



Kaspersky Anti-Virus

Guía del usuario

Versión de la aplicación: 16.0 Maintenance Release 1

Estimado usuario:

Gracias por elegir nuestro producto. Esperamos que este documento le ayude en su trabajo y le proporcione respuestas sobre este producto de software.

Atención. El presente documento es propiedad de AO Kaspersky Lab (en adelante también denominado Kaspersky Lab): todos los derechos del presente documento están reservados por la normativa de copyright de la Federación Rusa y por los tratados internacionales. La reproducción y distribución ilícitas de este documento o de cualquiera de sus partes tendrá las repercusiones civiles, administrativas y penales establecidas por la legislación aplicable.

Cualquier tipo de reproducción o distribución de los materiales, incluidas las traducciones, requiere un permiso por escrito de Kaspersky Lab.

Este documento y las imágenes gráficas relacionadas con él solo pueden utilizarse con fines informativos, personales y no comerciales.

Kaspersky Lab se reserva el derecho a modificar este documento sin previo aviso. Puede encontrar la última versión de este documento en el sitio Web de Kaspersky Lab, en <http://www.kaspersky.com/sp/docs>.

Kaspersky Lab no se responsabiliza del contenido, calidad, pertinencia o veracidad de los materiales utilizados en este documento cuyos derechos sean propiedad de terceros, ni de los posibles perjuicios asociados al uso de dichos documentos.

Fecha de revisión del documento: 30/11/2015

© 2015 AO Kaspersky Lab. Todos los derechos reservados.

<http://www.kaspersky.es>

<https://help.kaspersky.com/es>

<http://support.kaspersky.com/sp>

Tabla de Contenidos

Acerca de esta guía	7
En esta Guía.....	7
Convenciones del documento	11
Fuentes de información en relación con la aplicación	13
Fuentes de información para una investigación independiente	13
Discusiones sobre las aplicaciones de Kaspersky Lab en el foro.....	15
Kaspersky Anti-Virus.....	16
Acerca de Kaspersky Anti-Virus	16
Novedades	19
Kit de distribución	19
Requisitos de hardware y software.....	20
Instalación y eliminación de la aplicación	22
Procedimiento de instalación estándar	22
Paso 1. Búsqueda de una versión más reciente de la aplicación.....	24
Paso 2. Inicio de la instalación de la aplicación.....	24
Paso 3. Revisión del contrato de licencia	25
Paso 4. Declaración de Kaspersky Security Network.....	25
Paso 5. Instalación	25
Paso 6. Finalización de la instalación.....	27
Paso 7. Activación de la aplicación	27
Paso 8. Registro de un usuario	28
Paso 9. Finalización de la activación.....	28
Instalación de la aplicación desde la línea de comandos	28
Primeros pasos.....	29
Actualización de una versión anterior de la aplicación	30
Paso 1. Búsqueda de una versión más reciente de la aplicación.....	32
Paso 2. Inicio de la instalación de la aplicación.....	32
Paso 3. Revisión del contrato de licencia	33
Paso 4. Declaración de Kaspersky Security Network.....	33
Paso 5. Instalación	34
Paso 6. Finalización de la instalación.....	35

Cambio de Kaspersky Anti-Virus a Kaspersky Internet Security o Kaspersky Total Security.....	35
Uso temporal de Kaspersky Internet Security	37
Cambio al uso permanente de Kaspersky Internet Security.....	39
Eliminación de la aplicación.....	39
Paso 1. Introducción de la contraseña para desinstalar la aplicación	40
Paso 2. Almacenamiento de datos para su uso posterior	40
Paso 3. Confirmación de la eliminación de la aplicación	42
Paso 4. Eliminación de la aplicación. Completando eliminación	42
Licencias de la aplicación	43
Acerca del Contrato de licencia de usuario final.....	43
Acerca de la licencia.....	44
Acerca del modo de funcionalidad limitada	45
Acerca del código de activación	47
Acerca de la suscripción.....	48
Acerca de la provisión de datos.....	49
Compra de una licencia	50
Activación de la aplicación.....	51
Renovación de una licencia	52
Solución de problemas del sistema operativo después de una infección	53
Recuperación del sistema operativo después de una infección	53
Solución de problemas del sistema operativo mediante el asistente de solución de problemas de Microsoft Windows	54
Acerca de Kaspersky Rescue Disk.....	56
Administración de las notificaciones de la aplicación	57
Evaluación de los problemas de protección del equipo y resolución de los problemas de seguridad	58
Actualización de las bases de datos y los módulos de la aplicación	59
Acerca de las actualizaciones de las bases de datos y los módulos de la aplicación.....	59
Inicio de una actualización de las bases de datos y los módulos de la aplicación	61
Análisis del equipo	62
Análisis completo.....	62
Análisis selectivo	63

Análisis rápido	64
Análisis de vulnerabilidades	65
Restauración de un objeto que la aplicación ha eliminado o desinfectado	66
Configuración de Antivirus de correo	67
Protección de datos personales en Internet.....	69
Acerca de la protección de datos personales en Internet.....	69
Acerca del Teclado en pantalla	70
Inicio del Teclado en pantalla	72
Comprobación de seguridad de un sitio web.....	73
Eliminación de rastros de actividad en el equipo y en Internet	76
Gestión remota de la protección del equipo.....	79
Información sobre la gestión remota de la protección del equipo	79
Acerca de cuenta My Kaspersky	80
Acceso a la gestión remota de la protección del equipo.....	81
Reserva de los recursos del sistema operativo para videojuegos	82
Acceso protegido con contraseña a las opciones de administración de Kaspersky Anti-Virus	83
Suspensión y reanudación de la protección del equipo	84
Restablecimiento de los parámetros predeterminados de la aplicación	86
Visualización del informe acerca del funcionamiento de una aplicación.....	87
Aplicación de la configuración de la aplicación en otro equipo	88
Participación en Kaspersky Security Network (KSN).....	90
Activar y desactivar la participación en Kaspersky Security Network	90
Comprobación de la conexión a Kaspersky Security Network.....	91
Participación en el programa Proteger a un amigo.....	93
Crear una cuenta en portal My Kaspersky.....	94
Iniciar sesión en su perfil del programa Proteger a un amigo	95
Uso de la aplicación desde la línea de comandos	96
Cómo ponerse en contacto con el servicio de Soporte técnico	97
Cómo conseguir soporte técnico	97

Soporte técnico por teléfono	98
Obtención de soporte técnico en el portal de My Kaspersky	98
Recopilación de información para Soporte técnico.....	99
Creación de un informe de estado del sistema	100
Envío de archivos de datos	101
Contenido y almacenamiento de archivos de depuración	102
Ejecución de scripts de AVZ.....	103
Limitaciones y advertencias.....	104
Glosario	109
AO Kaspersky Lab.....	120
Información sobre el código de terceros.....	122
Información de marcas registradas.....	123
Índice	124

Acerca de esta guía

Este documento es la Guía del usuario de Kaspersky Anti-Virus 2016 (en adelante, Kaspersky Anti-Virus).

Para una utilización adecuada de Kaspersky Anti-Virus, debe estar familiarizado con la interfaz del sistema operativo que utiliza, manejar las principales técnicas específicas de ese sistema, y saber trabajar con el correo electrónico y con Internet.

Este Guía proporciona instrucciones sobre:

- La preparación de Kaspersky Anti-Virus para instalación, la instalación y la activación de la aplicación
- La configuración y la utilización de Kaspersky Anti-Virus

Este Guía también enumera fuentes de información sobre la aplicación y formas de obtener el soporte técnico.

En esta sección

En esta Guía	7
Convenciones del documento	11

En esta Guía

Este documento contiene las siguientes secciones:

Fuentes de información sobre la aplicación (consulte la página [13](#))

Esta sección enumera las fuentes de información sobre la aplicación.

Puede seleccionar la fuente de información más adecuada, en función del nivel de importancia y urgencia del problema.

Kaspersky Anti-Virus (consulte la página [16](#))

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Anti-Virus, y proporciona una lista de requisitos de hardware y software de Kaspersky Anti-Virus.

Instalación y eliminación de la aplicación (consulte la página [22](#))

Esta sección contiene instrucciones paso a paso sobre cómo instalar y eliminar Kaspersky Anti-Virus.

Licencias de la aplicación (consulte la página [43](#))

Esta sección abarca los aspectos principales de las licencias de la aplicación.

Administración de las notificaciones de la aplicación (consulte la página [57](#))

Esta sección proporciona información sobre cómo gestionar notificaciones de la aplicación.

Evaluación de los problemas de protección del equipo y resolución de los problemas de seguridad (consulte la página [58](#))

Esta sección proporciona información sobre cómo evaluar el estado de seguridad del equipo y corregir las amenazas para la seguridad.

Actualización de las bases de datos y los módulos de la aplicación (consulte la página [59](#))

Esta sección contiene instrucciones paso a paso sobre cómo actualizar las bases de datos y módulos de la aplicación.

Análisis del equipo (consulte la página [62](#))

Esta sección contiene instrucciones paso a paso sobre cómo analizar su equipo en busca de virus, software malicioso y vulnerabilidades.

Restauración de un objeto que la aplicación ha eliminado o desinfectado (consulte la página [66](#))

Esta sección contiene instrucciones paso a paso sobre cómo restaurar un objeto que se ha eliminado o desinfectado.

Solución de problemas del sistema operativo después de una infección (consulte la página [53](#))

Esta sección proporciona información sobre cómo restaurar el sistema operativo después de que se haya infectado con virus.

Configuración de Antivirus de correo (consulte la página [67](#))

Esta sección contiene instrucciones sobre cómo configurar Antivirus de correo.

Protección de datos personales en Internet (consulte la página [69](#))

Esta sección proporciona información sobre cómo hacer su navegación en Internet segura y proteger sus datos contra robos.

Protección de transacciones financieras y compras en línea

Esta sección ofrece instrucciones sobre cómo puede proteger las transacciones financieras y las compras en línea con Kaspersky Anti-Virus.

Eliminación de rastros de actividad en el equipo y en Internet (consulte la página [76](#))

Esta sección proporciona información sobre cómo borrar rastros de la actividad del usuario en el equipo.

Gestión remota de la protección del equipo (consulte la página [79](#))

Esta sección describe cómo puede gestionar la protección de su equipo de forma remota mediante el portal My Kaspersky.

Reserva de los recursos del sistema operativo para videojuegos (consulte la página [82](#))

Esta sección contiene instrucciones paso a paso sobre cómo mejorar el rendimiento del sistema operativo para los videojuegos y otras aplicaciones.

Acceso protegido con contraseña a Kaspersky Anti-Virus (consulte la página [83](#))

Esta sección contiene instrucciones sobre cómo proteger la configuración de la aplicación con una contraseña.

Suspensión y reanudación de la protección del equipo (consulte la página [84](#))

Esta sección contiene instrucciones paso a paso sobre cómo activar y desactivar la aplicación.

Restablecimiento de los parámetros predeterminados de la aplicación (consulte la página [86](#))

Esta sección contiene instrucciones sobre cómo restaurar la configuración predeterminada de la aplicación.

Visualización del informe acerca del funcionamiento de la aplicación (consulte la página [87](#))

Esta sección contiene instrucciones sobre cómo ver informes de la aplicación.

Aplicación de la configuración de la aplicación en otro equipo (consulte la página [88](#))

Esta sección proporciona información sobre cómo exportar la configuración de la aplicación y aplicarla en otro equipo.

Participación en Kaspersky Security Network (consulte la página [90](#))

Esta sección proporciona información sobre Kaspersky Security Network y cómo participar en Kaspersky Security Network.

Participación en el programa Proteger a un amigo program (consulte la página [93](#))

Esta sección proporciona información sobre el programa Proteger a un amigo, que le permite acumular puntos de bonificación y recibir descuentos para las aplicaciones de Kaspersky Lab.

Uso de la aplicación desde la línea de comandos (consulte la página [96](#))

Esta sección proporciona información sobre cómo controlar la aplicación mediante la línea de comandos.

Asistencia del Soporte Técnico de Kaspersky Lab (consulte la página [97](#))

Esta sección describe las formas de obtener soporte técnico y las condiciones según las cuales está disponible.

