa del sistema

Originalmente, el archivo msert.exe está localizado en la subcarpeta “C:\Archivos de Programas” u otra del disco C:\. Sin embargo, si ves este archivo en otras localizaciones, por ejemplo, C:\Windows\System32, puede ser señal de infección malware. Aquí, la comprobación del sistema con Fortect u otro anti-malware es necesaria.

Puedes sospechar que tu ordenador está infectado con un virus de ordenador si encuentras algunos de estos síntomas:

- el archivo msert.exe en el administrador de tareas usa muchos recursos del CPU del ordenador;
- no puedes abrir algunos archivos debido a sus extensiones desconocidas;
- los programas desconocidos o extensiones del navegador se instalan sin tu conocimiento;
- una cantidad incrementada de los anuncios que aparecen mientras navegas;
- redirecciones del navegador a sitios cuestionables;
- ralentización general del ordenador;
- errores desconocidos que aparecen en pantalla.

En este caso, puedes considerar la eliminación de msert.exe ya que este archivo puede estar relacionado con un troyano. No obstante, es mejor asegurarse de cuál es el archivo responsable de esta actividad comprobando Windows con un programa de eliminación de malware legítimo.

Los ordenadores pueden capturar infecciones debido a un incorrecto comportamiento de los usuarios en Internet

Como puedes entender, el archivo msert.exe legítimo y seguro llega el sistema junto a una aplicación de Microsoft. Mientras tanto, las versiones corruptas del

archivo se difunden como un troyano y puede engañar a los usuarios para que las descarguen.

El troyano puede presentarse como un programa útil, actualización o contenido similar. Recuerda que los programas maliciosos a menudo se esconden en sitios de descargas de programas gratuitos o *sharewares*. Aquí, es altamente recomendable alejarse de estos sitios y siempre ir directamente a los sitios webs de descarga oficiales.

Adicionalmente, nunca deberías hacer click en anuncios o pop-ups que alerten sobre actualizaciones de programas disponibles, virus detectados o sugerencias de comprobación del sistema en busca de virus con herramientas desconocidas. Estos anuncios suelen estar cargados de malware.

Microsoft Safety Scanner es una herramienta descargable gratuita que proporciona análisis bajo demanda y ayuda a eliminar cualquier malware u otro contenido malicioso en su computadora. Funciona con el software antivirus existente.
Examen de seguridad de Microsoft es una herramienta de examen diseñada para buscar y quitar el malware de equipos Windows. Simplemente descárguela y ejecute un examen para buscar malware e intentar revertir los cambios realizados por las amenazas identificadas.
Microsoft Safety Scanner no reemplaza el uso de un programa de software antivirus que brinda protección continua.

Para una protección en tiempo real que ayude a proteger las PC de su hogar o pequeña empresa contra virus, spyware y otro software malicioso, descargue Malwarebytes PRO u otro sistema similar.

Requisitos del sistema

Safety Scanner ayuda a quitar software malintencionado de equipos que ejecutan Windows 11, Windows 10, Windows 10 Tech Preview, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server Tech Preview, Windows Server 2012 R2, Windows Server 2012 o Windows Server 2008 R2.

Cómo ejecutar un examen

1. Descargue esta herramienta y ábrala.
2. Seleccione el tipo de examen que desea ejecutar e inicie el examen.
3. Revise los resultados del examen que se muestran en la pantalla. Para obtener resultados de detección detallados, vea el registro en **%SYSTEMROOT%\debug\msert.log**.

