

G DATA

Security Software



G DATA ANTIVIRUS for Mac

G DATA ANTIVIRUS for Mac

fecha de publicación 2015.01.26

Copyright© 2015 G DATA Software AG

Advertencia legal

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de G DATA Software AG. La inclusión de citas breves en artículos sólo es posible con la mención de la fuente citada. El contenido no puede modificarse de forma alguna.

Advertencia y Renuncia de Responsabilidad. El presente producto y su documentación están protegidos por copyright. La información en este documento se provee "tal como está", sin garantía. Aunque se ha tomado toda precaución en la preparación de este documento, los autores no tendrán ninguna responsabilidad con ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en este trabajo.

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de G DATA Software AG, por lo que G DATA Software AG no se hace responsable del contenido de cualquier sitio enlazado. Si usted accede a los sitios web de terceros listados en este documento, lo hará bajo su propia responsabilidad. G DATA ANTIVIRUS for Mac proporciona estos enlaces sólo por conveniencia, y la inclusión del enlace no implica que G DATA Software AG apruebe o acepte ninguna responsabilidad por el contenido del sitio del tercero.

Marcas Registradas. En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas, en este documento, son propiedad exclusiva de sus respectivos propietarios, y respectivamente reconocidas.



Tabla de contenidos

Uso de la guía	v
1. Propósito y público al que va dirigida	v
2. Cómo usar esta guía	v
3. Convenciones utilizadas en esta guía	vi
3.1. Convenciones Tipográficas	vi
3.2. Admoniciones	vi
4. Petición de Comentarios	vii
1. Instalación y Desinstalación	1
1.1. Requisitos del Sistema	1
1.2. Instalando G DATA ANTIVIRUS for Mac	1
1.2.1. Paso 1 - Ventana de Bienvenida	3
1.2.2. Paso 2 - Ver el Archivo Readme	4
1.2.3. Paso 3 - Lea los Términos del Contrato de Licencia	5
1.2.4. Paso 4 - Iniciar la Instalación	6
1.2.5. Paso 5 - Instalando G DATA ANTIVIRUS for Mac	7
1.2.6. Paso 6 - Finalizar	8
1.3. Eliminando G DATA ANTIVIRUS for Mac	9
2. Iniciando	10
2.1. Acerca de G DATA ANTIVIRUS for Mac	10
2.2. Abrir G DATA ANTIVIRUS for Mac	10
2.3. Ventana Aplicación Principal	11
2.4. Icono Aplicación Dock	13
3. Protección contra Software Malicioso	14
3.1. Mejores Prácticas	14
3.2. Analizando Su Mac	15
3.3. Activar o desactivar el Análisis continuo	17
3.4. Asistente del Análisis	17
3.5. Reparar Incidencias	18
3.6. Cuarentena	20
3.7. Protección Web	21
3.8. Actualizaciones	23
3.8.1. Solicitando una Actualización	24

G DATA ANTIVIRUS for Mac

3.8.2. Obteniendo Actualizaciones a través de un Servidor Proxy	24
3.8.3. Actualice a una nueva versión	24
4. Preferencias de Configuración	26
4.1. Preferencias de Acceso	26
4.2. Preferencias Generales	26
4.3. Preferencias de análisis	27
4.4. Exclusiones del Análisis	30
5. Registro de G DATA ANTIVIRUS for Mac	32
5.1. Sobre el Registro	32
5.2. Registro de G DATA ANTIVIRUS for Mac	32
5.3. Adquiera una Licencia	33
6. Preguntas frecuentes	34
7. Soporte e Información de Contacto	37
Tipos de Software Malicioso	38

Uso de la guía

1. Propósito y público al que va dirigida

Esta guía está dirigida a todos los usuarios Macintosh que han elegido **G DATA ANTIVIRUS for Mac** como solución de seguridad para sus ordenadores personales. La información presentada en este libro es apta no sólo para expertos en informática, sino para todo aquel capaz de trabajar bajo Macintosh.

Averiguará cómo configurar y usar G DATA ANTIVIRUS for Mac para protegerse contra virus y otro software malicioso. Aprenderá a sacarle el máximo partido a G DATA ANTIVIRUS for Mac.

Le deseamos una útil y placentera lectura.

2. Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Iniciando (p. 10)

Comience con G DATA ANTIVIRUS for Mac y su interfaz de usuario.

Protección contra Software Malicioso (p. 14)

Aprenda a como utilizar G DATA ANTIVIRUS for Mac para protegerse contrasoftware malicioso.

Preferencias de Configuración (p. 26)

Aprenda más sobre las preferencias de G DATA ANTIVIRUS for Mac.

Soporte e Información de Contacto (p. 37)

Dónde consultar y dónde pedir ayuda si se produce una situación inesperada.

3. Convenciones utilizadas en esta guía

3.1. Convenciones Tipográficas

En esta guía se utilizan distintos estilos de texto con el fin de mejorar su lectura. En la siguiente tabla se indican su aspecto y significado.

Apariencia	Descripción
ejemplo de sintaxis	Ejemplos de sintaxis se muestran con letras monospaced.
http://www.gdata.es	Los enlaces URL le dirigen a alguna localización externa, en servidores http o ftp.
info@gdata.es	Las direcciones de e-mail se incluyen en el texto como información de contacto.
Uso de la guía (p. v)	Este es un enlace interno, hacia alguna localización dentro del documento.
nombre de archivo	Los archivos y carpetas se muestran usando una fuente monoespaciada.
opción	Todas las opciones del producto se muestran utilizando caracteres en negrita .
palabra clave	La palabras o frase más importantes se destacan utilizando caracteres en negrita .

3.2. Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.



Nota

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.



Importante

Este tipo de advertencia requiere su atención y no es recomendable omitirla. Normalmente proporciona información importante, aunque no extremadamente crítica.



Aviso

Se trata de información crítica que debería tratar con extrema cautela. No ocurrirá nada malo si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente arriesgado.