Limitaciones y advertencias (consulte la página [104](#))

Esta sección describe las limitaciones que no son esenciales para el funcionamiento de la aplicación.

Glosario (consulte la página [109](#))

Esta sección contiene una lista de términos que se mencionan en el documento y sus respectivas definiciones.

AO Kaspersky Lab (consulte la página [120](#))

Esta sección ofrece información sobre AO Kaspersky Lab.

Información sobre el código de terceros (consulte la página [122](#))

Esta sección ofrece información sobre el código de otro fabricante que se usa en la aplicación.

Información de marcas registradas (consulte la página [123](#))

Esta sección incluye una lista de marcas registradas de otros fabricantes que se utilizan en este documento.

Índice

Esta sección permite encontrar rápidamente la información requerida dentro del documento.

Convenciones del documento

Este documento utiliza las convenciones siguientes (consulte la tabla a continuación).

Tabla 1. Convenciones del documento

Texto de muestra	Descripción de la convención de documento
Tenga en cuenta que...	Las advertencias se resaltan en rojo y se encuadran. Las advertencias muestran información sobre las acciones que pueden tener consecuencias no deseadas.
Le recomendamos que utilice...	Las notas se encuadran. Las notas proporcionan información adicional y de referencia.
Ejemplo:	Los ejemplos se muestran en un fondo azul claro bajo el título "Ejemplo".

Texto de muestra	Descripción de la convención de documento
<p><i>Actualización</i> significa que...</p> <p>Se produce el evento <i>Las bases de datos están desactualizadas</i>.</p>	<p>Los siguientes elementos aparecen en cursiva en el texto:</p> <ul style="list-style-type: none"> • Nuevos términos • Nombres de estados y eventos de la aplicación
<p>Pulse INTRO.</p> <p>Pulse ALT+F4.</p>	<p>Los nombres de las teclas del teclado aparecen en negrita y en mayúsculas.</p> <p>Los nombres de las teclas conectadas mediante un signo + (más) indican el uso de una combinación de teclas. Dichas teclas se deben pulsar de forma simultánea.</p>
<p>Haga clic en el botón Activar.</p>	<p>Los nombres de los elementos de la interfaz de la aplicación, como campos de entrada, elementos de menú y botones, se resaltan en negrita.</p>
<p>► <i>Para configurar una planificación de tareas:</i></p>	<p>Las frases introductorias de las instrucciones se muestran en cursiva y están acompañadas de la señal de flecha.</p>
<p>En la línea de comandos, escriba <code>help</code>.</p> <p>Aparecerá el siguiente mensaje:</p> <p>Especifique la fecha con el formato <code>dd:mm:aa</code>.</p>	<p>Los siguientes tipos de contenido de texto se resaltan con una fuente especial:</p> <ul style="list-style-type: none"> • Texto en la línea de comandos • Texto de los mensajes que la aplicación muestra en pantalla • Datos que se introducirán usando el teclado
<p><Nombre de usuario></p>	<p>Las variables se enmarcan entre corchetes angulares. En lugar de la variable, inserte el valor correspondiente, sin incluir los corchetes angulares.</p>

Fuentes de información en relación con la aplicación

Esta sección enumera las fuentes de información sobre la aplicación.

Puede seleccionar la fuente de información más adecuada, en función del nivel de importancia y urgencia del problema.

En esta sección

Fuentes de información para una investigación independiente	13
Discusiones sobre las aplicaciones de Kaspersky Lab en el foro	15

Fuentes de información para una investigación independiente

Puede utilizar las siguientes fuentes de información sobre Kaspersky Anti-Virus para investigar usted mismo:

- Página de Kaspersky Anti-Virus en el sitio web de Kaspersky Lab
- Página de Kaspersky Anti-Virus en el sitio web de Soporte técnico (Base de conocimientos)
- Ayuda en línea
- Documentación

Si no encuentra la solución al problema, le recomendamos ponerse en contacto con el servicio de Soporte Técnico de Kaspersky Lab (consulte la sección "Soporte técnico por teléfono" en la página [97](#)).

Se requiere conexión a Internet para utilizar fuentes de información en los sitios web.

Página de Kaspersky Anti-Virus en el sitio web de Kaspersky Lab

En la página de Kaspersky Anti-Virus

(<http://www.kaspersky.es/software-antivirus-domestico/antivirus>), puede ver información general acerca de la aplicación, sus funciones y características.

La página de Kaspersky Anti-Virus contiene un vínculo a la tienda en línea. Desde ahí, podrá comprar o renovar la aplicación.

Página de Kaspersky Anti-Virus en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de Soporte técnico.

En la página de Kaspersky Anti-Virus de la Base de conocimientos

(<http://support.kaspersky.com/sp/kav2016>), puede leer artículos que ofrecen información útil y recomendaciones, además de respuestas a preguntas frecuentes sobre la manera de comprar, instalar y usar la aplicación.

Los artículos de la Base de conocimientos pueden proporcionar respuestas a las preguntas relacionadas con Kaspersky Anti-Virus y otras aplicaciones de Kaspersky Lab. Los artículos de la Base de conocimientos también pueden contener novedades de Soporte técnico.

Ayuda en línea

La aplicación incluye ayuda completa y ayuda contextual.

La ayuda completa proporciona la información acerca de cómo configurar y usar Kaspersky Anti-Virus.

La ayuda contextual proporciona información sobre las ventanas de Kaspersky Anti-Virus, describe la configuración de Kaspersky Anti-Virus y contiene vínculos a descripciones de las tareas en las que se utiliza dicha configuración.

La ayuda puede encontrarse en el kit de distribución o en el recurso web de Kaspersky Lab. Si está disponible la ayuda en línea, se abrirá una ventana de navegador al acceder a ella. Se requiere conexión a Internet para ver la ayuda en línea.

Documentación

La guía del usuario de la aplicación ofrece información sobre cómo instalar, activar y configurar la aplicación, así como información sobre su funcionamiento. El documento también describe la interfaz de la aplicación y las diferentes formas de llevar a cabo las tareas típicas del usuario cuando se trabaja con la aplicación.

Discusiones sobre las aplicaciones de Kaspersky Lab en el foro

Si su pregunta no requiere una respuesta inmediata, puede compartirla con los expertos de Kaspersky Lab y con otros usuarios en nuestro foro

(<http://forum.kaspersky.com/index.php?showforum=45>).

En el foro puede ver los temas existentes, dejar sus comentarios y crear nuevos temas.

Kaspersky Anti-Virus

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Anti-Virus, y proporciona una lista de requisitos de hardware y software de Kaspersky Anti-Virus.

En esta sección

Acerca de Kaspersky Anti-Virus	16
Novedades.....	19
Kit de distribución.....	19
Requisitos de hardware y software	20

Acerca de Kaspersky Anti-Virus

Kaspersky Anti-Virus proporciona la protección completa contra diversos tipos de amenazas de la seguridad de la información. Con el fin de proporcionar esta protección completa, se encuentran disponibles como parte de Kaspersky Anti-Virus varias funciones y componentes de protección.

Protección del equipo

Los *Componentes de protección* se han diseñado para proteger el equipo de varios tipos de amenazas de seguridad de la información, ataques de red y de phishing. Un componente de protección individual se encarga de gestionar cada tipo de amenaza (consulte la descripción de los componentes en esta sección). Los componentes se pueden activar o desactivar de forma independiente y es posible configurar su configuración.

Además de la protección en tiempo real que proporcionan los componentes de seguridad, le recomendamos que *analice* con regularidad su equipo en busca de virus y otro software malicioso. Esto es necesario para evitar la propagación de programas maliciosos que no hayan detectado los componentes de protección como consecuencia de un bajo nivel de seguridad o por otros motivos.

Para mantener actualizado Kaspersky Anti-Virus, tendrá que *actualizar* las bases de datos y los módulos de la aplicación.

Algunas tareas específicas que deberían ejecutarse ocasionalmente (como la eliminación de rastros de la actividad de un usuario determinado en el sistema operativo) se ejecutan mediante *herramientas y asistentes avanzados*.

Los siguientes componentes de protección se encargarán de vigilar su equipo en tiempo real:

A continuación, encontrará una descripción de la lógica de cómo los componentes de la protección interactúan cuando se ha establecido Kaspersky Anti-Virus en el modo recomendado por los especialistas de Kaspersky Lab (es decir, con los ajustes predeterminados de la aplicación).

Antivirus de archivos

El componente Antivirus de archivos protege el equipo frente a la infección del sistema de archivos. Este componente se ejecuta al iniciarse el sistema operativo, permanece activo todo el tiempo en la memoria RAM del equipo y analiza todos los archivos que se abren, guardan o inician en el equipo y en todas las unidades conectadas. Kaspersky Anti-Virus intercepta todos los intentos de acceso a un archivo y lo analiza en busca de virus y software malicioso conocidos. Solo se permite el acceso al archivo si no está infectado o si la aplicación lo desinfecta correctamente. Si, por cualquier motivo, no se puede desinfectar un archivo, se elimina. Cuando sucede esto, se mueve una copia del archivo a Cuarentena. Si se coloca un archivo infectado en la misma ubicación donde estaba el archivo borrado del mismo nombre, Cuarentena guarda solo una copia del último archivo. No se guarda una copia del archivo anterior con el mismo nombre.

Antivirus de correo

El componente Antivirus de correo analiza los mensajes de correo electrónico entrantes y salientes del equipo. El destinatario solo podrá recibir mensajes de correo electrónico si no contienen objetos peligrosos.

Antivirus Internet

El componente Antivirus Internet intercepta y bloquea la ejecución de scripts de los sitios web si suponen una amenaza. Este componente también supervisa todo el tráfico web y bloquea el acceso a sitios web peligrosos.

Antivirus para chat

El componente Antivirus para chat garantiza el uso seguro de los clientes de MI. Este componente protege la información que llegue al equipo a través de protocolos de mensajería instantánea. Antivirus para chat garantiza el funcionamiento seguro de diversas aplicaciones de mensajería instantánea.

Monitor de red

El componente Monitor de red se ha diseñado para supervisar la actividad de red en tiempo real.

System Watcher

El componente System Watcher se puede utilizar para restaurar acciones llevadas a cabo por el software malintencionado en el sistema operativo.

Anti-Phishing

Anti-Phishing permite comprobar las URL para averiguar si están incluidas en la lista de URL fraudulentas. Este componente se integra en los componentes Antivirus Internet y Antivirus para chat.

Teclado en pantalla

Teclado en pantalla evita la interceptación de los datos introducidos en el teclado físico y protege los datos personales contra aquellos intentos de interceptación que utilizan capturas de pantalla.

Gestión en línea

Si Kaspersky Anti-Virus está instalado en un equipo y tiene una cuenta del portal de My Kaspersky, puede gestionar la protección de este equipo de forma remota.

Participación en el programa Proteger a un amigo

Al participar en el programa Proteger a un amigo, puede recibir puntos de bonificación si comparte vínculos de Kaspersky Anti-Virus con sus amigos. Puede canjear los puntos de bonificación acumulados por un código de activación de bonificación de Kaspersky Anti-Virus.

Novedades

Kaspersky Anti-Virus ofrece las siguientes novedades:

- Las limitaciones de compatibilidad de Microsoft® Windows® 10 ya no existen.
- Se han añadido notificaciones de caducidad de la licencia conformes al estándar del Microsoft.
- En el sistema operativo Windows 10, las notificaciones de las aplicaciones se han reemplazado por mensajes emergentes conformes al estándar de Microsoft.
- El programa Proteger a un amigo se ha movido al portal de My Kaspersky. Ahora es posible registrarse e iniciar sesión en el programa Proteger a un amigo al conectarse al portal de My Kaspersky. Las páginas del programa Proteger a un amigo se pueden ver en el portal de My Kaspersky.
- Se ha añadido compatibilidad con el protocolo HTTP/2.
- Se ha añadido compatibilidad parcial para los navegadores Yandex y Microsoft Edge.
- Se ha añadido compatibilidad con escritorios virtuales en Microsoft Windows 10.
- Se ha mejorado la interfaz de usuario gráfica.