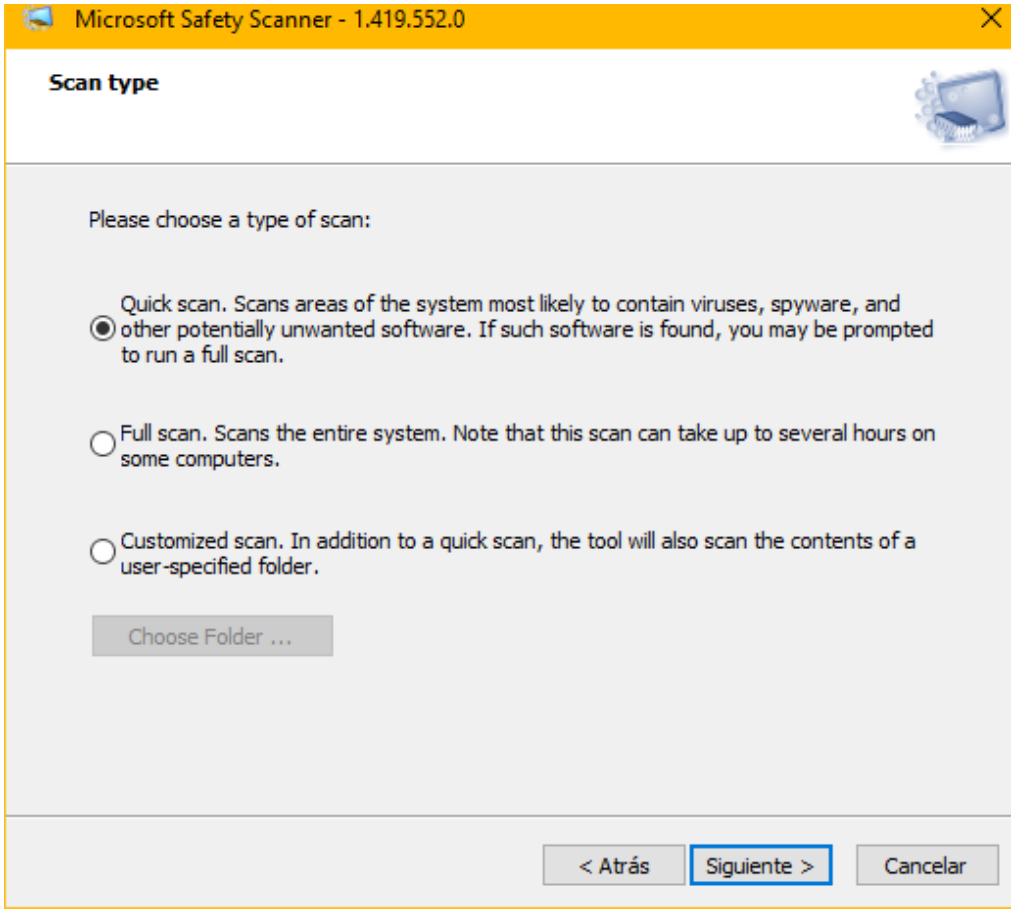
Para quitar esta herramienta, elimine el archivo ejecutable (msert.exe de forma predeterminada).

Hay tres tipos de escaneo:

Escaneo Rápido: analiza las áreas del sistema con mayor probabilidad de contener virus, software espía y otro software potencialmente no deseado. Si se encuentra dicho software, es posible que se le solicite ejecutar un análisis completo.

Escaneo Completo: Escanea todo el sistema. Tenga en cuenta que este análisis puede tardar hasta varias horas en algunas computadoras.

Escaneo Personalizado: Además de un escaneo rápido, la herramienta también escaneará el contenido de una carpeta especifica por el usuario.



