UADER – Facultad de Ciencia y Tecnología

Laboratorios GUGLER

Nombre del trabajo: Virus Informáticos.

Curso: Reparación y Mantenimiento de PC con Herramientas Libres.

Año: 2023.

Alumno: Tomás Portela.

Índice:

Introducción:

Los virus informáticos son una constante amenaza en el mundo digital actual.
En estos tiempos es algo común escuchar casos en donde nuestra computadora posee una infección por uno o varios virus que podrían haber sido a causa de un simple correo electrónico o bien por medio de un archivo descargado. Que terminan siendo perjudiciales tanto para el usuario como también para entes políticos o empresariales, ya sea por su capacidad para dañar sistemas o bien para robar información valiosa y personal.
La lucha contra los virus informáticos es una tarea constante y desafiante, es por esto que en esta sección analizaremos en detalle que son los virus informáticos, su impacto y la importancia de comprender y protegerse de ellos. Como también adentrarnos al mundo de los famosos antivirus que serán de gran utilidad para la protección de nuestra computadora.

¿Que son los virus informáticos?

La palabra virus es un tema muy grande en el ámbito informático y abarca mucha información, lo que sí sabemos es que un virus también llamados malware son programas maliciosos diseñados para infectar sistemas informáticos y causar daños o alteraciones en el funcionamiento de los mismos. Es decir que un malware puede replicarse, controlar el equipo, robar información como también infectar desde archivos diarios hasta entrar al sistema de arranque de la computadora.
Estos virus se propagan y reproducen al adjuntarse a otros programas, archivos o documentos y pueden ser trasmitidos a través de medios de almacenamiento, redes o incluso a través de un correo electrónico.
Muchos virus simulan ser programas legítimos para convencer a los usuarios de que los ejecuten en su dispositivo, insertando así la carga útil del virus.
En el caso de que dicho virus quiera infectar un archivo, este mismo ingresa su propio código malicioso en las líneas del código del programa y se ejecutara cada vez que se inicie ese mismo programa.

Tipos de virus informáticos:

Hoy en día existen nueve clases principales de virus informáticos, algunos podrían estar repletos de otro malware para incrementar la posibilidad de infección y daño. Estos virus informáticos son los siguientes:

- ***Virus de sector de arranque***

En este tipo de virus, daña o controla el sector de arranque del disco, analizando al equipo, los atacantes suelen diseminar este tipo de virus mediante un dispositivo USB malintencionado. El virus se activa cuando los usuarios conectan el dispositivo USB y arrancan su equipo.

- ***Virus de script***

Es este tipo de virus, la mayoría de los navegadores tienen defensas contra los scripts malintencionados, pero los navegadores más antiguos u obsoletos tienen vulnerabilidades que pueden permitir a un delincuente cibernético ejecutar un código en el dispositivo local.

● ***Virus en ejecutables***

En este tipo de virus, infectan a los ejecutables con extensión .exe, .com, .bat, .dll, entre otros. En donde al ser ejecutado infectan con su código y luego vuelve al curso normal al programa que está infectado. Este mismo se resguarda en la memoria y comienza a infectar a otros archivos que son abiertos luego de la ejecución del ejecutable infectado.

● ***Virus residentes***

En este tipo de virus, se incrustan en la memoria del ordenador y permanecen ocultos hasta ser activados, este malware puede permanecer en hibernación hasta una fecha u hora especificas o bien hasta que un usuario ejecuta una cierta acción.

● ***Virus polimórfico***

En este tipo de virus, el creador del malware puede usar un código polimórfico para cambiar la huella del programa y así evitar su detección, estos virus dificultan a los antivirus a ser detectados y eliminados.

● ***Virus gusanos***

En este tipo de virus, es un tipo de malware bastante conocido el cual consiste en hacer copias de sí mismo y propagarlas a otros usuarios. Los gusanos también pueden insertar carga útil y agotar recursos del sistema.

● ***Virus de macros***

En este tipo de virus, los archivos de Microsoft office u otro software similar pueden ejecutar macros y estas macros se pueden usar para descargar malware adicional o ejecutar un código malintencionado. Los virus macro despliegan su carga útil cuando se abre el archivo y se ejecutan los macros.

● ***Virus multipartitos***

En este tipo de virus, son programas malintencionados que se diseminan por las redes de otros sistemas o bien copiándose a sí mismos o inyectando código en recursos informáticos esenciales.