Kit de distribución

Puede comprar la aplicación de las siguientes maneras:

- En caja. Distribuido en las tiendas de nuestros socios.
- En la tienda en línea. Distribuido en las tiendas en línea de Kaspersky Lab (por ejemplo, <http://www.kaspersky.es>, en la sección Tienda en línea) o a través de las empresas asociadas.

Si compra la versión en caja de la aplicación, el kit de distribución contiene los siguientes elementos:

- Sobre sellado con el CD de instalación que contiene los archivos de la aplicación y de la documentación.
- Breve Guía del usuario con un código de activación.
- Contrato de licencia que estipula las condiciones según las cuales puede utilizar la aplicación.

El contenido del kit de distribución puede variar en función de la región en la que se distribuye la aplicación.

Si compra Kaspersky Anti-Virus en una tienda en línea, copie la aplicación del sitio web de la tienda. Recibirá la información necesaria para la activación de la aplicación, incluido un código de activación, por correo electrónico tras la recepción del pago.

Requisitos de hardware y software

Requisitos generales:

- 480 MB de espacio libre en el disco duro
- CD-ROM/DVD-ROM (para instalar desde el CD)
- Acceso a Internet (para instalar y activar la aplicación, y actualizar las bases de datos y los módulos de software)
- Microsoft® Internet Explorer® 8.0 o posterior

Para acceder al portal de My Kaspersky, recomendamos usar Microsoft Internet Explorer 9.0 o posterior.

- Microsoft Windows® Installer 3.0 o posterior
- Microsoft .NET Framework 4 o posterior

Requisitos para Microsoft Windows XP Home Edition (Service Pack 3 o superior), Microsoft Windows XP Professional (Service Pack 3 o superior) y Microsoft Windows XP Professional x64 Edition (Service Pack 2 o superior):

- Procesador con una velocidad del reloj de 1 GHz o superior
- 512 MB libres de memoria RAM

Requisitos para Microsoft Windows Vista® Home Basic (Service Pack 1 o posterior), Microsoft Windows Vista Home Premium (Service Pack 1 o posterior), Microsoft Windows Vista Business (Service Pack 1 o posterior), Microsoft Windows Vista Enterprise (Service Pack 1 o posterior), Microsoft Windows Vista Ultimate (Service Pack 1 o posterior), Microsoft Windows 7 Starter (Service Pack 1 o posterior), Microsoft Windows 7 Home Basic (Service Pack 1 o posterior), Microsoft Windows 7 Home Premium (Service Pack 1 o posterior), Microsoft Windows 7 Professional (Service Pack 1 o posterior), Microsoft Windows 7 Ultimate (Service Pack 1 o posterior), Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Windows 8.1 Pro (Windows 8.1 Update), y Windows 8.1 Enterprise (Windows 8.1 Update) y Microsoft Windows 10 Home, Microsoft Windows 10 Enterprise y Microsoft Windows 10 Pro:

- Procesador con una velocidad del reloj de 1 GHz o superior
- 1 GB libre de RAM (para sistemas operativos de 32 bits); 2 GB libres de RAM (para sistemas operativos de 64 bits)

Requisitos para tabletas:

- Microsoft Tablet PC
- Intel® Celeron® CPU 1.66 GHz o superior
- 1000 MB libres de memoria RAM

Requisitos para netbooks:

- Intel Atom™ CPU 1,60 GHz o superior
- 1024 MB libres de memoria RAM
- Pantalla de 10,1 pulgadas con una resolución de 1024x600
- Núcleo gráfico Intel GMA 950

Instalación y eliminación de la aplicación

Esta sección contiene instrucciones paso a paso sobre cómo instalar y eliminar Kaspersky Anti-Virus.

En esta sección

Procedimiento de instalación estándar.....	22
Instalación de la aplicación desde la línea de comandos	28
Primeros pasos	29
Actualización de una versión anterior de la aplicación	30
Cambio de Kaspersky Anti-Virus a Kaspersky Internet Security o Kaspersky Total Security	35
Eliminar la aplicación	39

Procedimiento de instalación estándar

Kaspersky Anti-Virus se instalará en su equipo de forma interactiva mediante el asistente de configuración.

El asistente consta de una serie de páginas (pasos) por los que usted puede navegar mediante los botones **Atrás** y **Siguiente**. Para cerrar el asistente cuando haya concluido, haga clic en el botón **Finalizar**. Para detener la actividad del asistente en cualquier paso de la instalación, cierre la ventana.

Si la aplicación está destinada a la protección de más de un equipo (los términos del contrato de licencia de usuario final definen el número máximo de equipos permitidos), se debe instalar de la misma forma en todos los equipos.

► *Para instalar Kaspersky Anti-Virus en su equipo,*

En el CD de instalación, ejecute el archivo con la extensión .exe.

La aplicación se instalará a continuación con la ayuda de un asistente de configuración estándar.

En algunas regiones, el CD de instalación no incluye el paquete de instalación de la aplicación. El CD de instalación solo contiene el archivo de autoejecución. Cuando se ejecuta este archivo, se abre la ventana de descarga de la aplicación.

► *Instalar Kaspersky Anti-Virus usando el archivo de la autocarrera:*

1. Haga clic en el botón **Descargar e instalar** en la ventana de descarga de la aplicación.

Al hacer clic en el botón **Descargar e Instalar**, está enviando información sobre la versión de su sistema operativo a Kaspersky Lab.

2. Si se produjera algún error en la descarga, haga clic en el vínculo **Descargar del sitio web e instalar manualmente** que le llevará a un sitio web desde el que podrá descargar la aplicación manualmente.

La aplicación se instalará a continuación con la ayuda de un asistente de configuración estándar.

Para instalar Kaspersky Anti-Virus, también puede descargar un paquete de instalación de Internet. En este caso, el asistente de configuración muestra varios pasos adicionales para la instalación en el caso de algunos idiomas.

Junto con la aplicación, se instalan complementos para navegadores a fin de garantizar una navegación por Internet segura.

En esta sección

Paso 1. Búsqueda de una versión más reciente de la aplicación	24
Paso 2. Inicio de la instalación de la aplicación	24
Paso 3. Revisión del contrato de licencia	25
Paso 4. Declaración de Kaspersky Security Network	25
Paso 5. Instalación.....	25

Paso 6. Finalización de la instalación.....	27
Paso 7. Activación de la aplicación.....	27
Paso 8. Registro de un usuario.....	28
Paso 9. Finalización de la activación.....	28

Paso 1. Búsqueda de una versión más reciente de la aplicación

Antes de la instalación, el asistente de configuración buscará la versión más reciente de Kaspersky Anti-Virus en los servidores de actualización de Kaspersky Lab.

Si el asistente de configuración no detecta ninguna versión más reciente de la aplicación en los servidores de actualización, comenzará a instalar la versión actual.

Si el asistente de configuración detecta una versión más reciente de Kaspersky Anti-Virus en los servidores de actualización de Kaspersky Lab, le preguntará si desea descargarla e instalarla en su equipo. Le recomendamos que instale la nueva versión de la aplicación porque las versiones más recientes incluyen más mejoras que le permiten garantizar una protección más fiable de su equipo. Si no desea instalar la nueva versión, el asistente comenzará a instalar la versión actual de la aplicación. Si acepta instalar la nueva versión de la aplicación, el asistente de configuración copiará los archivos de instalación del paquete de distribución en su equipo y comenzará a instalar la nueva versión.

Paso 2. Inicio de la instalación de la aplicación

Durante este paso, el asistente de configuración le ofrecerá instalar la aplicación.

Para continuar con la instalación, haga clic en el botón **Instalar**.

Según el tipo de instalación y el idioma, en este paso el asistente de configuración le preguntará si desea visualizar el contrato de licencia formalizado entre usted y Kaspersky Lab, así como si desea participar en Kaspersky Security Network.

Paso 3. Revisión del contrato de licencia

Este paso del asistente de configuración se muestra en algunos de los idiomas de localización al instalar Kaspersky Anti-Virus desde un paquete de instalación descargado de Internet.

En este paso, el asistente de configuración le ofrecerá revisar el contrato de licencia formalizado entre usted y Kaspersky Lab.

Lea el contrato de licencia en su totalidad y, si acepta las condiciones, haga clic en el botón **Aceptar**. Entonces continúa la instalación de la aplicación en su equipo.

Si no se aceptan las condiciones del contrato de licencia, la aplicación no se instalará.

Paso 4. Declaración de Kaspersky Security Network

En este paso, el asistente de configuración le invitará a participar en Kaspersky Security Network. La participación en el programa implica el envío a AO Kaspersky Lab de información acerca de las nuevas amenazas que se detecten en su ordenador, al ejecutar aplicaciones y en las solicitudes firmadas que se ha descargado, así como información de su sistema operativo. No se recopilan, procesan ni almacenan sus datos personales.

Revise la declaración de Kaspersky Security Network. Si acepta todas las condiciones, haga clic en el botón **Aceptar** de la ventana del asistente.

Si no desea participar en Kaspersky Security Network, haga clic en el botón **Rechazar**.

Después aceptar o rechazar participar en Kaspersky Security Network, continuará la instalación de la aplicación.

Paso 5. Instalación

En algunas versiones de Kaspersky Anti-Virus distribuidas bajo suscripción, se deberá introducir una contraseña que se recibe del proveedor de servicios antes de la instalación.

Después de introducir la contraseña, comenzará la instalación de la aplicación.

La instalación de la aplicación lleva algún tiempo. Espere hasta que finalice.

Cuando finaliza la instalación, el asistente de configuración accederá automáticamente al paso siguiente.

Kaspersky Anti-Virus realiza diferentes comprobaciones durante la instalación. Estas comprobaciones pueden detectar los problemas siguientes:

- *El no cumplimiento de los requisitos del software por parte del sistema operativo.* Durante la instalación, el asistente comprueba las siguientes condiciones:
 - Si el sistema operativo y los Service Packs cumplen los requisitos del software.
 - Que todas las aplicaciones necesarias estén disponibles.
 - Si la cantidad de espacio libre en disco es suficiente para la instalación.
 - Si el usuario que instala la aplicación tiene privilegios de administrador

Si no se cumple alguno de los requisitos indicados anteriormente, aparece la notificación correspondiente.

- *Presencia de aplicaciones incompatibles en el equipo.* Si se detectan aplicaciones incompatibles, se muestran en una lista en la pantalla y se le sugiere que las elimine. Se aconseja eliminar manualmente cualquier aplicación que Kaspersky Anti-Virus no pueda eliminar automáticamente. Al eliminar aplicaciones incompatibles, deberá reiniciar el sistema operativo, tras lo cual continuará automáticamente la instalación de Kaspersky Anti-Virus.
- *Presencia de programas maliciosos en el equipo.* Si se detecta en el equipo cualquier programa malintencionado que interfiera con la instalación del software antivirus, el asistente de configuración le solicitará descargar *Kaspersky Virus Removal Tool*, una herramienta especial diseñada para neutralizar infecciones.

Si acepta instalar la herramienta, el asistente de configuración la descarga del servidor de Kaspersky Lab, tras lo cual se instala de forma automática. Si el asistente no puede descargar la herramienta, se le ofrecerá descargarla manualmente haciendo clic en el vínculo que se le proporciona.

Paso 6. Finalización de la instalación

En este paso, el asistente le informa de que se ha completado la instalación de la aplicación.

Para empezar a usar Kaspersky Anti-Virus inmediatamente, asegúrese de que la casilla **Ejecutar Kaspersky Anti-Virus** está seleccionada y haga clic en el botón **Finalizar**.

Si ha desactivado la casilla de verificación **Ejecutar Kaspersky Anti-Virus** antes de cerrar el asistente, tendrá que ejecutar la aplicación de forma manual.

En algunos casos, es posible que tenga que reiniciar el sistema operativo para completar la instalación.

Paso 7. Activación de la aplicación

El asistente de activación se inicia la primera vez que se ejecuta Kaspersky Anti-Virus.

La *activación* es el proceso que consiste en poner en funcionamiento una versión completamente funcional de la aplicación durante un determinado período de tiempo.