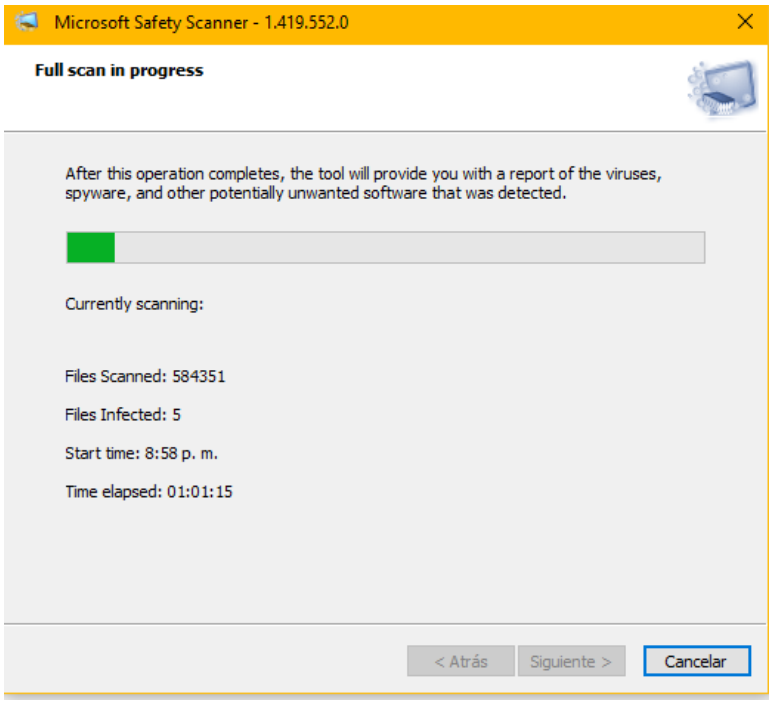
Una vez completada esta información, la herramienta le proporcionara un informe del software que fue detectado y eliminado.

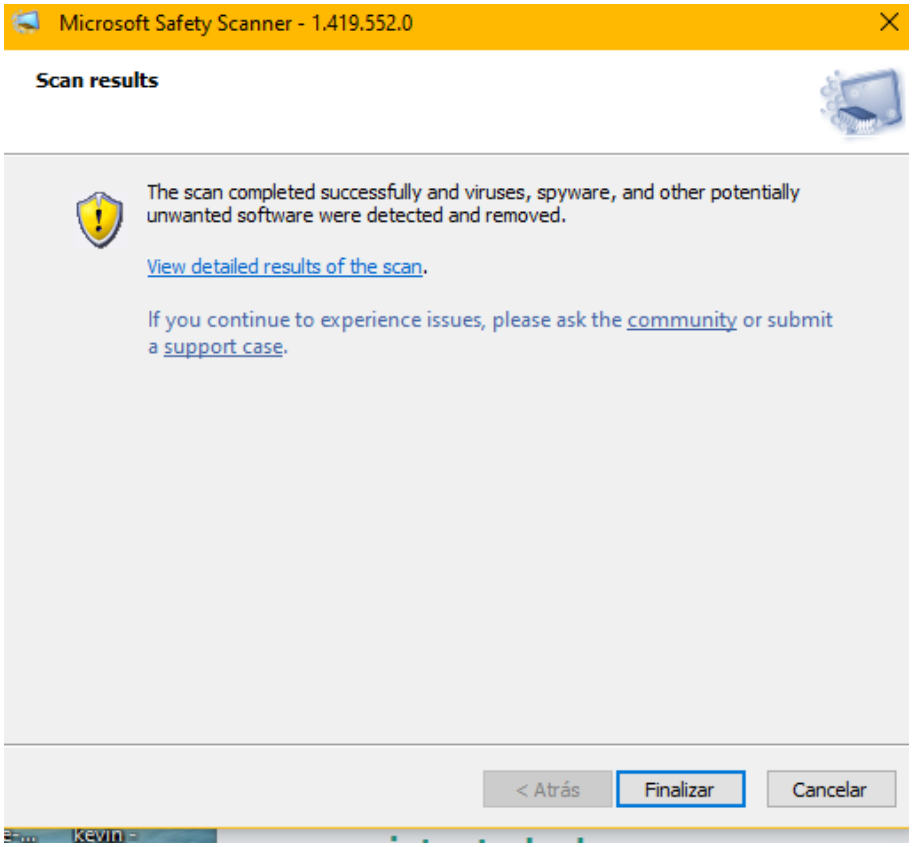
En la imagen se muestra los archivos escaneados: 584351