● ***Virus troyano***

En este tipo de virus, es un virus muy conocido y común, suelen ser programas disfrazados sin aparentar nada malo pero cuando terminan siendo ejecutados, el hacker tiene acceso al computador y puede robar informacional personal, controlar y descargar contenido malicioso al mismo.

¿Cómo detectar un virus informático?

Como bien sabemos los creadores del malware generan un código que resulta muy difícil de detectar hasta que se ejecuta la carga útil. Sin embargo pueden ocurrir errores mientras se ejecuta el virus. Es por ello que mencionaremos algunas señales de que nuestra computadora podría estar infectada.

● *La página de inicio de su navegador web es diferente sin que usted haya hecho cambios.*

● *Las contraseñas cambian sin tu consentimiento o sin haber interactuado con la cuenta.*

● *Se inician programas desconocidos cuando el ordenador arranca o cuando se abren programas específicos.*

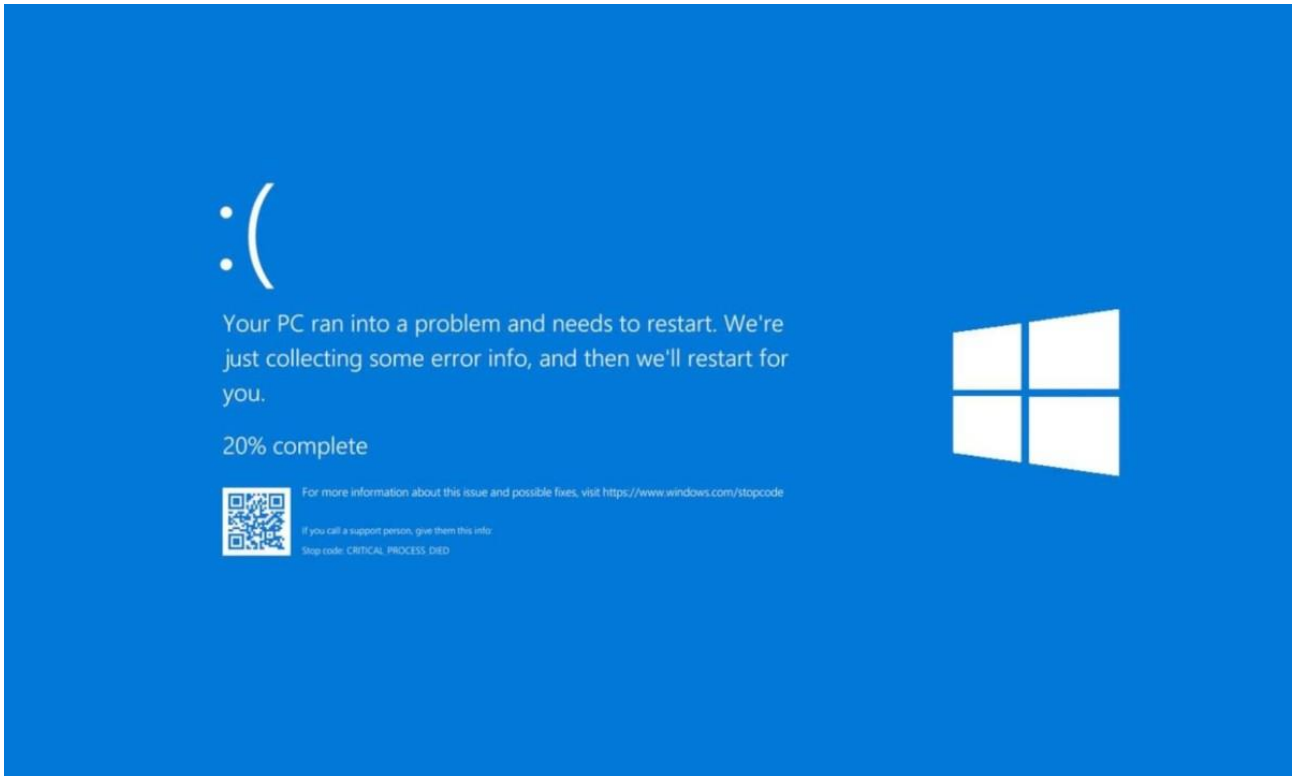
● *Ventanas emergentes, como anuncios o enlaces a páginas web malintencionadas.*

● *Envío automático de correos electrónicos a tu lista de contactos que le alertan de que tú cuenta está enviando mensajes extraños.*

● *El computador se cuelga con frecuencia, se le agota la memoria con unos pocos programas activos o bien aparece la pantalla azul de Windows.*

Caso del Windows 7:

Caso del Windows 10:



Medidas de seguridad y prevención:

Debido a que muchas veces el virus termina dañando la computadora, hay diferentes métodos y consejos para evitar estos riesgos. Es por ello que nombrare algunos consejos que me sirvieron y que sigo utilizando día a día.