Se ofrecen las opciones siguientes para la activación de Kaspersky Anti-Virus:

- **Activar aplicación.** Seleccione esta opción e introduzca un código de activación (consulte la sección "Acerca del código de activación" en la página [47](#)) si ha comprado una licencia para la aplicación.

Si especifica un código de activación de Kaspersky Internet Security o Kaspersky Total Security en el campo de entrada, el procedimiento de cambio a Kaspersky Internet Security o Kaspersky Total Security se iniciará en cuanto finalice la activación.

- **Activar la versión de evaluación de la aplicación.** Seleccione esta opción de activación si desea instalar la versión de evaluación de la aplicación antes de tomar la decisión de comprar una licencia. Puede usar la aplicación y todas sus funciones durante un breve período de prueba. Una vez que haya caducado la licencia de evaluación de la aplicación, la versión de evaluación de la aplicación no se podrá activar una segunda vez.

Se requiere una conexión a Internet para activar la aplicación.

Durante la activación de la aplicación, puede tener que registrarse en el portal de My Kaspersky.

Paso 8. Registro de un usuario

Este paso no está disponible en todas las versiones de Kaspersky Anti-Virus.

Los usuarios registrados podrán enviar solicitudes a Soporte técnico y a Virus Lab a través del portal de My Kaspersky, gestionar códigos de activación cómodamente, y recibir la información más reciente sobre nuevas aplicaciones y ofertas especiales de Kaspersky Lab.

Si acepta registrarse, especifique los datos de registro en los campos correspondientes y haga clic en el botón **Iniciar sesión** para enviar los datos a Kaspersky Lab.

En algunos casos, es necesario que el usuario se registre para empezar a usar la aplicación.

Paso 9. Finalización de la activación

El asistente le informará de que Kaspersky Anti-Virus ha sido activado con éxito.

Haga clic en **Finalizar** para salir el asistente.

Instalación de la aplicación desde la línea de comandos

Puede instalar Kaspersky Anti-Virus desde la línea de comandos.

Sintaxis de la línea de comandos:

```
<ruta al archivo del paquete de instalación> [parámetros]
```

Dispone de instrucciones detalladas y de una lista de los parámetros de instalación en el sitio web de Soporte Técnico (<http://support.kaspersky.com/sp/12257>).

Primeros pasos

Para que Kaspersky Anti-Virus sea totalmente compatible con los navegadores, debe instalar y activar la extensión Kaspersky Protection en cada uno de ellos. Kaspersky Anti-Virus usa la extensión de Kaspersky protection para inyectar un script en el tráfico. La aplicación usa este script para interactuar con la página web. La aplicación protege los datos que transmite el script a través de una firma digital. Kaspersky Anti-Virus puede integrar el script sin necesidad de usar la extensión Kaspersky Protection.

Kaspersky Anti-Virus firma los datos transmitidos por el script mediante las bases de datos antivirus instaladas y las solicitudes remitidas a Kaspersky Security Network. La aplicación envía las solicitudes a Kaspersky Security Network con independencia de si aceptó o no la declaración de las condiciones de Kaspersky Security Network.

La extensión Kaspersky Protection se instala en los navegadores durante la instalación de Kaspersky Anti-Virus.

Después de instalar Kaspersky Anti-Virus, tiene que activar la extensión Kaspersky Protection:

- Para activar la extensión en Mozilla™ Firefox™, tiene que permitir que se instale la extensión en la ventana del navegador.
- En Google Chrome™, tiene que permitir que se active la extensión Kaspersky Protection. Si rechaza activar la extensión, tendrá que instalar y activar la extensión Kaspersky Protection de forma manual más adelante desde Chrome™ Web Store.

En Microsoft Internet Explorer, la extensión Kaspersky Protection se activa automáticamente.

Si su equipo funciona con el sistema operativo Windows 10, debe instalar la extensión de Kaspersky Protection en el navegador Microsoft Internet Explorer manualmente. Puede instalar la extensión mediante el mensaje informativo en el Centro de notificaciones (consulte la sección "Evaluación de los problemas de protección del equipo y resolución de los problemas de seguridad" en la página [58](#)).

Actualización de una versión anterior de la aplicación

Instalación de una nueva versión de Kaspersky Anti-Virus sobre una versión anterior de Kaspersky Anti-Virus

Si ya había instalado una versión anterior de Kaspersky Anti-Virus en su equipo, puede actualizarlo a la última versión de Kaspersky Anti-Virus. Si dispone de una licencia válida de una versión anterior de Kaspersky Anti-Virus, no tendrá que activar la aplicación: el asistente de instalación recuperará automáticamente la información de la licencia de la versión anterior de Kaspersky Anti-Virus y la aplicará durante la instalación de la nueva versión.

La aplicación se puede cambiar desde una versión anterior automáticamente en el fondo si la opción **Descargar e instalar las nuevas versiones automáticamente** se selecciona en la ventana **Configuración de actualización (Configuración → Adicional Actualizar)**.

Instalación de una nueva versión de Kaspersky Anti-Virus sobre una versión anterior de Kaspersky Internet Security

Si instala una nueva versión de Kaspersky Anti-Virus en un equipo en el que ya se ha instalado una versión anterior de Kaspersky Internet Security con una licencia vigente, el asistente de activación le solicitará que seleccione una de las opciones siguientes para continuar:

- Continuar usando Kaspersky Internet Security con la licencia actual. En este caso, se iniciará el asistente de migración. Cuando finalice el asistente de migración, la nueva versión de Kaspersky Internet Security estará instalada en su equipo. Puede utilizar Kaspersky Internet Security hasta que caduque la licencia de la versión anterior de Kaspersky Internet Security.
- Proceda con la instalación de la nueva versión de Kaspersky Anti-Virus. En este caso, la aplicación se instala y se activa según el procedimiento estándar.

Kaspersky Anti-Virus se instalará en su equipo de forma interactiva mediante el asistente de configuración.

El asistente consta de una serie de páginas (pasos) por los que usted puede navegar mediante los botones **Atrás** y **Siguiente**. Para cerrar el asistente cuando haya concluido, haga clic en el botón **Finalizar**. Para detener la actividad del asistente en cualquier paso de la instalación, cierre la ventana.

Si la aplicación está destinada a la protección de más de un equipo (los términos del contrato de licencia de usuario final definen el número máximo de equipos permitidos), se debe instalar de la misma forma en todos los equipos.

► *Para instalar Kaspersky Anti-Virus en su equipo,*

En el CD de instalación, ejecute el archivo con la extensión .exe.

La aplicación se instalará a continuación con la ayuda de un asistente de configuración estándar.

En algunas regiones, el CD de instalación no incluye el paquete de instalación de la aplicación. El CD de instalación solo contiene el archivo de autoejecución. Cuando se ejecuta este archivo, se abre la ventana de descarga de la aplicación.

► *Método de instalación de Kaspersky Anti-Virus mediante el archivo autoejecutable:*

1. Haga clic en el botón **Descargar e instalar** en la ventana de descarga de la aplicación.

Al hacer clic en el botón **Descargar e Instalar**, está enviando información sobre la versión de su sistema operativo a Kaspersky Lab.

2. Si se produjera algún error en la descarga, haga clic en el vínculo **Descargar del sitio web e instalar manualmente** que le llevará a un sitio web desde el que podrá descargar la aplicación manualmente.

La aplicación se instalará a continuación con la ayuda de un asistente de configuración estándar.

Para instalar Kaspersky Anti-Virus, también puede descargar un paquete de instalación de Internet. En este caso, el asistente de configuración muestra varios pasos adicionales para la instalación en el caso de algunos idiomas.

Junto con la aplicación, se instalan complementos para navegadores a fin de garantizar una navegación por Internet segura.

La actualización desde versiones anteriores tiene algunas limitaciones (consulte la sección "Limitaciones y advertencias" en la página [104](#)).

En esta sección

Paso 1. Búsqueda de una versión más reciente de la aplicación	32
Paso 2. Inicio de la instalación de la aplicación	32
Paso 3. Revisión del contrato de licencia	33
Paso 4. Declaración de Kaspersky Security Network	33
Paso 5. Instalación.....	34
Paso 6. Finalización de la instalación.....	35

Paso 1. Búsqueda de una versión más reciente de la aplicación

Antes de la instalación, el asistente de configuración buscará la versión más reciente de Kaspersky Anti-Virus en los servidores de actualización de Kaspersky Lab.

Si el asistente de configuración no detecta ninguna versión más reciente de la aplicación en los servidores de actualización, comenzará a instalar la versión actual.

Si el asistente de configuración detecta una versión más reciente de Kaspersky Anti-Virus en los servidores de actualización de Kaspersky Lab, le preguntará si desea descargarla e instalarla en su equipo. Le recomendamos que instale la nueva versión de la aplicación porque las versiones más recientes incluyen más mejoras que le permiten garantizar una protección más fiable de su equipo. Si no desea instalar la nueva versión, el asistente comenzará a instalar la versión actual de la aplicación. Si acepta instalar la nueva versión de la aplicación, el asistente de configuración copiará los archivos de instalación del paquete de distribución en su equipo y comenzará a instalar la nueva versión.

Paso 2. Inicio de la instalación de la aplicación

Durante este paso, el asistente de configuración le ofrecerá instalar la aplicación.

Para continuar con la instalación, haga clic en el botón **Instalar**.

Según el tipo de instalación y el idioma, en este paso el asistente de configuración le preguntará si desea visualizar el contrato de licencia formalizado entre usted y Kaspersky Lab, así como si desea participar en Kaspersky Security Network.

Paso 3. Revisión del contrato de licencia

Este paso del asistente de configuración se muestra en algunos de los idiomas de localización al instalar Kaspersky Anti-Virus desde un paquete de instalación descargado de Internet.

En este paso, el asistente de configuración le ofrecerá revisar el contrato de licencia formalizado entre usted y Kaspersky Lab.

Lea el contrato de licencia en su totalidad y, si acepta las condiciones, haga clic en el botón **Aceptar**. Entonces continúa la instalación de la aplicación en su equipo.

Si no se aceptan las condiciones del contrato de licencia, la aplicación no se instalará.

Paso 4. Declaración de Kaspersky Security Network

En este paso, el asistente de configuración le invitará a participar en Kaspersky Security Network. La participación en el programa implica el envío a AO Kaspersky Lab de información acerca de las nuevas amenazas que se detecten en su ordenador, al ejecutar aplicaciones y en las solicitudes firmadas que se ha descargado, así como información de su sistema operativo. No se recopilan, procesan ni almacenan sus datos personales.

Revise la declaración de Kaspersky Security Network. Si acepta todas las condiciones, haga clic en el botón **Aceptar** de la ventana del asistente.

Si no desea participar en Kaspersky Security Network, haga clic en el botón **Rechazar**.

Después aceptar o rechazar participar en Kaspersky Security Network, continuará la instalación de la aplicación.

Paso 5. Instalación

En algunas versiones de Kaspersky Anti-Virus distribuidas bajo suscripción, se deberá introducir una contraseña que se recibe del proveedor de servicios antes de la instalación.

Después de introducir la contraseña, comenzará la instalación de la aplicación.

La instalación de la aplicación lleva algún tiempo. Espere hasta que finalice.

Cuando finaliza la instalación, el asistente de configuración accederá automáticamente al paso siguiente.

Kaspersky Anti-Virus realiza diferentes comprobaciones durante la instalación. Estas comprobaciones pueden detectar los problemas siguientes:

- *El no cumplimiento de los requisitos del software por parte del sistema operativo.* Durante la instalación, el asistente comprueba las siguientes condiciones:
 - Si el sistema operativo y los Service Packs cumplen los requisitos del software.
 - Que todas las aplicaciones necesarias estén disponibles.
 - Si la cantidad de espacio libre en disco es suficiente para la instalación.
 - Si el usuario que instala la aplicación tiene privilegios de administrador

Si no se cumple alguno de los requisitos indicados anteriormente, aparece la notificación correspondiente.