4. Petición de Comentarios

Le invitamos a ayudarnos a mejorar el manual. Hemos comprobado y verificado toda la información como mejor hemos sabido. Por favor, escribanos para explicarnos cualquier tipo de defecto que encuentre en este manual o cómo podría mejorarse, y así ayudarnos a ofrecerle la mejor documentación posible.

Haganoslo saber mandando un e-mail a info@gdata.es. Por favor, escriba en Inglés todos los correos relacionados con la documentación, para poder procesarlos correctamente.

1. Instalación y Desinstalación

Este capítulo incluye los siguientes temas:

- *Requisitos del Sistema* (p. 1)
- *Instalando G DATA ANTIVIRUS for Mac* (p. 1)
- *Eliminando G DATA ANTIVIRUS for Mac* (p. 9)

1.1. Requisitos del Sistema

Puede instalar G DATA ANTIVIRUS for Mac en equipos con OS X Lion (10.7.5), OS X Mountain Lion (10.8.5) u OS X Mavericks (10.9 o posterior).

Su Mac también debe cumplir con todos estos requisitos adicionales:

- Mínimo 1 Gb de Memoria RAM
- Mínimo 400 MB de espacio libre en disco

Se requiere de una conexión a Internet para registrar y actualizar G DATA ANTIVIRUS for Mac.



Cómo saber que versión de MAC OS X tiene y la información de hardware sobre su Mac

Haga clic en el icono Apple en la esquina izquierda superior de la ventana y elija **Acerca de este Mac**. En la ventana que aparece puede ver la versión del sistema operativo y otra información útil. Haga clic en **Más Info** para información detallada del hardware.

1.2. Instalando G DATA ANTIVIRUS for Mac

Para instalar G DATA ANTIVIRUS for Mac:

1. Inicie sesión como administrador.
2. Realice una de las siguientes acciones:

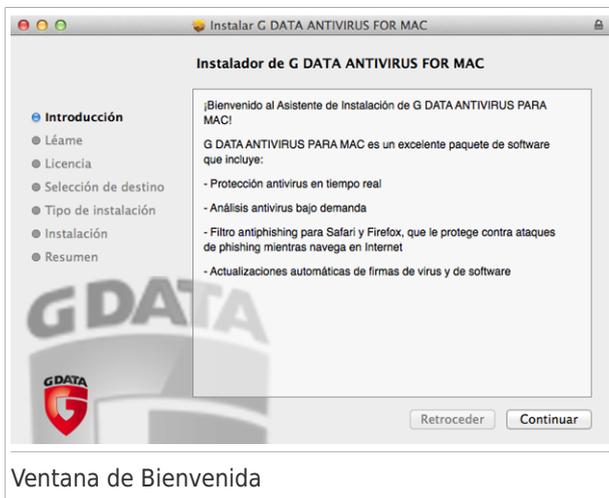
G DATA ANTIVIRUS for Mac

- Introduzca el CD/DVD de instalación en la unidad. Normalmente, se mostrará al cabo de unos instantes una ventana con los paquetes de instalación y desinstalación. Si no fuese así, busque la imagen de disco en su escritorio y ábrala.
- Descargue o copie la imagen de la instalación (un archivo .dmg o .iso) en su escritorio y ábrala. Aparecerá inmediatamente una ventana con los paquetes de instalación y desinstalación.



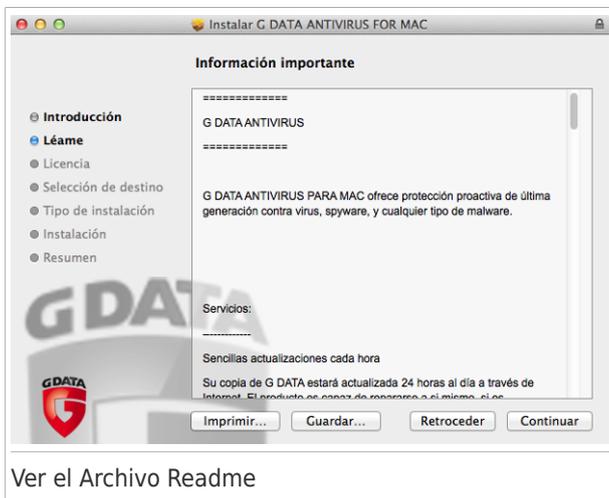
3. Haga clic en G DATA ANTIVIRUS for Mac .pkg. Se iniciará un asistente que le guiará a través del proceso de instalación.
4. Siga el asistente de instalación.

1.2.1. Paso 1 - Ventana de Bienvenida



Haga clic en **Continuar**.

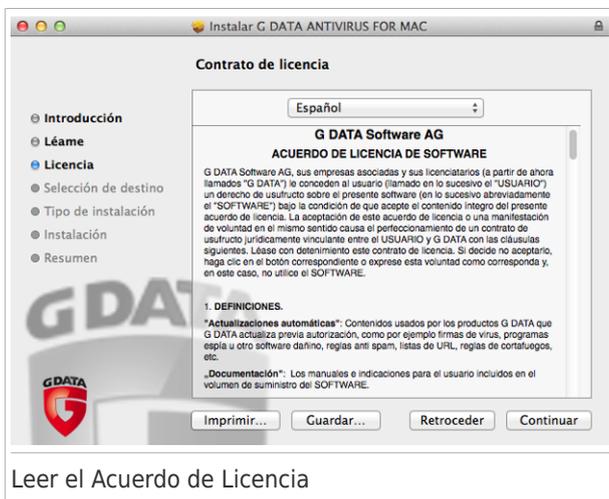
1.2.2. Paso 2 - Ver el Archivo Readme



El archivo readme proporciona información completa sobre G DATA ANTIVIRUS for Mac. Puede imprimir o guardar el archivo readme de modo que puede revisar este más tarde.

Haga clic en **Continuar**.

1.2.3. Paso 3 - Lea los Términos del Contrato de Licencia



El Acuerdo de Licencia es un acuerdo legal entre usted y G DATA Software AG para el uso de G DATA ANTIVIRUS for Mac. Puede imprimir o guardar el Acuerdo de Licencia y puede ver estos más tarde.