Archivos infectados: 5

Hora de Inicio: 8:58 pm

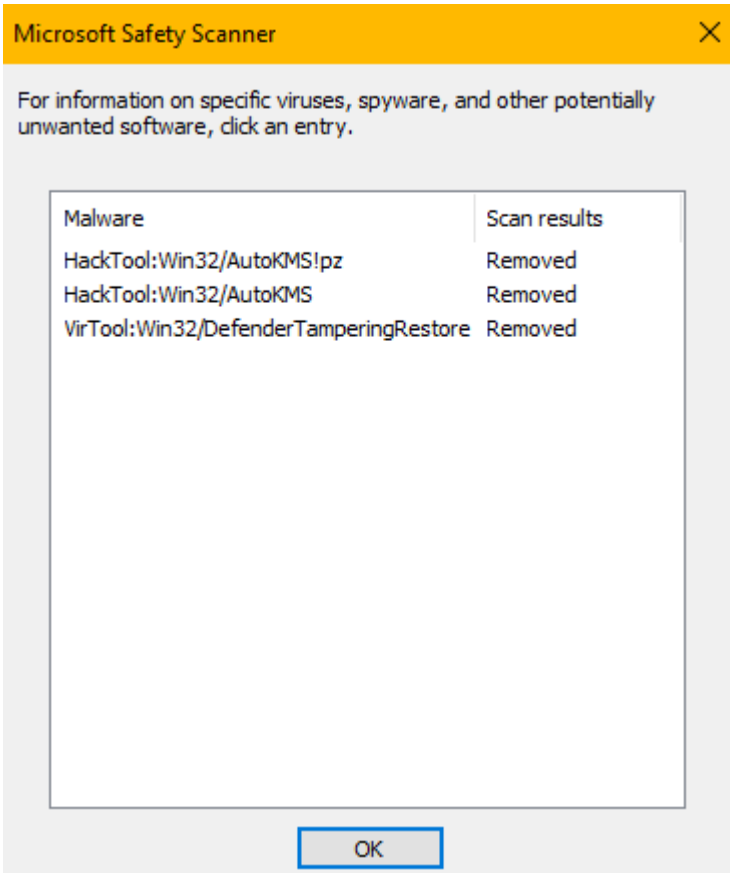
Tiempo transcurrido: 01:01:15





Para obtener información sobre virus y otros programas potencialmente software no deseado haga clic en una entrada malware.

Aquí se muestran los resultados del análisis y se procede a remover o eliminar aquello que afecta al sistema y sus nos indica el nombre del software malintencionado que está afectando el sistema o archivos de nuestra computadora.



En conclusión, MSERT (Microsoft Safety Scanner) es una herramienta útil de Microsoft diseñada para detectar y eliminar malware bajo demanda, pero presenta algunas limitaciones importantes. Si bien destaca por su agilidad, practicidad y compatibilidad con una amplia gama de sistemas operativos Windows, no ofrece soluciones automáticas para eliminar las infecciones detectadas. El hecho de que no genere un informe detallado o log de los virus encontrados limita la capacidad del usuario para realizar una remediación manual eficaz. Además, su uso temporal, limitado a diez

días tras la descarga, puede generar problemas una vez caducado, lo que reduce su utilidad a largo plazo.

A pesar de ser una herramienta de emergencia eficaz en la detección de amenazas, MSERT no sustituye un antivirus de tiempo real ni proporciona una solución completa para la protección continua. Requiere la intervención del usuario o la combinación con otros programas de seguridad para la eliminación total de malware y la corrección de los cambios realizados por las amenazas. Por tanto, aunque es útil para situaciones puntuales, no debe considerarse como una solución de seguridad primaria, y se recomienda el uso de herramientas más robustas, como Malwarebytes PRO u otros sistemas con protección en tiempo real, para una defensa integral.