- *Presencia de aplicaciones incompatibles en el equipo.* Si se detectan aplicaciones incompatibles, se muestran en una lista en la pantalla y se le sugiere que las elimine. Se aconseja eliminar manualmente cualquier aplicación que Kaspersky Anti-Virus no pueda eliminar automáticamente. Al eliminar aplicaciones incompatibles, deberá reiniciar el sistema operativo, tras lo cual continuará automáticamente la instalación de Kaspersky Anti-Virus.
- *Presencia de programas maliciosos en el equipo.* Si se detecta en el equipo cualquier programa malintencionado que interfiera con la instalación del software antivirus, el asistente de configuración le solicitará descargar *Kaspersky Virus Removal Tool*, una herramienta especial diseñada para neutralizar infecciones.

Si acepta instalar la herramienta, el asistente de configuración la descarga del servidor de Kaspersky Lab, tras lo cual se instala de forma automática. Si el asistente no puede descargar la herramienta, se le ofrecerá descargarla manualmente haciendo clic en el vínculo que se le proporciona.

Paso 6. Finalización de la instalación

En este paso, el asistente le informa de que se ha completado la instalación de la aplicación.

Una vez instalada la aplicación, reinicie el sistema operativo.

Si la casilla de verificación **Ejecutar Kaspersky Anti-Virus** está activada, la aplicación se iniciará automáticamente cuando reinicie el equipo.

Si ha desactivado la casilla de verificación **Ejecutar Kaspersky Anti-Virus** antes de cerrar el asistente, tendrá que ejecutar la aplicación de forma manual.

Cambio de Kaspersky Anti-Virus a Kaspersky Internet Security o Kaspersky Total Security

Kaspersky Anti-Virus permite el cambio a Kaspersky Internet Security sin instalación ni descargas de software adicional.

Kaspersky Internet Security es una aplicación diseñada para garantizar una protección completa del equipo. En comparación con Kaspersky Anti-Virus, Kaspersky Internet Security proporciona una amplia gama de opciones avanzadas adicionales como parte de los siguientes componentes y funciones:

- Control de aplicaciones
- Modo Aplicaciones de confianza
- Control Parental
- Firewall
- Prevención de intrusiones
- Pago seguro
- Bloqueo del acceso a los sitios Web peligrosos.
- Control de cambios del sistema

- Monitor de red
- Acceso a la cámara web
- Navegación privada
- Anti-Spam
- Anti-Banner
- Entrada segura desde el teclado

Puede cambiar temporalmente a la versión de evaluación de Kaspersky Internet Security para probar sus funciones, o puede comprar una licencia y empezar a utilizarlo.

En algunas regiones, se puede cambiar de Kaspersky Anti-Virus a Kaspersky Total Security.

Kaspersky Total Security ofrece las mismas funciones que Kaspersky Internet Security y toda una gama de funciones adicionales.

Kaspersky Total Security incluye las funciones siguientes:

- Copia de seguridad y restauración
- Cifrado de datos
- Protección con contraseña

El cambio a Kaspersky Total Security se lleva a cabo del mismo modo que el cambio a Kaspersky Internet Security.

Cuando se utiliza en algunas regiones o por suscripción, el cambio temporal a la versión de evaluación de Kaspersky Internet Security y Kaspersky Total Security no está disponible.

En esta sección

Uso temporal de Kaspersky Internet Security.....	37
Cambio al uso permanente de Kaspersky Internet Security	39

Uso temporal de Kaspersky Internet Security

Puede cambiar temporalmente a la versión de evaluación de Kaspersky Internet Security para conocer sus funciones. Después podrá comprar una licencia para seguir utilizando esta aplicación.

► *Para cambiar temporalmente a la versión de evaluación de Kaspersky Internet Security, haga lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Actualizar**.
3. Haga clic en el botón **Versión de evaluación** en la ventana que se abre.
Se inicia el Asistente de migración.
4. Siga las instrucciones del asistente.

Cuando se utiliza en algunas regiones o por suscripción, el cambio temporal a la versión de evaluación de Kaspersky Internet Security no está disponible. En estos casos, la opción **Ampliación de la protección** no está disponible en la lista **Más herramientas**.

Paso 1. Solicitud de activación de la versión de evaluación de Kaspersky Internet Security

Si la solicitud de activación de la versión de evaluación de Kaspersky Internet Security se realiza correctamente, el asistente continúa automáticamente con el paso siguiente.

Paso 2. Comienzo de la actualización

En este paso, el asistente muestra un mensaje que le informa sobre el cumplimiento de los requisitos para la migración a la versión de evaluación de Kaspersky Internet Security. Para seguir con el asistente, haga clic en el botón **Siguiente**.

Paso 3. Eliminación de aplicaciones incompatibles

En este paso, el asistente comprueba si hay alguna aplicación incompatible con Kaspersky Internet Security instalada en el equipo. Si no se encuentran aplicaciones de este tipo, el asistente automáticamente procede con el paso siguiente. Si se encuentran aplicaciones de este tipo, el Asistente muestra una lista de ellas en la ventana y le sugiere su desinstalación.

Después de desinstalar las aplicaciones incompatibles, puede que sea necesario reiniciar el sistema operativo. Después de reiniciar, el asistente se iniciará automáticamente y continuará la migración a la versión de evaluación de Kaspersky Internet Security.

Paso 4. Cambio a la versión de evaluación de Kaspersky Internet Security

En este paso, el Asistente conecta los componentes de Kaspersky Internet Security. Esto puede tardar un poco. En cuanto el proceso haya finalizado, el asistente procederá automáticamente al siguiente paso.

Paso 5. Reinicio de la aplicación

En este paso de la migración a la versión de evaluación de Kaspersky Internet Security, debe salir de la aplicación y reiniciarla. Para ello, en el cuadro de diálogo de la notificación, haga clic en el botón **Finalizar**.

Paso 6. Finalización de la activación

Después de reiniciar la aplicación, el Asistente se abre automáticamente. Una vez activada correctamente la versión de evaluación de Kaspersky Internet Security, la ventana del Asistente muestra la información sobre el plazo durante el cual podrá utilizar la versión de evaluación.

Paso 7. Análisis del sistema operativo

En este paso, se recopila información acerca de las aplicaciones Microsoft Windows. Estas aplicaciones se agregan a la lista de aplicaciones de confianza. No se establecen restricciones en las acciones que las aplicaciones de confianza realicen en el sistema operativo.

Una vez finalizada la búsqueda, el asistente pasará automáticamente al paso siguiente.

Paso 8. Fin de la migración

Para cerrar el asistente cuando haya completado su tarea, haga clic en el botón **Finalizar**.

Cuando caduque la licencia de evaluación de Kaspersky Internet Security, ya no podrá volver a cambiar temporalmente de Kaspersky Anti-Virus a la versión de evaluación de Kaspersky Internet Security.

Cambio al uso permanente de Kaspersky Internet Security

Si desea cambiar al uso permanente de Kaspersky Internet Security, tiene que comprar una licencia para Kaspersky Total Security y a continuación activar la aplicación (consulte la sección "Activación de la aplicación" en la página [51](#)).

► *Para comprar una licencia de Kaspersky Internet Security:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Actualizar**.
3. Haga clic en el vínculo **Comprar código de activación** para ir al sitio web de la tienda en línea de Kaspersky Lab o de una empresa asociada, donde podrá comprar una licencia de Kaspersky Internet Security.

Cuando se utiliza en algunas regiones o por suscripción, Kaspersky Anti-Virus no permite el cambio a la versión de evaluación de Kaspersky Internet Security. En estos casos, la opción **Actualizar** no está disponible.

Eliminación de la aplicación

Después de desinstalar Kaspersky Anti-Virus, su equipo y sus datos personales estarán desprotegidos.

Kaspersky Anti-Virus se desinstala con la ayuda del asistente de configuración.

► *Para iniciar el Asistente en un equipo con el sistema operativo Microsoft Windows 7 o versiones anteriores,*

en el menú **Inicio**, seleccione **Todos los programas** → **Kaspersky Anti-Virus** → **Quitar Kaspersky Anti-Virus**.

► *Para iniciar el Asistente en un equipo con el sistema operativo Microsoft Windows 8 o versiones posteriores:*

1. En la pantalla del inicio, haga clic en el icono de Kaspersky Anti-Virus con el botón derecho para abrir la barra de herramientas.
2. Haga clic en el botón **Desinstalar** en la barra de herramientas.
3. En la ventana que abre, seleccione Kaspersky Anti-Virus en la lista.
4. Haga clic en el botón **Desinstalar**, situado en la parte superior de la lista.

En esta sección

Paso 1. Introducción de la contraseña para desinstalar la aplicación	40
Paso 2. Almacenamiento de datos para su uso posterior	40
Paso 3. Confirmación de la eliminación de la aplicación	42
Paso 4. Eliminación de la aplicación. Completando eliminación	42

Paso 1. Introducción de la contraseña para desinstalar la aplicación

Para eliminar Kaspersky Anti-Virus, debe introducir la contraseña. De lo contrario, no podrá acceder a los ajustes de la aplicación. Si no puede especificar la contraseña por cualquier motivo, no podrá eliminar la aplicación.

Este paso solo se muestra si se ha establecido una contraseña para eliminar la aplicación.

Paso 2. Almacenamiento de datos para su uso posterior

En este paso, puede especificar qué datos que utiliza la aplicación quiere conservar para utilizarlos durante la siguiente instalación de la aplicación (p. ej., al instalar una versión más reciente de la aplicación).

De forma predeterminada, la aplicación le ofrece guardar la información de la licencia.

► *Para guardar datos y utilizarlos más adelante, seleccione las casillas que se encuentran al lado de los tipos de datos que desea guardar:*

- La **información de licencia** es un conjunto de datos que elimina la necesidad de activar la aplicación durante una futura instalación al permitirle usarla con la licencia actual, a menos que la licencia caduque antes de iniciar la instalación.
- **Archivos en cuarentena** son los archivos analizados por la aplicación y movidos a Cuarentena.

Cuando se elimina Kaspersky Anti-Virus del equipo, los datos en cuarentena dejan de estar disponibles. Para realizar operaciones con estos archivos, Kaspersky Anti-Virus debe estar instalado.

- Los **Configuración operativa de la aplicación** son los ajustes de la aplicación seleccionados durante la configuración.

Kaspersky Lab no garantiza la compatibilidad con la configuración de versiones anteriores de la aplicación. Tras instalar la versión nueva, le recomendamos que compruebe que la configuración es correcta.

También puede exportar la configuración de la protección en la línea de comandos con el siguiente comando:

```
avp.com EXPORT <nombre_del_archivo>
```

- Los **datos iChecker** son archivos que contienen información acerca de los objetos que ya se han analizado con la tecnología iChecker.

Paso 3. Confirmación de la eliminación de la aplicación

Ya que la desinstalación de la aplicación supone una amenaza para la seguridad del equipo y de sus datos personales, se le solicitará que confirme su deseo de eliminar la aplicación. Para ello, haga clic en **Eliminar**.

Paso 4. Eliminación de la aplicación. Completando eliminación

Durante este paso, el asistente elimina la aplicación del equipo. Espere a que se complete la eliminación.

Después de desinstalar Kaspersky Anti-Virus, puede especificar la razón por la que decidió desinstalar la aplicación mediante un comentario en el sitio web de Kaspersky Lab. Para ello, debe ir al sitio web de Kaspersky Lab mediante el botón **Completar formulario**.

Es posible que esta funcionalidad no esté disponible en algunas regiones.

Durante la eliminación de la aplicación, debe reiniciar su sistema operativo. Si cancela un reinicio inmediato, el proceso de eliminación no concluirá hasta que se reinicie el sistema operativo o hasta que se apague y se vuelva a encender el equipo.

Licencias de la aplicación

Esta sección abarca los aspectos principales de las licencias de la aplicación.

En esta sección

Acerca del Contrato de licencia de usuario final	43
Acerca de la licencia	44
Acerca del modo de funcionalidad limitada	45
Acerca del código de activación	47
Acerca de la suscripción	48
Acerca de la provisión de datos	49
Compra de una licencia.....	50
Activación de la aplicación	51
Renovación de una licencia	52

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* es un contrato vinculante entre usted y AO Kaspersky Lab en el que se estipulan las condiciones en las que puede utilizar la aplicación.