Por favor, lea el Acuerdo de Licencia cuidadosamente. Para continuar instalando el software debe aceptar los términos del acuerdo de licencia del software. Haga clic en **Continuar** y entonces **Aceptar**.



Importante

Si no acepta estos términos, haga clic en **Continuar** y después en **No aceptar** para cancelar la instalación y quitar el instalador.

1.2.4. Paso 4 - Iniciar la Instalación



G DATA ANTIVIRUS for Mac se instalará en Macintosh HD/Library/G DATA. Usted no puede cambiar la ruta de instalación.

Haga clic en **Instalar** para iniciar la instalación.

1.2.5. Paso 5 - Instalando G DATA ANTIVIRUS for Mac



Espere a que la instalación se complete y entonces haga clic en **Continuar**.

1.2.6. Paso 6 - Finalizar



Haga clic en **Cerrar** para cerrar la ventana del instalador. En la ventana de bienvenida que se abre una vez que se completa la instalación, puede seleccionar una de las siguientes opciones:

- **Comenzar evaluación:** le permite evaluar el producto por un período de 30 días.
- **Introducir clave:** le permite registrar una clave de licencia válida que ya tenga.
- **Ir a la tienda:** le lleva a la página Web de G DATA Software AG donde puede ver las ofertas disponibles o comprar una clave de licencia.

Para obtener más información sobre cada una de las opciones, consulte *Registro de G DATA ANTIVIRUS for Mac* (p. 32).

1.3. Eliminando G DATA ANTIVIRUS for Mac

Al ser una aplicación compleja, G DATA ANTIVIRUS for Mac puede ser eliminando de forma normal, arrastrando el icono de la aplicación de la carpeta de Aplicaciones a la Papelera.

Para eliminar G DATA ANTIVIRUS for Mac, siga estos pasos:

1. Abra una ventana del **Finder** y acceda a la carpeta de Aplicaciones.
2. Seleccione la carpeta de Utilidades.
3. Haga doble clic en el desinstalador de G DATA ANTIVIRUS for Mac para abrirlo.
4. Siga los pasos de desinstalación para completar el proceso y, a continuación, haga clic en **Cerrar** para finalizar.



Importante

Si hay un error, puede contactar con Atención al Cliente de G DATA ANTIVIRUS for Mac como se describe en *Soporte e Información de Contacto* (p. 37).

2. Iniciando

Este capítulo incluye los siguientes temas:

- *Acerca de G DATA ANTIVIRUS for Mac (p. 10)*
- *Abrir G DATA ANTIVIRUS for Mac (p. 10)*
- *Ventana Aplicación Principal (p. 11)*
- *Icono Aplicación Dock (p. 13)*

2.1. Acerca de G DATA ANTIVIRUS for Mac

G DATA ANTIVIRUS for Mac es un potente analizador antivirus que puede detectar y eliminar todo tipo de software malicioso ("malware"), incluyendo:

- virus
- spyware
- Caballos de Troya
- keyloggers
- gusanos
- adware

Esta aplicación detecta y elimina no solo malware de Mac, sino también malware de Windows, evitando por tanto que envíe accidentalmente archivos infectados a su familia, amigos y compañeros de trabajo que usen PCs.

2.2. Abrir G DATA ANTIVIRUS for Mac

Hay diferentes maneras de abrir G DATA ANTIVIRUS for Mac.

- Haga clic en el icono G DATA ANTIVIRUS for Mac en el Launchpad.
- Haga clic en el icono  en la barra de menú y seleccione **Abrir la ventana principal**.

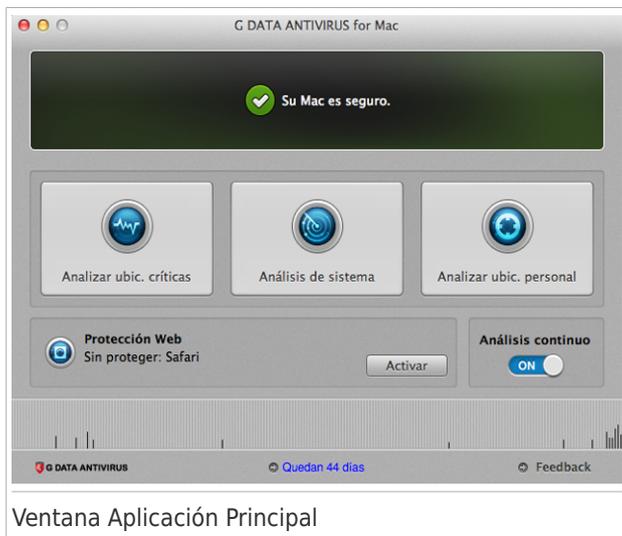
G DATA ANTIVIRUS for Mac

- Abra una ventana del Finder, acceda a Aplicaciones y haga doble clic en el icono G DATA ANTIVIRUS for Mac.

Alternativamente, puede utilizar Spotlight para encontrar y abrir la aplicación.

2.3. Ventana Aplicación Principal

En la ventana principal de la aplicación puede llevar a cabo importantes acciones para mejorar la protección de su sistema. Puede comprobar el estado de seguridad de su equipo, proteger su navegación Web o registrar el producto.



La barra de estado en la parte superior de la ventana le informa sobre el estado de seguridad del sistema mediante mensajes explícitos y colores asociados. Si G DATA ANTIVIRUS for Mac carece de avisos, la barra de estado exhibe tonos verdes.

Cuando se detecta un problema de seguridad, los tonos verdes de la barra de estado se sustituyen por tonos amarillos. También puede incluir un botón para ayudarle a solucionar rápidamente el problema. Para información detalla de incidencias y cómo repararlas, diríjase a [Reparar Incidencias \(p. 18\)](#).