- ***No abrir archivos adjuntos ejecutables en correos electrónicos***

Muchos de los ataques de malware son a causa de este suceso, por ello los archivos adjuntos ejecutables jamás deben abrirse y los usuarios deben evitar ejecutar macros en archivos.

- ***Evite visitar webs que generen desconfianza***

Tanto algunas webs como los navegadores antiguos tienen vulnerabilidades que pueden ser aprovechadas por los hackers. Usted debe mantener siempre actualizado su navegador. Además si usted no visita estas páginas, se evita posibles descargas o el redirecionamiento a páginas malintencionadas que contienen virus.

- ***No usen software pirata***

Si bien muchos de los programas que se suelen utilizar son de pago, también hay múltiples opciones de programas originales libres y gratuitos a la hora de necesitar un programa. Es por ello que usted debe evitar el uso de software pirata ya que muchos de ellos suelen contener virus. Descargue el software solamente desde la página web oficial de los proveedores.

- ***Instale un antivirus***

Los antivirus se deben ejecutar en cualquier dispositivo que esté conectado a la red. Ya que el antivirus evita que los ejecutables del virus se ejecuten en su computador local. Con este punto podemos dar hincapié a un tema de suma importancia.

Los antivirus:

Un antivirus es un software diseñado para proteger un dispositivo como una computadora contra programas maliciosos, como un virus, malware, ransomware, entre otras amenazas. Su propósito principal es el detectar, prevenir y eliminar estas amenazas para mantener el dispositivo y la información almacenada en el seguro.

Los antivirus utilizan una gran variedad de técnicas para identificar y combatir con las amenazas.

● ***Detección de firmas***

Los antivirus mantienen una base de datos de firmas o patrones conocidos de programas maliciosos. Escanean los archivos en busca de coincidencias con estas firmas y si se encuentra una coincidencia, el antivirus toma medidas para eliminar la amenaza.

● ***Detección heurística***

Los antivirus también utilizan algoritmos heurísticos para detectar comportamientos sospechosos o características comunes de los programas maliciosos. Por lo tanto si se detecta un comportamiento sospechoso, el antivirus puede bloquear o poner en cuarentena el archivo.

● ***Análisis de comportamiento***

Algunos antivirus monitorean el comportamiento de los programas en tiempo real para detectar actividades maliciosas. Si un programa se comporta de manera sospechosa, el antivirus puede tomar medidas para detenerlo y eliminarlo.

Además de la detención y eliminación de amenazas, los antivirus pueden ofrecer funciones adicionales, como cortafuegos, protección de navegación web, como también del correo electrónico y actualizaciones periódicas de seguridad para mantenerse al día con las últimas amenazas.

Tipos de antivirus:

La elección del antivirus adecuado dependerá de tus necesidades y del tipo de dispositivo que pretendas proteger. Es por ello que te presentare una lista de diferentes tipos de antivirus.

● ***Antivirus de escritorio***

Este tipo de antivirus está diseñado para proteger las computadoras de amenazas de malware como virus, gusanos, troyanos y spyware, en donde escanean el sistema en busca de software malicioso y lo eliminan o lo ponen en cuarentena.

● ***Antivirus en la nube***

Este tipo de antivirus funcionan en conjunto con servicios en la nube y requieren una conexión a internet activa. En lugar de realizar el análisis de seguridad en el dispositivo local, envían archivos sospechosos a servidores en la nube para su análisis. Lo que permite una detección más rápida y actualizaciones de seguridad en tiempo real.

● ***Antivirus de firma***

Este tipo de antivirus de firma utilizan una base de datos de firmas conocidas de malware para identificar y eliminar amenazas. Estas firmas son patrones de código específicos que se encuentran en el malware. Este antivirus compara los archivos del sistema con la base de datos de firmas para detectar amenazas conocidas.