Lea los términos y condiciones del Contrato de Licencia en su totalidad antes de empezar a utilizar la aplicación.

Estará aceptando las condiciones del contrato de licencia al confirmar que está de acuerdo con este cuando instale la aplicación. Si no acepta las condiciones del contrato de licencia, deberá cancelar la instalación de la aplicación y renunciar a su uso.

Acerca de la licencia

Una *licencia* es un derecho de duración limitada para utilizar la aplicación garantizado en el Contrato de licencia de usuario final. La licencia está vinculada a su código único para activar la copia de Kaspersky Anti-Virus.

Una licencia le da derecho a los siguientes tipos de servicios:

- El derecho a utilizar la aplicación en uno o varios dispositivos.

El número de dispositivos en el que puede utilizar la aplicación se especifica en el Contrato de licencia de usuario final.

- Asistencia del Soporte técnico de Kaspersky Lab.
- Otros servicios de Kaspersky Lab o de sus socios disponibles durante el período de licencia

Para gestionar la aplicación, debe comprar una licencia de uso de la aplicación.

La licencia tiene un plazo limitado. A la caducidad de la licencia le sigue un período de gracia durante el cual puede utilizar todas las funciones de la aplicación sin limitaciones.

Si no ha renovado la licencia (consulte la sección "Renovación de una licencia" en la página [52](#)), la aplicación pasará al modo de funcionalidad limitada (consulte la sección "Acerca del modo de funcionalidad limitada" en la página [45](#)) cuando caduque el período de gracia. Algunas funciones de la aplicación no están disponibles en el modo de funcionalidad limitada. La duración del modo de funcionalidad limitada depende de la región y las condiciones de la licencia. Cuando caduca el modo de funcionalidad limitada, las funciones de la aplicación dejan de estar disponibles.

Encontrará la información acerca de la duración del período de gracia y el modo de funcionalidad limitada en la ventana **Licencia** que se puede abrir haciendo clic en el vínculo **Licencia** de la parte inferior de la ventana principal.

Para garantizar que su equipo se encuentre protegido al máximo contra todas las amenazas de seguridad, le recomendamos que renueve la licencia antes de que caduque.

Antes de comprar una licencia, puede obtener una versión de evaluación gratuita de Kaspersky Anti-Virus. La versión de evaluación de Kaspersky Anti-Virus seguirá siendo funcional durante un corto período de evaluación. Cuando caduca el período de evaluación, se desactivan todas las funciones de Kaspersky Anti-Virus. Para continuar usando la aplicación, debe comprar una licencia.

Si no desea renovar la protección de su equipo, puede eliminar Kaspersky Anti-Virus (consulte la sección "Eliminación de la aplicación" en la página [39](#)).

Acercas del modo de funcionalidad limitada

La siguiente tabla muestra las funciones de Kaspersky Anti-Virus que están disponibles y las que no lo están cuando la aplicación funciona en el modo de funcionalidad limitada. Si el valor de la columna Modo de funcionalidad limitada es "sí", significa que la funcionalidad correspondiente está disponible en el modo de funcionalidad limitada. Si el valor de la columna Modo de funcionalidad limitada es "no", la funcionalidad correspondiente no está disponible. Dispone de información adicional en la columna Restricciones.

Tabla 2. Funcionalidad de Kaspersky Anti-Virus en el modo de funcionalidad limitada

Funcionalidad	Restricciones	Modo de funcionalidad limitada
Antivirus de archivos		sí
Análisis antivirus	El análisis se puede iniciar manualmente. El análisis planificado y la configuración del análisis no están disponibles.	sí
Análisis de vulnerabilidades		no
Actualización de las bases de datos y módulos de la aplicación	Los parámetros no se pueden configurar.	sí
Protección contra el software publicitario y el software espía		sí
Antivirus Internet	Funciona sin restricciones.	sí
Antivirus de correo	Funciona sin restricciones.	sí
Antivirus para chat	Funciona sin restricciones.	sí

Funcionalidad	Restricciones	Modo de funcionalidad limitada
Análisis heurístico	Funciona sin restricciones.	sí
Protección contra rootkits		no
Protección frente a vulnerabilidades		no
System Watcher		no
Protección frente a las actividades fraudulentas		sí
Comprobación de la reputación de los archivos y vínculos en Kaspersky Security Network		sí
Herramientas de protección y administración adicionales		sí
Supervisor de direcciones URL		no
Entrada segura desde el teclado		no
Disco de recuperación	Se pueden realizar descargas a través de la interfaz de la aplicación.	sí
Protección con contraseña de la configuración de la aplicación		sí
Rendimiento	Los parámetros de rendimiento de la aplicación se pueden configurar.	sí

Funcionalidad	Restricciones	Modo de funcionalidad limitada
Administrador de tareas	El Administrador de tareas solo muestra los resultados del análisis sin proporcionar herramientas para controlar el análisis o su configuración.	sí
Perfil para juegos	Funciona sin restricciones.	sí
Amenazas y Exclusiones	Funciona sin restricciones.	sí
Autoprotección	Funciona sin restricciones.	sí
Cuarentena	Funciona sin restricciones.	sí
Notificaciones	Solo se puede configurar el parámetro que controla el envío de los anuncios de Kaspersky Lab.	sí
"Proteger a un amigo"	Todas las funciones de la participación en el programa Proteger a un amigo están disponibles.	sí
Configuración de la apariencia de la aplicación	Funciona sin restricciones.	sí
Cuenta My Kaspersky		sí
Administración remota de sus dispositivos	Solo ver y administrar códigos de activación	sí

Acerca del código de activación

El *código de activación* es un código que recibe al comprar una licencia de Kaspersky Anti-Virus. Este código es necesario para activar la aplicación.

El código de activación es una secuencia exclusiva de veinte dígitos y caracteres latinos con el formato xxxxx-xxxxx-xxxxx-xxxxx.

En función del método de compra de la aplicación, podrá obtener el código de activación por una de las siguientes vías:

- Cuando compra una versión en caja de Kaspersky Anti-Virus, se suministra el código de activación en el manual o en la caja que contiene el CD de instalación.
- Cuando compra Kaspersky Anti-Virus en una tienda en línea, se le envía el código de activación por correo electrónico a la dirección que especifique al realizar el pedido.
- Si participa en el programa Proteger a un amigo (consulte la sección "Participación en el programa Proteger a un amigo" en la página [93](#)), puede recibir un código de activación de bonificación a cambio de puntos de bonificación.

El período de validez de la licencia se inicia a partir de la fecha en la que se activa la aplicación. Si ha comprado una licencia para el uso de Kaspersky Anti-Virus en varios dispositivos, el período de validez de esta comenzará a partir de la fecha en que haya aplicado el código de activación por primera vez.

Si pierde o elimina por error su código tras activar la aplicación, póngase en contacto con el servicio de Soporte Técnico de Kaspersky Lab para restaurarlo (<http://support.kaspersky.com/sp>).

Acerca de la suscripción

La *suscripción a Kaspersky Anti-Virus* determina el uso de la aplicación con los parámetros seleccionados (fecha de caducidad y número de dispositivos protegidos). Puede obtener una suscripción a Kaspersky Anti-Virus de un proveedor de servicios (por ejemplo, de su proveedor de Internet). Puede pausar o reanudar la suscripción, renovarla automáticamente, o cancelarla. Puede gestionar su suscripción a través de la página de su cuenta personal en el sitio web del proveedor de servicios.

Los proveedores ofrecen dos tipos de suscripción a Kaspersky Anti-Virus: suscripción para actualizaciones y suscripción para actualizaciones y protección.

La suscripción puede ser limitada (por ejemplo, anual) o ilimitada (sin fecha de caducidad). Para continuar usando Kaspersky Anti-Virus después de que caduque la suscripción limitada, debe renovarla. Las suscripciones ilimitadas se renuevan automáticamente siempre y cuando se haya realizado el pago por adelantado al proveedor de servicios.

Cuando caduca una suscripción limitada, se le ofrece un período de gracia para renovarla. La funcionalidad de la aplicación permanece igual durante este tiempo.

Si no se renueva la suscripción antes de la expiración del período de gracia, Kaspersky Anti-Virus detiene las actualizaciones de las bases de datos de la aplicación (en el caso de las suscripciones de actualizaciones), abandona la interacción con Kaspersky Security Network, y detiene la protección del equipo y la ejecución de tareas de análisis (en el caso de las suscripciones de actualizaciones y protección).

Para utilizar Kaspersky Anti-Virus bajo suscripción, debe aplicar el código de activación que recibió del proveedor de servicios. En algunos casos, se puede descargar y activar el código de activación automáticamente. Al usar la aplicación bajo suscripción, no puede aplicar otro código de activación para renovar su licencia. Solo puede hacerlo cuando caduque el período de suscripción.

Si Kaspersky Anti-Virus ya se está usando con una licencia actual cuando registra su suscripción, Kaspersky Anti-Virus funcionará bajo suscripción después del registro. El código de activación utilizado para activar la aplicación puede aplicarse en otro equipo.

Para cancelar la suscripción, póngase en contacto con el proveedor de servicios al que le haya comprado Kaspersky Anti-Virus.

En función del proveedor de suscripciones, el conjunto de opciones de administración de la suscripción puede variar. Además, podría no recibir el período de gracia durante el cual puede renovar la suscripción.

Acerca de la provisión de datos

A fin de mejorar la protección de datos y mejorar el rendimiento de Kaspersky Anti-Virus, acepta proporcionar automáticamente información de las estadísticas y el funcionamiento de Kaspersky Lab, tales como, entre otros, la información sobre el hardware y el software instalado en el equipo, los datos de la licencia, la información sobre las amenazas e infecciones detectadas, las sumas de verificación de los objetos analizados, la información técnica sobre el equipo y los dispositivos conectados a él y la información sobre la actividad de un dispositivo en Internet. Puede encontrar más información detallada en el sitio web (<http://help.kaspersky.com/es>).

Si participa en Kaspersky Security Network, acepta enviar automáticamente a Kaspersky Lab la siguiente información generada por Kaspersky Anti-Virus (<http://help.kaspersky.com/es>). Puede ver la declaración de Kaspersky Security Network en la ventana **Configuración de herramientas de protección adicionales**.

Kaspersky Lab protege cualquier información recibida de esta manera según lo prescrito por la ley y las normas aplicables de Kaspersky Lab.

Kaspersky Lab usa cualquier información recibida en formularios anonimizados y solo como estadísticas generales. Las estadísticas generales se generan automáticamente a través de la información original recibida y no contienen datos personales o confidenciales. La información original recibida se destruye, ya que se acumula información nueva (una vez al año). Las estadísticas generales se almacenan de forma indefinida.

Compra de una licencia

Puede comprar una licencia o renovar una existente. Cuando compra una licencia, recibe un código de activación que se usa para activar la aplicación (consulte la sección "Activación de la aplicación" en la página [51](#)).

► *Para adquirir una licencia:*

1. Abra la ventana principal de la aplicación.
2. Puede abrir la ventana **Licencia** de alguna de las siguientes formas:
 - Haciendo clic en el vínculo **No se encuentra la licencia** de la parte inferior de la ventana principal si la aplicación no está activada.
 - Haciendo clic en el vínculo **Licencia** de la parte inferior de la ventana principal si la aplicación está activada.
3. En la ventana que se abre, haga clic en el botón **Comprar código de activación**.

Se abrirá la página web de la tienda en línea de Kaspersky Lab o de una empresa asociada, donde podrá comprar una licencia.

Activación de la aplicación

Para aprovechar las funciones de la aplicación y sus servicios adicionales, antes debe activarla.

Si no activó la aplicación durante la instalación, puede hacerlo más tarde. Kaspersky Anti-Virus le recordará mediante mensajes en el área de notificaciones de la barra de tareas que es necesario activar la aplicación.

► Para activar Kaspersky Anti-Virus:

1. Abra la ventana principal de la aplicación.
2. En la parte inferior de la ventana principal de la aplicación, haga clic en el vínculo **Introducir el código de activación**. Se abrirá la ventana **Activación**.
3. En la ventana **Activación**, introduzca el código de activación en el campo de entrada y haga clic en el botón **Activar**.