Bajo la barra de estado, hay disponibles cuatro botones de análisis para ayudarle a analizar su Mac:

- **Analizar ubicaciones críticas** - comprueba en busca de malware las ubicaciones mas vulnerables en su sistema (por ejemplo, las carpetas que contienen los documentos, descargar, descargas de correo y archivos temporales de cada usuario).
- **Análisis completo del sistema** - realiza una comprobación exhaustiva en busca de malware en todo el sistema. Todos los dispositivos montados se analizarán también.
- **Analizar una ubicación personalizada** - le ayuda a comprobar archivos específicos, carpetas o volúmenes en busca de malware.
- **Análisis continuo** - monitoriza continuamente las aplicaciones que se están ejecutando en el equipo, buscando acciones sintomáticas del malware, y evita que entre nuevo malware en su sistema.

Para más información, diríjase a [Analizando Su Mac \(p. 15\)](#).

Además de los botones de análisis, existen ciertas opciones adicionales disponibles:

- **Protección Web** - filtra todo el tráfico Web y bloquea cualquier contenido malicioso para proteger su navegación en la Web. Para obtener más información, consulte [Protección Web \(p. 21\)](#).
- **Tipo de clave de licencia y número de días que quedan:** muestra el tipo de clave de licencia que está utilizando, de pago o de evaluación, y el tiempo que queda hasta que caduque su licencia actual. Haga clic en el enlace para abrir una pantalla donde puede ver más información sobre su clave de licencia o registrar su producto con una nueva clave.

- **Comentarios** - abre una nueva ventana en su cliente de correo electrónico predeterminado mediante el cual puede contactar con nosotros.

2.4. Icono Aplicación Dock

El icono de G DATA ANTIVIRUS for Mac puede verse en el Dock en cuanto abre la aplicación. El icono del Dock le proporciona una manera fácil para analizar archivos y carpetas en busca de malware. Simplemente arrastre y suelte el archivo o la carpeta en el icono del Dock y el análisis comenzará inmediatamente.



3. Protección contra Software Malicioso

Este capítulo incluye los siguientes temas:

- *Mejores Prácticas* (p. 14)
- *Analizando Su Mac* (p. 15)
- *Activar o desactivar el Análisis continuo* (p. 17)
- *Asistente del Análisis* (p. 17)
- *Reparar Incidencias* (p. 18)
- *Cuarentena* (p. 20)
- *Protección Web* (p. 21)
- *Actualizaciones* (p. 23)

3.1. Mejores Prácticas

Para mantener su sistema libre de malware y evitar la infección accidental de otros sistemas, siga estas recomendaciones:

- Tenga activado el **Análisis continuo**, para permitir que G DATA ANTIVIRUS for Mac analice los archivos del sistema.
- Mantenga G DATA ANTIVIRUS for Mac actualizado con las últimas firmas de malware y actualizaciones de producto, al tiempo que tiene activado el **Análisis continuo**.
- Compruebe y repare regularmente las incidencias reportadas por G DATA ANTIVIRUS for Mac. Para información detallada, diríjase a *Reparar Incidencias* (p. 18).
- Verifique el registro detallado de eventos relativos a la actividad de G DATA ANTIVIRUS for Mac en su equipo. Siempre que sucede algo relevante para la

seguridad de su sistema o de sus datos, se añade un nuevo mensaje al historial de G DATA ANTIVIRUS for Mac.

Para acceder a los registros del historial, siga estos pasos:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Realice una de estas acciones:
 - ▶ En la barra de menús, haga clic en G DATA ANTIVIRUS for Mac y elija **Mostrar historial**.
 - ▶ Pulse Comando-I.

Se muestra información detallada acerca de la actividad del producto.

- También debería seguir estas recomendaciones:
 - ▶ Acostúmbrase a analizar los archivos que descargue de una fuente de almacenamiento externa (como por ejemplo una memoria USB o un CD), especialmente cuando desconoce el origen de los mismos.
 - ▶ Si tiene un archivo DMG, móntelo y analice su contenido (los archivos del volumen/imagen montado).

La vía fácil para analizar un archivo, una carpeta o un volumen es arrastrando&oltando sobre la ventana de G DATA ANTIVIRUS for Mac o al icono del Dock.

No se requiere otra acción o configuración. Sin embargo, si lo desea, puede ajustar la configuración de la aplicación y las preferencias para satisfacer mejor sus necesidades. Para más información, diríjase a *Preferencias de Configuración (p. 26)*.

3.2. Analizando Su Mac

Puede analizar su Mac o archivos específicos en cualquier momento que desee.

La vía fácil para analizar un archivo, una carpeta o un volumen es arrastrando&oltando sobre la ventana de G DATA ANTIVIRUS for Mac o al icono

del Dock. El asistente de análisis aparecerá y le guiará a través del proceso de análisis.

También puede iniciar un análisis de la siguiente manera:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Haga clic en uno de los cuatro botones de análisis para iniciar el análisis deseado.
 - **Analizar ubicaciones críticas** - comprueba en busca de malware las ubicaciones mas vulnerables en su sistema (por ejemplo, las carpetas que contienen los documentos, descargar, descargas de correo y archivos temporales de cada usuario).
 - **Análisis completo del sistema** - realiza una comprobación exhaustiva en busca de malware en todo el sistema. Todos los dispositivos montados se analizarán también.



Nota

Dependiendo del tamaño de su disco duro, analizar todo el sistema puede tardar bastante (hasta una hora o incluso más). Para mejorar el rendimiento, se recomienda no ejecutar esta tarea mientras se estén llevando a cabo otras tareas que consuman muchos recursos (como por ejemplo la edición de vídeo). Si lo prefiere, puede escoger no analizar volúmenes montados determinados añadiéndolos a la lista de **Exclusiones** en la ventana de Preferencias.

- **Analizar una ubicación personalizada** - le ayuda a comprobar archivos específicos, carpetas o volúmenes en busca de malware.
- **Análisis continuo** - monitoriza continuamente las aplicaciones que se están ejecutando en el equipo, buscando acciones automáticas del malware, y evita que entre nuevo malware en su sistema.

3.3. Activar o desactivar el Análisis continuo

Para activar o desactivar el Análisis continuo, puede hacer lo siguiente:

- Abra G DATA ANTIVIRUS for Mac y haga clic en el conmutador para activar o desactivar el Análisis continuo.
- Haga clic en el icono  en la barra de menús y seleccione **Desactivar el Análisis continuo**.