● ***Antivirus de múltiples motores***

Estos antivirus utilizan varios motores de detección de malware para mejorar la precisión y la eficacia de la detección. Combinan diferentes tecnologías de detección como el análisis de firmas y el análisis heurístico, para proporcionar una protección más completa contra las amenazas.

● ***Antivirus para dispositivos móviles***

Estos antivirus están diseñados específicamente para proteger dispositivos móviles, como teléfonos inteligentes y tabletas, contra malware y otras amenazas móviles. Además ofrecen características adicionales adaptadas a las necesidades de seguridad de los dispositivos móviles.

Avast Free Antivirus

En este caso nos centraremos en el antivirus Avast ya que es un software gratuito y es bastante útil a la hora de optar por un antivirus. Además es un antivirus apto para computadoras de bajo requisitos gracias a sus especificaciones. Como también sencillo y fácil de usar.

Los requisitos mínimos que solicita Avast son los siguientes:

◦ ***Sistema Operativo:*** *Windows 7 SP1, Windows 8/8.1, Windows 10 y Windows 11. (También disponible para Mac, Android y iOS.)*

◦ ***Memoria RAM:*** *1 GB de RAM o más.*

◦ ***Espacio en disco:*** *Al menos 2 GB de espacio libre en el disco duro.*

◦ ***Tipo de CPU:*** *Intel Pentium 4 / AMD Athlon 64 en adelante. (Basados en ARM no son compatibles.)*

◦ ***Pantalla:*** *Se recomienda una resolución estándar no inferior a 1024x768 pixeles.*

◦ ***Requisito extra:*** *Conexión a internet para descargar, activar y mantener las actualizaciones del programa y la base de datos del antivirus.*

Instalación de Avast Free Antivirus:

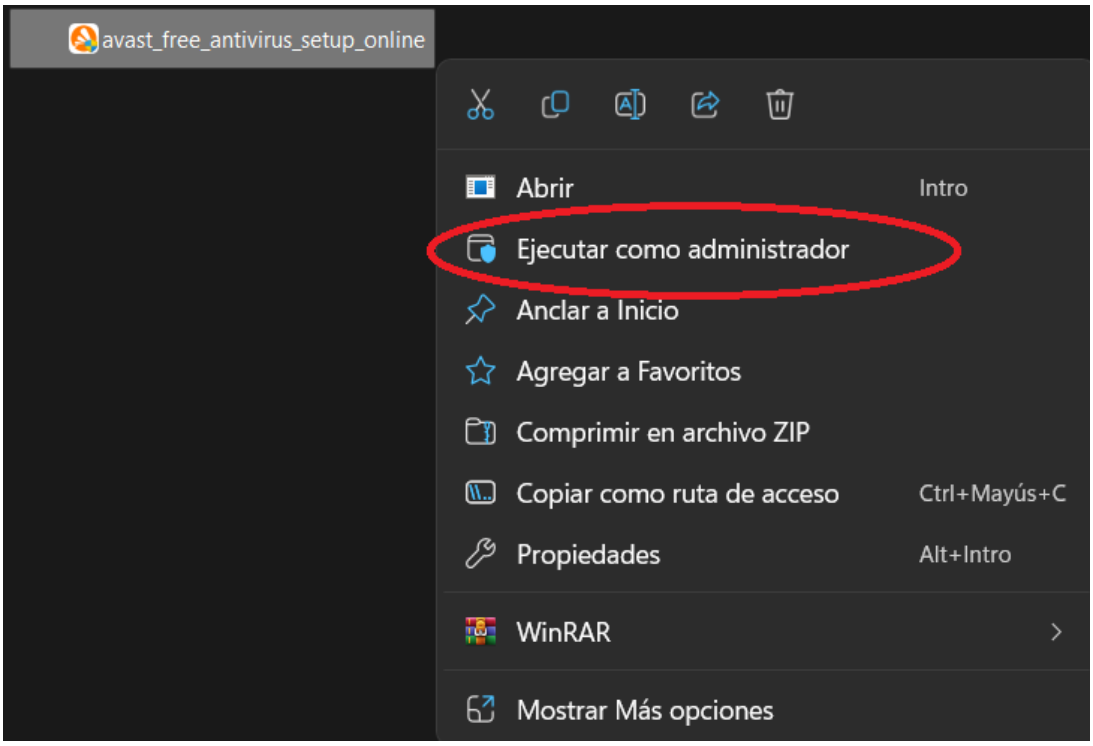
Para la instalación de este antivirus nos guiaremos en diferentes pasos:

Paso Numero 1:

Lo primero que debemos hacer es descargar el programa desde la página oficial https://www.avast.com/index en donde aparecerá un botón llamado ***DESCARGAR GRATIS*** *en la parte central.*

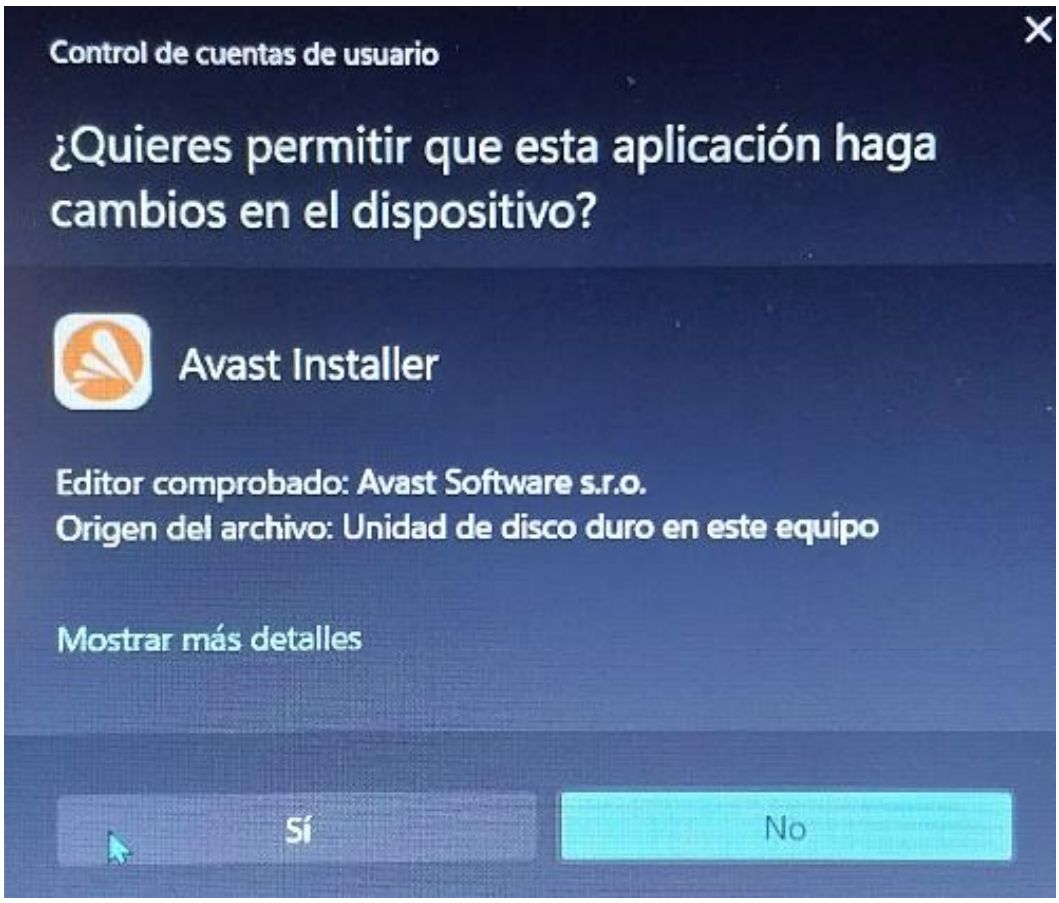
Paso Numero 2:

Luego de haber descargado el archivo de instalación en la ubicación que usted haya asignado, haga click con el botón derecho en el archivo de instalación descargado y seleccione Ejecutar como administrador en recuadro que le aparecerá.



Paso Numero 3:

Si en caso de que le pidan permisos en el cuadro de dialogo Control de cuentas de usuario, haga click en Sí.