Se realizará una solicitud de activación de la aplicación.

4. Introduzca los datos de registro del usuario.

En función de las condiciones de uso, la aplicación puede solicitarle iniciar sesión en el portal de My Kaspersky. Si no es usuario registrado, rellene el formulario de registro para acceder a las funciones adicionales.

Los usuarios registrados pueden realizar las siguientes acciones:

- Contactar con Soporte técnico y con Virus Lab
- Gestionar códigos de activación
- Recibir información sobre nuevas aplicaciones y ofertas especiales de Kaspersky Lab

Este paso no está disponible en todas las versiones de Kaspersky Anti-Virus.

5. Haga clic en el botón **Finalizar** en la ventana **Activación** para completar el procedimiento de registro.

Renovación de una licencia

Puede renovar una licencia cuando esté a punto de caducar. Para hacer esto, puede especificar un nuevo código de activación sin tener que esperar a que caduque la licencia actual. Cuando la licencia actual caduca, Kaspersky Anti-Virus se activa automáticamente con el código de activación adicional.

► *Para especificar un código de activación adicional para la renovación automática de la licencia, realice lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. En la parte inferior de la ventana principal, haga clic en el vínculo **Licencia** para abrir la ventana **Licencia**.
3. En la ventana que se abrirá, en la sección **Código de activación nuevo**, haga clic en el botón **Introducir el código de activación**.
4. Introduzca el código de activación en los campos correspondientes y haga clic en el botón **Agregar**.

Kaspersky Anti-Virus enviará los datos al servidor de activación de Kaspersky Lab para verificarlos.

5. Haga clic en el botón **Finalizar**.

El nuevo código de activación aparecerá en la ventana **Licencia**.

La aplicación se activará automáticamente con el nuevo código de activación cuando la licencia caduque. También puede activar la aplicación manualmente con un nuevo código de activación haciendo clic en el botón **Activar ahora**. Este botón estará disponible si no se ha activado la aplicación automáticamente. Este botón no estará disponible antes de que la licencia caduque.

Si el nuevo código de activación que especifique ya se ha utilizado en otro equipo o en este mismo, la fecha de activación para la renovación de la licencia será la fecha en la que se activó la aplicación por primera vez con este código.

Solución de problemas del sistema operativo después de una infección

Esta sección proporciona información sobre cómo restaurar el sistema operativo después de que se haya infectado con virus.

En esta sección

Recuperación del sistema operativo después de una infección.....	53
Solución de problemas del sistema operativo mediante el asistente de solución de problemas de Microsoft Windows.....	54
Acerca de Kaspersky Rescue Disk	56

Recuperación del sistema operativo después de una infección

Si sospecha que el sistema operativo de su equipo puede estar dañado o haber sido modificado debido a la actividad de software malicioso, utilice el *asistente de solución de problemas de Microsoft Windows* para limpiar el sistema de cualquier rastro de objetos maliciosos. Kaspersky Lab recomienda ejecutar el asistente después de desinfectar el equipo, para asegurarse de que se eliminan todas las amenazas y se reparan todos los daños debidos a infecciones.

El asistente comprueba si hay cambios en el sistema, entre los que se incluyen bloqueos de acceso a la red, cambios de extensiones de nombres de archivo de formatos conocidos o bloqueos en el panel de control. Existen distintos motivos para estos distintos tipos de daños. Entre ellos se incluyen actividades de software malicioso, configuraciones incorrectas del sistema, errores del sistema o incluso el funcionamiento incorrecto de las aplicaciones de optimización del sistema.

Al finalizar la revisión, el asistente analiza la información recopilada para evaluar la presencia de daños en el sistema que requieren atención inmediata. En función de la revisión, el asistente genera una lista de acciones necesarias para eliminar el daño. El asistente agrupa estas acciones por categorías en función de la gravedad de los problemas detectados.

Solución de problemas del sistema operativo mediante el asistente de solución de problemas de Microsoft Windows

► *Para iniciar el asistente para la solución de problemas de Microsoft Windows:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Solución de problemas de Microsoft Windows**.

Se abre la ventana Asistente para la solución de problemas de Microsoft Windows.

El asistente consta de una serie de páginas (pasos) por los que usted puede navegar mediante los botones **Atrás** y **Siguiente**. Para cerrar el asistente cuando haya concluido, haga clic en el botón **Finalizar**. Para interrumpir el asistente en cualquier momento, utilice **Cancelar**.

Examinemos más detalladamente los pasos del asistente.

Paso 1. Iniciar la recuperación del sistema operativo

Asegúrese de que la opción del asistente **Buscar daños causados por actividades de software malicioso** esté seleccionada y haga clic en el botón **Siguiente**.

Paso 2. Búsqueda de problemas

El asistente busca los problemas y los daños que se deben solucionar. Cuando la búsqueda finaliza, el asistente procede automáticamente al paso siguiente.

Paso 3. Seleccionar acciones para reparar daños

Todos los daños encontrados durante el paso anterior se agrupan en función del tipo de peligro que suponen. Para cada grupo de daños, Kaspersky Lab recomienda una secuencia de acciones para repararlos. Hay tres grupos:

- Las *acciones altamente recomendadas* eliminan los problemas que suponen una amenaza seria para la seguridad. Se recomienda reparar todos los daños de este grupo.
- Las *acciones recomendadas* están dirigidas a reparar los daños que supongan una amenaza. También se recomienda reparar los daños de este grupo.
- Las *acciones adicionales* repararan los daños que no suponen ninguna amenaza actualmente, pero que pueden representar un peligro futuro para la seguridad del equipo.

Para consultar los daños de un grupo, haga clic en el icono ► situado a la izquierda del nombre del grupo.

Para obtener el asistente adecuado para corregir un tipo de daño concreto, seleccione la casilla de verificación que se encuentra a la izquierda de la descripción del daño. De forma predeterminada, el asistente corrige los daños que pertenecen a los grupos de acciones recomendadas y altamente recomendadas. Si no desea corregir un tipo de daño en particular, desactive la casilla de verificación que se encuentra a su lado.

Se recomienda encarecidamente no desactivar las casillas seleccionadas de forma predeterminada; de lo contrario, su equipo quedará expuesto a amenazas.

Cuando haya definido las acciones que debe realizar el asistente, haga clic en el botón **Siguiente**.

Paso 4. Arreglo de daños

El asistente llevará a cabo las acciones seleccionadas durante el paso anterior. Este proceso puede tardar unos minutos. Una vez reparado el daño, el asistente pasa automáticamente al siguiente paso.

Paso 5. Fin del asistente

Haga clic en **Finalizar** para cerrar el asistente.

Acerca de Kaspersky Rescue Disk

El disco de recuperación es una copia de Kaspersky Rescue Disk almacenada en una unidad extraíble (CD o dispositivo USB). Puede utilizar Kaspersky Rescue Disk para analizar y desinfectar equipos infectados que no se puedan desinfectar de ningún otro modo (por ejemplo, con aplicaciones antivirus).

Si ha comprado una versión en caja de Kaspersky Anti-Virus, además del paquete de instalación de Kaspersky Anti-Virus, el CD de instalación también incluirá Kaspersky Rescue Disk. Puede usar este CD de instalación como disco de recuperación.

Puede obtener más información sobre cómo utilizar Kaspersky Rescue Disk en el sitio web de Soporte técnico (<http://support.kaspersky.com/sp/viruses/rescuedisk/main>).

Administración de las notificaciones de la aplicación

Las notificaciones que aparecen en el área de notificaciones de la barra de tareas le informan de los eventos de la aplicación que requieren su atención. En función del grado de gravedad del evento, puede recibir los siguientes tipos de notificaciones:

- En la sección *Notificaciones críticas* recibirá información acerca de eventos importantes para la seguridad del equipo como, por ejemplo, la detección de objetos maliciosos o de actividades peligrosas en el sistema operativo. Las ventanas de notificaciones y mensajes emergentes críticos son de color rojo.
- En la sección *Notificaciones importantes* obtendrá información de aquellos eventos que pueden ser importantes para la seguridad del equipo, como la detección de objetos posiblemente infectados o de actividades sospechosas en el sistema operativo. Las ventanas de notificaciones y mensajes emergentes importantes son de color amarillo.
- *Notificaciones informativas*: le informan de eventos que no son importantes para la seguridad del equipo. Las ventanas de notificaciones y mensajes emergentes informativos son de color verde.

Si aparece en pantalla una notificación, debe seleccionar una de las opciones que en ella se sugieren. De forma predeterminada, la opción más adecuada es la que recomiendan los expertos de Kaspersky Lab.

Una notificación se puede cerrar automáticamente cuando se reinicia el equipo, cuando se cierra Kaspersky Anti-Virus o en modo en espera conectado en Windows 8. Las notificaciones sobre el inicio de aplicaciones se cierran al cabo de 1 hora. Cuando una notificación se cierra automáticamente, Kaspersky Anti-Virus lleva a cabo la acción recomendada predeterminada.

Las notificaciones no se muestran durante la primera hora de funcionamiento de la aplicación si ha comprado un equipo con Kaspersky Anti-Virus previamente instalado (distribución OEM). La aplicación procesa objetos detectados de acuerdo con las acciones recomendadas. Los resultados de este procesamiento se guardan en un informe.

Evaluación de los problemas de protección del equipo y resolución de los problemas de seguridad

Los problemas de protección del equipo se simbolizan mediante un indicador que se encuentra en la parte superior de la ventana principal de la aplicación. El verde indica que su equipo está protegido. El amarillo indica que hay problemas de la protección y el rojo indica serios riesgos para la seguridad de su equipo. Se recomienda corregir de inmediato los problemas y las amenazas contra la seguridad.

Al hacer clic en el indicador de la ventana principal de la aplicación, se abrirá la ventana **Centro de notificaciones** (consulte la figura siguiente), donde puede ver información detallada sobre el estado de protección del equipo y sugerencias para corregir los problemas y las amenazas detectados.

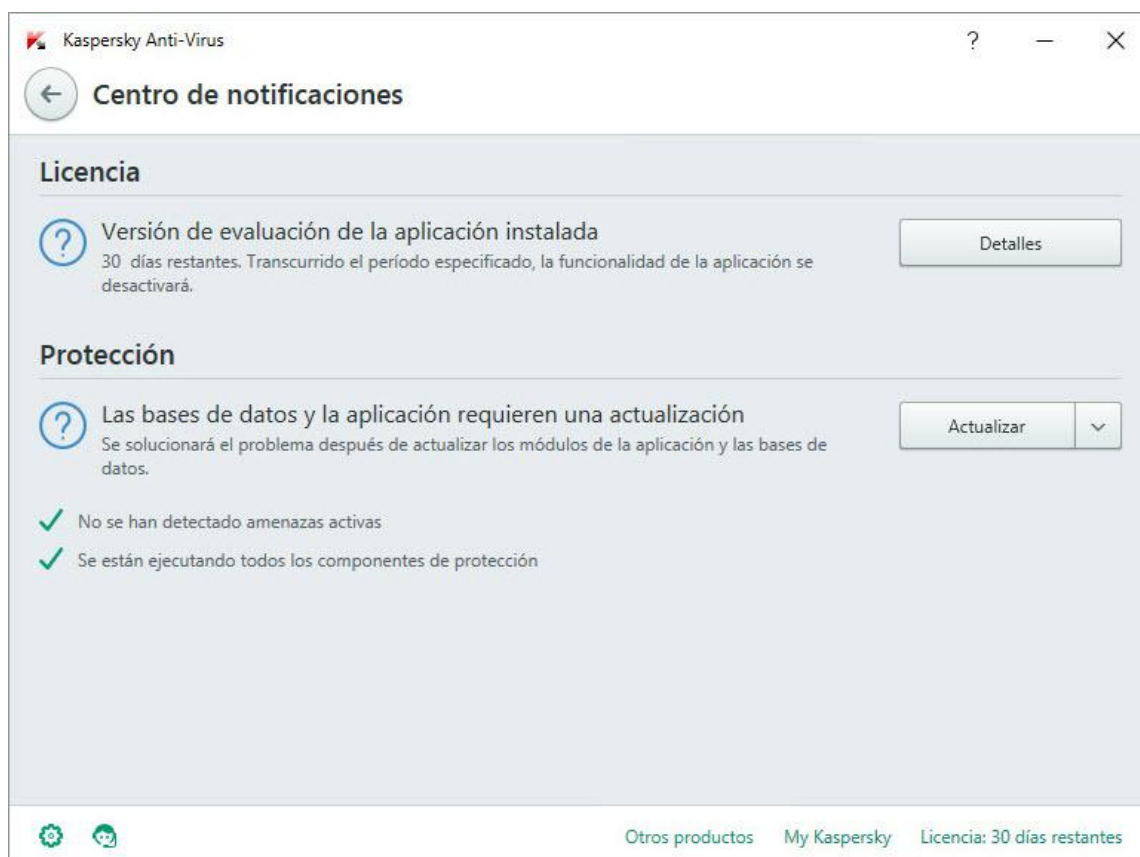


Figura 1. Ventana Centro de notificaciones

Los problemas con la protección se agrupan por categorías. Para cada problema, aparece una lista de medidas que puede tomar para solucionarlo.