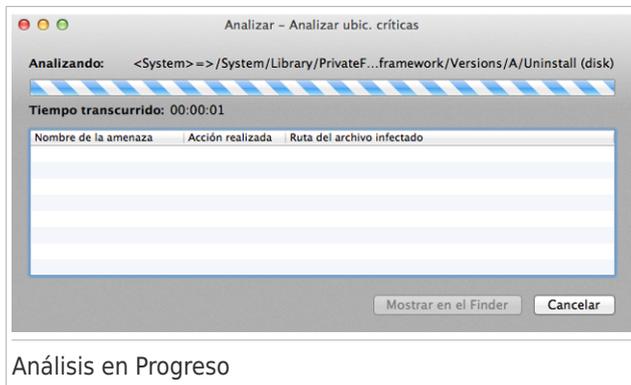


Aviso

Le recomendamos que desactive el Análisis continuo lo menos posible. Si desactiva el Análisis continuo, no estará protegido contra las amenazas de malware.

3.4. Asistente del Análisis

Cuando inicie una análisis, aparecerá el asistente de Análisis de G DATA ANTIVIRUS for Mac.



Puede ver información en tiempo real sobre el análisis. Las amenazas detectadas y la acción a realizar en estas se muestran en la sección Resultados de Análisis.

Espera a que G DATA ANTIVIRUS for Mac finalice el análisis.



Nota

El análisis puede llevar un tiempo, dependiendo de la complejidad del análisis.

3.5. Reparar Incidencias

G DATA ANTIVIRUS for Mac automáticamente detecta y le informa sobre una serie de incidencias que pueden afectar a la seguridad de su sistema y sus datos. De esta forma, puede evitar fácilmente y a tiempo riesgos para la seguridad.

La reparación de incidencias indicadas por G DATA ANTIVIRUS for Mac es una manera rápida y sencilla de asegurarse una magnífica protección de su sistema y de sus datos.

Los problemas detectados incluyen:

- Las nuevas firmas de malware y actualizaciones de producto no se descargaron de nuestros servidores, porque el **Análisis continuo** está desactivado.
- Se han detectado amenazas no resueltas en su sistema.
- **Análisis continuo** - está desactivado.

Para comprobar y reparar las incidencias detectadas:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Si G DATA ANTIVIRUS for Mac carece de avisos, la barra de estado exhibe tonos verdes. Cuando se detecta un problema de seguridad, los tonos verdes de la barra de estado se sustituyen por tonos amarillos.
3. Compruebe la descripción para más información.

4. Dependiendo del problema detectado, puede que haya un botón disponible en la barra de estado para ayudarle a solucionarlo rápidamente. Haga clic en el botón para eliminar el riesgo para la seguridad.

Normalmente, esto sucede cuando hay amenazas sin resolver. Puede verlas y decidir qué hacer con ellas.



Nota

G DATA ANTIVIRUS for Mac puede llevar a cabo acciones solo sobre los archivos del usuario actual. Esta app no puede limpiar ni poner en cuarentena los archivos infectados propiedad de otros usuarios. Se informará de tales archivos como incidencias sin resolver.

La lista de amenazas que no se pudieron desinfectar ni poner en cuarentena.

Número de amenazas: 1

Nombre de la amenaza	Ruta
EICAR-Test-File (not a virus)	/private/var/tmp/eicar.org

Mostrar el archivo en el Finder para que pueda tratar de borrarlo manualmente:

Añadir el archivo a la lista de Exclusiones y no volver a analizarlo nunca:
Puede gestionar las exclusiones desde la ventana de Preferencias.

Quitar el archivo de esta lista hasta el próximo análisis del sistema:

Ventana de amenazas no solucionadas

La lista de amenazas no solucionadas se actualiza después de cada análisis del sistema.

Puede escoger adoptar las siguientes medidas respecto a las amenazas no solucionadas:

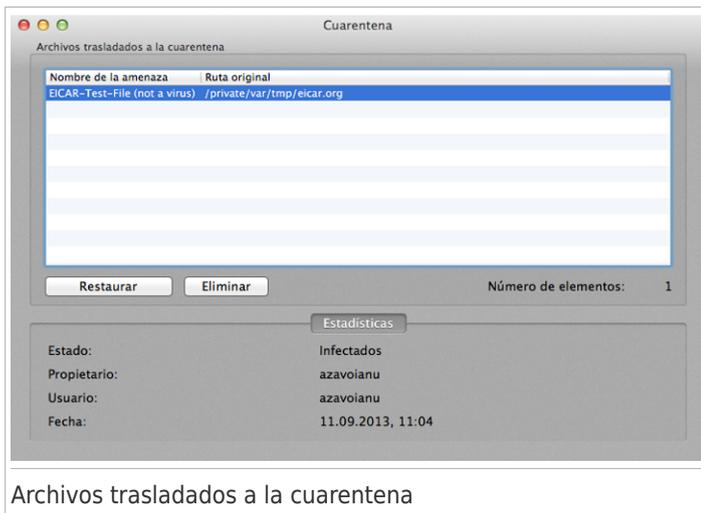
- Mostrar en el Finder. Lleve a cabo esta acción para eliminar manualmente las infecciones.
- Añadir a **Exclusiones**. Esta acción no está disponible para malware encontrado dentro de archivos comprimidos.
- Ignorar por ahora. El problema se eliminará de la barra de estado hasta el próximo análisis.

3.6. Cuarentena

G DATA ANTIVIRUS for Mac le permite aislar los archivos infectados o sospechosos en una área segura, llamada cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Para ver y gestionar los archivos en la cuarentena, abra la ventana de Cuarentena:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Haga clic en **Acciones** en la barra de menú.
3. Escoja **Ver cuarentena**.



El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena.

Para borrar un archivo de la cuarentena, selecciónelo y haga clic en **Eliminar**. Si desea restaurar un archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

3.7. Protección Web

G DATA ANTIVIRUS for Mac utiliza las extensiones Linkchecker para proteger completamente su navegación Web. Las extensiones Linkchecker interceptan, procesan y filtran todo el tráfico Web, bloqueando cualquier contenido malicioso.