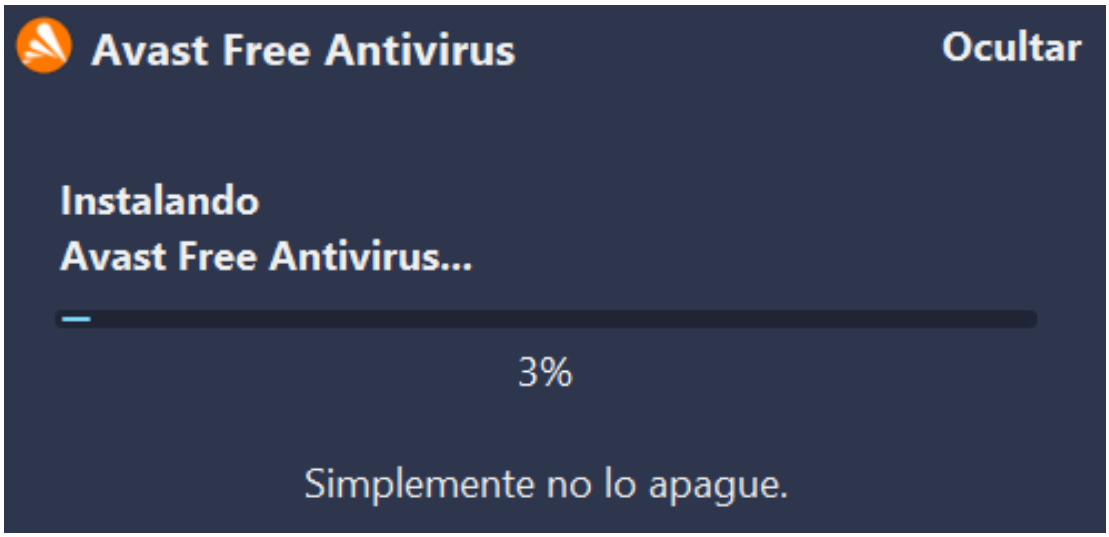


Paso Numero 4:

Para cambiar el idioma de instalación predeterminado, haga click en el idioma actual en la esquina superior derecha de la pantalla. Luego haga click en instalar para proceder con la instalación predeterminada o bien, haga click en Personalizar si necesita realizar cambios a la configuración por defecto.

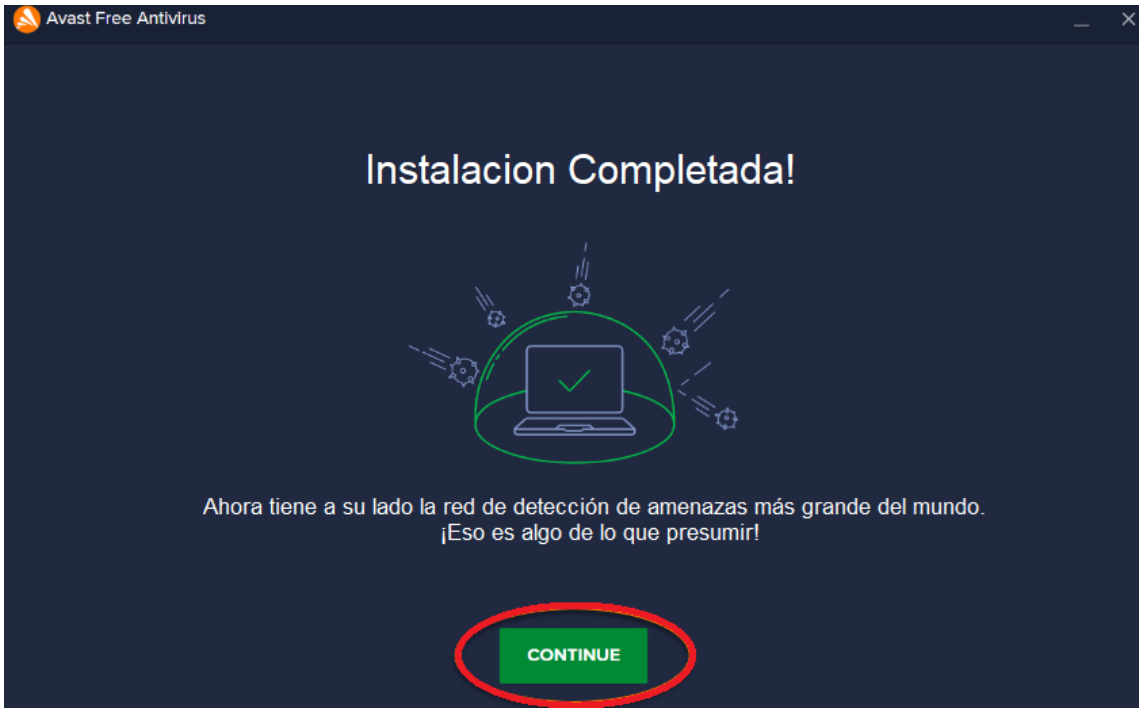
Paso Numero 5:

Espere mientras el asistente instala Avast Free Antivirus en su PC.