Las extensiones funcionan y se integran con los siguientes navegadores: Mozilla Firefox, Google Chrome y Safari.

Hay toda una serie de funciones disponibles para protegerle frente a todo tipo de amenazas que pueda encontrar mientras navega por la Web:

- Filtro de phishing avanzado - evita que acceda a sitios Web empleados para ataques de phishing.
- Filtro de malware - bloquea cualquier malware con el que entre en contacto mientras navega por Internet.
- Analizador de resultados de búsqueda - proporciona una advertencia anticipada sobre sitios Web peligrosos presentes en sus resultados de búsquedas.
- Filtro antifraude - proporciona protección contra sitios Web fraudulentos mientras navega por Internet.
- Notificación de seguimiento - detecta mecanismos de seguimiento en las páginas Web que visita para proteger su privacidad online.

Habilitación de extensiones Linkchecker

Para habilitar las extensiones Linkchecker, siga los pasos siguientes:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Haga clic en **Activar** para activar la protección Web.
3. G DATA ANTIVIRUS for Mac detectará qué navegador tiene instalado en su sistema. Para instalar la extensión Linkchecker en su navegador, haga clic en **Obtener extensión**.
4. Será redirigido a esta ubicación online:
<https://www.gdatasoftware.com/linkchecker.html>
5. Seleccione **Descarga gratuita**.
6. Siga los pasos para instalar la extensión Linkchecker correspondiente a su navegador.

Calificación de páginas y alertas

Dependiendo de la clasificación que Linkchecker otorgue a la página Web que esté viendo, mostrará en su área uno de los iconos siguientes:



Esta página es segura. Puede seguir trabajando.



Esta página Web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.



Debería abandonar la página Web inmediatamente. Como alternativa, puede escoger una de las opciones disponibles:

- Abandonar el sitio Web haciendo clic en **Liévame a un sitio seguro.**
- Dirigirse al sitio Web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos.**

3.8. Actualizaciones

Cada día se encuentran nuevas amenazas de malware. Por esta razón es muy importante mantener G DATA ANTIVIRUS for Mac actualizado con las últimas firmas de malware.

Mantenga activado el **Análisis continuo** para que las firmas de malware y las actualizaciones de producto se descarguen automáticamente en su sistema. Si se detecta una actualización, esta es automáticamente descargada e instalada en su equipo.

La actualización de firmas de malware se realiza al instante, reemplazándose progresivamente los archivos a actualizar. De este modo, la actualización no afecta al funcionamiento del producto y, al mismo tiempo, se evita cualquier riesgo.

- Si G DATA ANTIVIRUS for Mac está actualizado, este puede detectar las últimas amenazas descubiertas y limpiar los archivos infectados.

- Si G DATA ANTIVIRUS for Mac no está actualizado, no podrá detectar y eliminar el último malware descubierto por los laboratorios de G DATA Software AG.

3.8.1. Solicitando una Actualización

Puede solicitar una actualización manualmente en cualquier momento. La actualización por el usuario se recomienda antes de iniciar un análisis exhaustivo.

Se requiere conexión a Internet con el fin de comprobar las actualizaciones disponibles y descargarlas.

Para solicitar una actualización manual:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Haga clic en **Acciones** en la barra de menú.
3. Elija **Base de datos de virus**.

Puede ver el progreso de actualización y archivos descargados.

3.8.2. Obteniendo Actualizaciones a través de un Servidor Proxy

G DATA ANTIVIRUS for Mac puede actualizar solo a través de servidores proxy que no requiere autenticación. No tiene que configurar ninguna configuración del programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar a una conexión directa a Internet con el fin de obtener las actualizaciones de las firmas de malware.

3.8.3. Actualice a una nueva versión

Ocasionalmente, lanzamos actualizaciones del producto para solucionar problemas del mismo. Estas actualizaciones podrían requerir un reinicio del sistema para dar paso a la instalación de nuevos archivos. De forma predeterminada, si una actualización precisa un reinicio del equipo, G DATA ANTIVIRUS for Mac seguirá

funcionando con los archivos anteriores hasta que se reinicie el sistema. Así, el proceso de actualización no interferirá con el trabajo del usuario.

Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si no lee esta notificación, puede también hacer clic en **Reiniciar para actualizar** en la barra de menús o reiniciar manualmente el sistema.

4. Preferencias de Configuración

Este capítulo incluye los siguientes temas:

- *Preferencias de Acceso* (p. 26)
- *Preferencias Generales* (p. 26)
- *Preferencias de análisis* (p. 27)
- *Exclusiones del Análisis* (p. 30)

4.1. Preferencias de Acceso

Para abrir la ventana de Preferencias de G DATA ANTIVIRUS for Mac:

1. Abrir G DATA ANTIVIRUS for Mac.
2. Realice una de estas acciones:
 - Haga clic en la barra de menú de G DATA ANTIVIRUS for Mac y escoja **Preferencias**.
 - Haga clic en el icono  de la barra de menús y seleccione **Preferencias**.
 - Presione el comando coma(,).

4.2. Preferencias Generales

Las preferencias generales le permiten configurar el comportamiento general de la aplicación.



- **Activar notificaciones.** Le permite recibir notificaciones sobre actividades y eventos de G DATA ANTIVIRUS for Mac. En sistemas 10.8 y posteriores se le notificará automáticamente a través del Centro de notificaciones. En sistemas 10.7 se le notificará en Growl, si está instalada la aplicación. Si no ha instalado Growl, recibirá notificaciones mediante el mecanismo de notificación de G DATA ANTIVIRUS for Mac. La integración con Growl es una opción extra y no afecta de ninguna manera a su producto G DATA ANTIVIRUS for Mac.

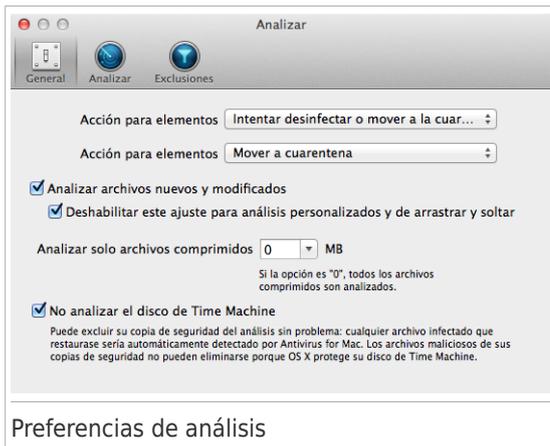


Nota

Growl es una aplicación de terceros desarrollada por The Growl Project. No está instalado por defecto en Mac OS X. Puede encontrar más información y descargar Growl desde <http://growl.info/>.

4.3. Preferencias de análisis

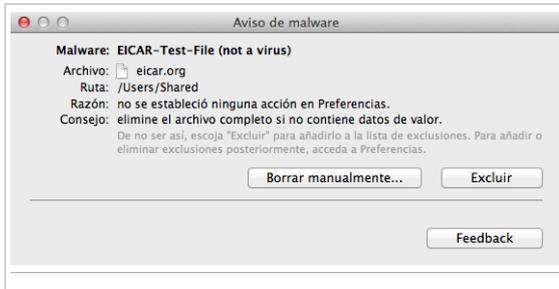
Las preferencias de análisis le permiten configurar el procedimiento general de análisis. Puede configurar las acciones a realizar en los archivos infectados y sospechosos detectados y otros ajustes generales.



- **Acción para elementos infectados.** Cuando detecta un virus u otro malware, G DATA ANTIVIRUS for Mac intentará eliminar automáticamente el código malware del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección. Los archivos que no pueden desinfectarse se trasladan a la **cuarentena** para contener la infección.

Aunque no se recomienda, puede establecer que la aplicación no haga nada con los archivos infectados. Los archivos detectados solo se mencionan en el registro.

El Análisis continuo asegura una buena protección contra el malware, con un impacto menor en el rendimiento del sistema. Si hay amenazas sin resolver, puede verlas y decidir qué hacer con ellas.



- **Acción para elementos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

De forma predeterminada, los archivos sospechosos se trasladan a la cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Si lo prefiere, puede escoger ignorar los archivos sospechosos. Los archivos detectados solo se mencionan en el registro.

- **Analizar archivos nuevos y modificados.** Seleccione esta casilla para que G DATA ANTIVIRUS for Mac analice sólo archivos que no han sido analizados antes o estos han sido modificados desde el último análisis.

Puede elegir no aplicar esta opción de análisis arrastrar& soltar seleccionando la correspondiente casilla.

- **Analizar solo archivos comprimidos de menos de {0} MB.** Utilice esta opción para optimizar el proceso de análisis excluyendo del mismo los archivos comprimidos más grandes.



Nota

El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

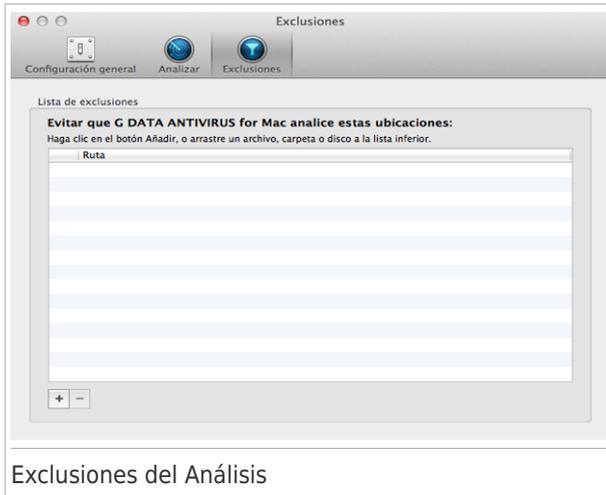
Especifique el tamaño máximo de los archivos a analizar (en megabytes) en la campo correspondiente. Los archivos que excedan del tamaño límite especificado no serán analizados. Si desea analizar todos los archivos comprimidos, independientemente de su tamaño, introduzca el valor 0.

- **No analizar el disco de Time Machine.** Seleccione esta casilla de verificación para excluir del análisis los archivos de copia de seguridad. Si posteriormente restaurase archivos infectados, G DATA ANTIVIRUS for Mac los detectaría automáticamente y adoptaría las medidas apropiadas.

4.4. Exclusiones del Análisis

Si así lo desea, puede hacer que G DATA ANTIVIRUS for Mac no analice ciertos archivos, carpetas o incluso un volumen entero. Por ejemplo, quizá querría excluir del análisis:

- Archivos que han sido identificados por error como infectados (conocidos como falsos positivos)
- Archivos que provocan errores de análisis
- Hacer copia de seguridad de los volúmenes



Exclusiones del Análisis

La lista de exclusiones contiene las rutas que han sido omitidas para el análisis. Existen dos modos de establecer una exclusión de análisis:

- Arrastrar y soltar un archivo, carpeta o volumen sobre la lista de exclusiones.
- Haga clic en el botón etiquetado con el signo más (+), ubicado bajo la lista de exclusiones. Luego, escoja el archivo, carpeta o volumen a excluir del análisis.

Para eliminar una exclusión de análisis, selecciónela en la lista y haga clic en el botón etiquetado con el signo menos (-), ubicado bajo la lista de exclusiones.

5. Registro de G DATA ANTIVIRUS for Mac

Este capítulo incluye los siguientes temas:

- *Sobre el Registro (p. 32)*
- *Registro de G DATA ANTIVIRUS for Mac (p. 32)*
- *Adquiera una Licencia (p. 33)*

5.1. Sobre el Registro

G DATA ANTIVIRUS for Mac incluye un periodo de evaluación de 30 días. Durante el período de evaluación, el producto es completamente funcional y lo puede probar para ver si cumple con sus expectativas.

Debe registrar el producto con una licencia después de que finalice el periodo de prueba. El número de licencia indica por cuánto tiempo puede utilizar el producto. Cuando el número de licencia caduca, G DATA ANTIVIRUS for Mac deja de realizar sus funciones y de proteger su equipo.