Paso Numero 6:

Cuando termine la instalación, haga click en continúe.

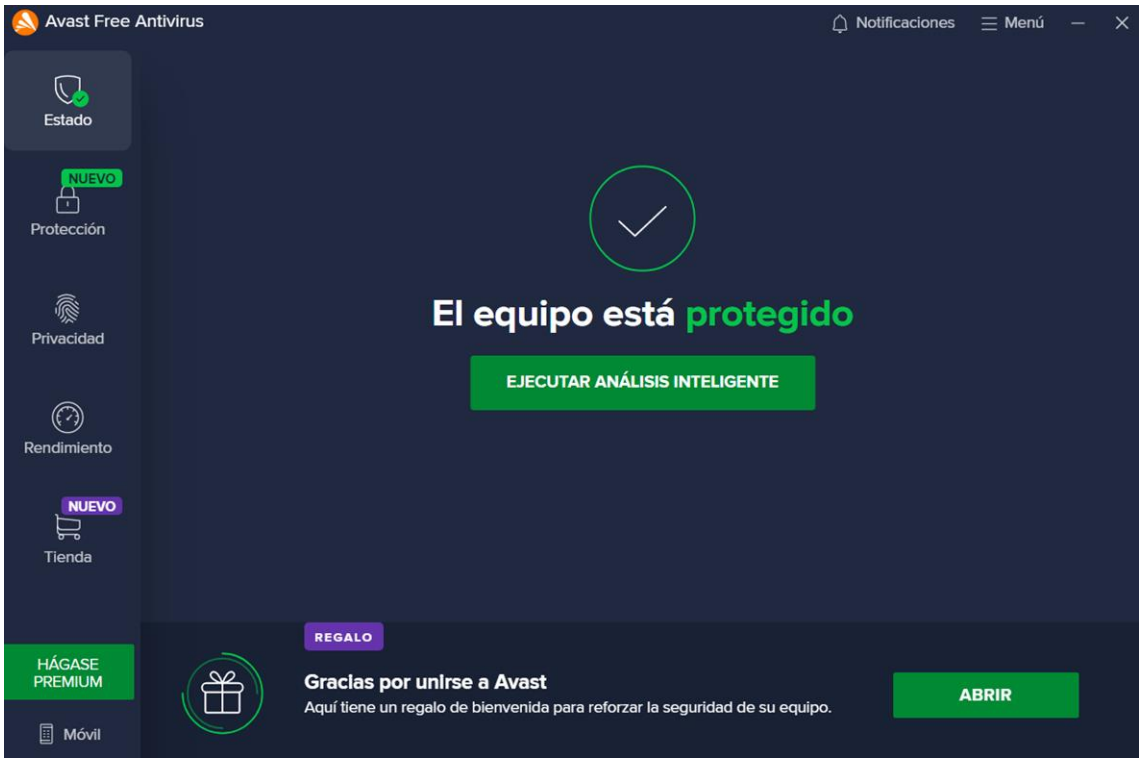


Paso Numero 7:

Haga click en Ejecutar primer análisis para iniciar un completo análisis inteligente, que detecta virus, malware, complementos problemáticos del navegador y otros problemas en su PC.

Paso Numero 8:

Avast Free Antivirus ya está instalado en su PC y listo para su uso, pero algunos componentes pueden no funcionar completamente hasta que reinicie su PC.



Ya no es necesario registrar Avast Free Antivirus, ya que su suscripción gratuita inicial se activa automáticamente después de la instalación.

Conclusión:

Siendo este el fin del trayecto, podemos dar como como conclusión que la lucha contra los virus informáticos es una responsabilidad compartida entre los usuarios y las empresas. La conciencia y la implementación de medidas de seguridad adecuadas son esenciales para prevenir y mitigar los efectos perjudiciales de estos programas maliciosos. Mantenerse actualizado, utilizar herramientas de seguridad confiables y adoptar una actitud cautelosa en línea son pasos cruciales para protegerse en el mundo digital cada vez más interconectado.