Debe comprar una clave de licencia o renovar su licencia unos días antes de que caduque la licencia actual. En la parte inferior de la interfaz de G DATA, haga clic en el enlace que indica el número de días que quedan para ver información acerca de su suscripción.

5.2. Registro de G DATA ANTIVIRUS for Mac

Se requiere una conexión a Internet para registrar G DATA ANTIVIRUS for Mac.

Para registrar G DATA ANTIVIRUS for Mac:

1. Abrir G DATA ANTIVIRUS for Mac.
2. En la parte inferior de la ventana de G DATA ANTIVIRUS for Mac aparece un enlace que indica el número de días que le quedan a su licencia. Haga clic en este enlace para abrir la ventana de registro.



3. Haga clic en **Cambiar serie** e introduzca su clave de licencia.

4. Haga clic en **Activar** para registrar su nueva licencia.

Después de completar el registro, puede ver la nueva información de registro en la ventana de registro.

5.3. Adquiera una Licencia

Cuando su versión de prueba o el periodo de la licencia finaliza, adquiera una licencia para registrar G DATA ANTIVIRUS for Mac y extienda la protección.

Para adquirir una licencia:

1. Abrir G DATA ANTIVIRUS for Mac.

2. En la parte inferior de la ventana de G DATA ANTIVIRUS for Mac aparece un enlace que indica el número de días que le quedan a su licencia.

Haga clic en este enlace para abrir la ventana de registro.

3. Haga clic en el botón **Compre una licencia**.

4. Siga las instrucciones de la página web para adquirir una licencia.

6. Preguntas frecuentes

El registro de análisis indica que todavía hay elementos sin resolver. ¿Cómo los elimino?

Los elementos sin resolver en el registro de análisis pueden ser:

- archivos de acceso restringido (xar, rar, etc.)

Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y borrarlo manualmente. Asegúrese de vaciar la Papelera.

- buzones de correo de acceso restringido (Thunderbird, etc.)

Solución: Utilice la aplicación para eliminar la entrada que contiene el archivo infectado.

- archivos pertenecientes a otro usuario

Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y contactar con el propietario para averiguar si es seguro eliminar ese archivo. Si es seguro eliminar el archivo, bórralo manualmente. Asegúrese de vaciar la Papelera.



Nota

Se entiende por archivos de acceso restringido aquellos que G DATA ANTIVIRUS for Mac solo puede abrir, pero no puede modificar.

¿Dónde puedo leer información detallada sobre la actividad del producto?

G DATA ANTIVIRUS for Mac mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para acceder a esta información, siga estos pasos:

1. Abrir G DATA ANTIVIRUS for Mac.

2. Realice una de estas acciones:

- En la barra de menús, haga clic en G DATA ANTIVIRUS for Mac y elija **Mostrar historial**.

- Pulse Comando-I.

Se muestra información detallada acerca de la actividad del producto.

¿Puedo actualizar G DATA ANTIVIRUS for Mac a través de un servidor proxy?

G DATA ANTIVIRUS for Mac se puede actualizar solo a través de servidores proxy que no requieran autenticación. No tiene que configurar ningún ajuste de programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar a una conexión directa a Internet con el fin de obtener las actualizaciones de las firmas de malware.

¿Cómo elimino las extensiones Linkchecker de mi navegador?

- Para eliminar las extensiones Linkchecker de Mozilla Firefox, siga los pasos siguientes:
 1. Abra su navegador Mozilla Firefox.
 2. Vaya a **Herramientas** y seleccione **Complementos**.
 3. Seleccione **Extensiones** en la columna izquierda.
 4. Seleccione las extensiones y haga clic en **Eliminar**.
 5. Reinicie el navegador para completar el proceso de eliminación.
- Para eliminar las extensiones Linkchecker de Google Chrome, siga los pasos siguientes:
 1. Abra su navegador Google Chrome.
 2. Haga clic en  en la barra de herramientas del navegador.
 3. Vaya a **Herramientas** y seleccione **Extensiones**.
 4. Seleccione las extensiones y haga clic en **Eliminar**.

5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.
- Para eliminar las extensiones Linkchecker de Safari, siga los pasos siguientes:
 1. Abra su navegador Safari.
 2. Haga clic en  en la barra de herramientas del navegador y haga clic en **Preferencias**.
 3. Seleccione la pestaña **Extensiones** y localice en la lista la extensión **G DATA Linkchecker en Safari**.
 4. Seleccione la extensión y haga clic en **Desinstalar**.
 5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.

7. Soporte e Información de Contacto

Si necesita ayuda o información adicional no dude en ponerse en contacto con nosotros.

G DATA Software AG

Koenigsallee 178 b
44799 Bochum

Teléfono: +49 234 / 97 62 - 0

Fax: +49 234 / 97 62 - 298

Página Web: <http://www.gdata.es>

Comprar: <http://www.gdata.es>

FAQ: <https://www.gdatasoftware.com/support.html>

Soporte Técnico: <https://www.gdatasoftware.com/support.html>

Tipos de Software Malicioso

Adware

El Adware habitualmente se combina con aplicaciones que son gratuitas a cambio que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan después que el usuario acepte los términos de licencia que declaran el propósito de la aplicación, no se comete ningún delito. Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar preocupación acerca de su privacidad a aquellos usuarios que no son plenamente conscientes de los términos de la licencia.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede agregar a otros programas.

Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers no son maliciosos por naturaleza. Pueden utilizarse para propósitos legítimos, como la vigilancia de empleados o de la actividad de sus hijos. Sin embargo, son cada vez más utilizados por los cibercriminales con fines ilegales (por ejemplo, para recoger los datos privados, tales como credenciales de acceso y números de identificación).

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricos, si éstos incorporan el software apropiado.

Los rootkits no son maliciosos por naturaleza. Por ejemplo, los sistemas operativos y algunas aplicaciones esconden sus archivos críticos mediante rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar archivos o logs, y evitar su detección.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al Troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio

de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del Spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de Troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.