Actualización de las bases de datos y los módulos de la aplicación

Esta sección contiene información sobre las actualizaciones de las bases de datos y los módulos de la aplicación.

En esta sección

Acerca de las actualizaciones de las bases de datos y los módulos de la aplicación	59
Inicio de una actualización de las bases de datos y los módulos de la aplicación	61

Acerca de las actualizaciones de las bases de datos y los módulos de la aplicación

El paquete de instalación de Kaspersky Anti-Virus incluye las bases de datos y los módulos de la aplicación. La aplicación utiliza estas bases de datos para proporcionar el *nivel de seguridad inicial*:

- Kaspersky Anti-Virus detecta la mayoría de las amenazas usando Kaspersky Security Network, que requiere conexión a Internet.
- Kaspersky Anti-Virus no detecta el software publicitario, los marcadores automáticos u software legítimo que los intrusos pueden usar para dañar su equipo o averiguar sus datos personales.

Para conseguir la protección completa, se recomienda actualizar las bases de datos y los módulos de la aplicación en cuanto la aplicación se haya instalado.

Las bases de datos y los módulos de programa se actualizan por fases:

1. Kaspersky Anti-Virus empieza a actualizar las bases de datos y los módulos de la aplicación según la configuración especificada: automáticamente, de forma planificada o a petición. La aplicación se pone en contacto con un origen de actualizaciones que almacene un paquete de actualización de las bases de datos y los módulos de la aplicación.
2. Kaspersky Anti-Virus compara las bases de datos existentes con las bases de datos disponibles en el origen de actualizaciones. Si las bases de datos son distintas, Kaspersky Anti-Virus descarga las partes que faltan de las bases de datos.

A continuación, la aplicación usa las bases de datos y los módulos de la aplicación actualizados para analizar el equipo en busca de virus y otras amenazas.

Puede usar los orígenes de actualizaciones siguientes:

- Servidores de actualización de Kaspersky Lab
- Servidor HTTP o FTP
- Carpeta de red

Las actualizaciones de bases de datos y los módulos de la aplicación están sujetos a las siguientes restricciones y especificidades:

- Las bases de datos se quedan obsoletas al cabo de dos días.
- Para descargar un paquete de actualización de los servidores de Kaspersky Lab, se requiere una conexión a Internet.
- Las actualizaciones de las bases de datos y los módulos de la aplicación no están disponibles en los casos siguientes:
 - La licencia ha caducado y el período de gracia o el modo de funcionalidad limitada no están disponibles.

- Se usa una conexión a Internet móvil de uso medido. Esta limitación se aplica a los equipos que se ejecutan con Microsoft Windows 8 o versiones más recientes de este sistema operativo si se activan las actualizaciones automáticas o planificadas y si se establece un límite de tráfico para una conexión móvil de uso medido. Si desea que la aplicación actualice las bases de datos y los módulos de la aplicación en este caso, desactive la casilla de verificación **Limitar el tráfico de las conexiones de uso medido** en **Configuración** → **Avanzado** → **Red**.
- La aplicación se usa bajo suscripción y la ha suspendido en el sitio web del proveedor de servicios.

Inicio de una actualización de las bases de datos y los módulos de la aplicación

- ▶ *Para iniciar una actualización de las bases de datos y los módulos de la aplicación,* seleccione el elemento **Actualizar** en el menú contextual del icono de la aplicación situado en el área de notificaciones de la barra de tareas.
- ▶ *Para ejecutar una actualización de las bases de datos y los módulos de la aplicación en la ventana principal de la aplicación, siga estos pasos:*
 1. Abra la ventana principal de la aplicación y haga clic en el botón **Actualizar**.

Se abrirá la ventana **Actualizar**.
 2. En la ventana **Actualizar**, haga clic en el botón **Ejecutar actualización**.

Análisis del equipo

Esta sección proporciona información sobre cómo analizar su equipo en busca de virus y otras amenazas.

En esta sección

Análisis completo	62
Análisis personalizado	63
Análisis rápido.....	64
Análisis de vulnerabilidades	65

Análisis completo

Durante el análisis completo, Kaspersky Anti-Virus analiza los siguientes objetos de forma predeterminada:

- Memoria del sistema
- Objetos cargados durante el inicio del sistema operativo
- Almacenamiento del sistema de copias de seguridad
- Discos duros y unidades extraíbles

Le recomendamos que ejecute un análisis completo inmediatamente después de instalar Kaspersky Anti-Virus en el equipo.

► *Para iniciar un análisis completo:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón **Analizar**.

Se abrirá la ventana **Análisis**.

3. En la ventana **Análisis**, seleccione la sección **Análisis completo**.
4. En la sección **Análisis completo**, haga clic en el botón **Ejecutar análisis**.

Kaspersky Anti-Virus iniciará el análisis completo de su equipo.

Análisis selectivo

Un análisis selectivo le permite analizar un archivo, una carpeta, o una unidad en busca de virus y otras amenazas.

Puede iniciar un análisis selectivo de los modos siguientes:

- Desde el menú contextual del objeto o
- Desde la ventana principal de la aplicación.

► *Para iniciar un análisis selectivo desde el menú contextual de un objeto:*

1. Abra el explorador de Microsoft Windows y vaya a la carpeta que contenga el objeto que desea analizar.
2. Haga clic con el botón derecho del ratón para abrir el menú contextual del objeto (figura inferior) y seleccione **Analizar en busca de virus**.



Figura 2. Menú contextual del objeto

► *Para iniciar un análisis selectivo desde la ventana principal de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón **Analizar**.
Se abrirá la ventana **Análisis**.
3. En la ventana **Análisis**, seleccione la sección **Análisis selectivo**.
4. Especifique los objetos que desea analizar de una de las siguientes formas:
 - Arrastre los objetos a la ventana **Análisis selectivo**.
 - Haga clic en el botón **Agregar** y especifique un objeto en la ventana de selección de archivo o carpeta que se abrirá.
5. Haga clic en el botón **Ejecutar análisis**.

Análisis rápido

Durante el análisis rápido, Kaspersky Anti-Virus analiza los siguientes objetos de forma predeterminada:

- Objetos cargados cuando se inicia el sistema operativo
- Memoria del sistema
- Sectores de arranque del disco

► *Para iniciar un análisis rápido:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón **Analizar**.
Se abrirá la ventana **Análisis**.
3. En la ventana **Análisis**, seleccione la sección **Análisis rápido**.
4. En la sección **Análisis rápido**, haga clic en el botón **Ejecutar análisis**.

Kaspersky Anti-Virus iniciará el análisis rápido de su equipo.

Análisis de vulnerabilidades

Vulnerabilidades son partes de código software sin proteger que pueden utilizar los intrusos de forma deliberada para sus propósitos, por ejemplo, para copiar datos de aplicaciones que utilizan código sin proteger. Analizar el equipo en busca de vulnerabilidades contribuye a revelar cualquier posible punto débil. Se aconseja corregir cualquier vulnerabilidad que se encuentre.

► *Para iniciar un análisis de vulnerabilidad:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Análisis de vulnerabilidades**.
3. En la ventana **Análisis de vulnerabilidades**, haga clic en el botón **Ejecutar análisis**.

Kaspersky Anti-Virus analizará su equipo en busca de vulnerabilidades.

Restauración de un objeto que la aplicación ha eliminado o desinfectado

Kaspersky Lab le recomienda que no restaure los objetos eliminados y desinfectados, puesto que pueden suponer una amenaza para su equipo.

Para restaurar un objeto eliminado o desinfectado, puede utilizar una copia de seguridad si la aplicación la creó durante un análisis del objeto.

Kaspersky Anti-Virus no desinfecta aplicaciones de la Tienda Windows. Si los resultados del análisis indican que esa aplicación es peligrosa, se elimina de su equipo.

Cuando se elimina una aplicación de la Tienda Windows, Kaspersky Anti-Virus no crea una copia de seguridad de ella. Para restaurar estos objetos, tendrá que utilizar las herramientas de recuperación del sistema operativo (para obtener más información, consulte la documentación del sistema operativo instalado en su equipo) o actualizar las aplicaciones mediante la Tienda Windows.

► *Para restaurar un archivo que la aplicación ha eliminado o desinfectado:*


1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Cuarentena**.
3. En la ventana **Cuarentena** que se abre, seleccione el archivo requerido en la lista y haga clic en el botón **Restaurar**.

Configuración de Antivirus de correo

Kaspersky Anti-Virus permite analizar mensajes de correo electrónico en busca de objetos peligrosos mediante el componente Antivirus de correo. El Antivirus de correo se inicia a la vez que el sistema operativo y permanece en la RAM constantemente, analizando todos los mensajes de correo electrónico que se envían o se reciben por medio de los protocolos POP3, SMTP, IMAP y NNTP, así como por medio de conexiones cifradas (SSL) por medio de POP3, SMTP e IMAP.

De forma predeterminada, Antivirus de correo analiza tanto los mensajes entrantes como los salientes. Si fuera necesario, puede activar el análisis de los mensajes entrantes solamente.

► *Para configurar Antivirus de correo:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la parte izquierda de la ventana, en la sección **Protección**, seleccione el componente Antivirus de correo.

La configuración de Antivirus de correo aparecerá en la ventana.

4. Asegúrese de que la opción en la parte superior de la ventana está activada para habilitar el Antivirus de correo.
5. Seleccione un nivel de seguridad:
 - **Recomendado.** Cuando se define este nivel de seguridad, Antivirus del correo analiza los mensajes entrantes y salientes, y realiza análisis heurísticos con el nivel de detalle **Análisis medio**.
 - **Bajo.** Si selecciona este nivel de seguridad, Antivirus de correo analizará únicamente los mensajes entrantes y no analizará los archivos adjuntos.

- **Alto.** Cuando se define este nivel de seguridad, Antivirus del correo analiza los mensajes entrantes y salientes, y realiza análisis heurísticos con el nivel de detalle **Análisis profundo.**

6. En la lista desplegable **Acción al detectar una amenaza**, seleccione la acción que debe realizar Antivirus de correo cuando se detecte un objeto infectado (por ejemplo, desinfectar).

Si no se detectan amenazas en un mensaje de correo electrónico, o si todos los objetos se han desinfectado correctamente, el mensaje vuelve a estar disponible. Si el componente no puede desinfectar un objeto, Antivirus de correo cambiará el nombre del objeto o lo eliminará del mensaje y agregará al asunto del mensaje una notificación de que Kaspersky Anti-Virus ha procesado dicho mensaje. Antes de eliminar un objeto, Kaspersky Anti-Virus crea una copia de seguridad y la coloca en Cuarentena (consulte la sección "Restauración de un objeto que la aplicación ha eliminado o desinfectado" en la página [66](#)).

Si Kaspersky Anti-Virus detecta la contraseña del archivo comprimido en el texto del mensaje durante el análisis, esta se utilizará para analizar su contenido en busca de software malicioso. La contraseña no se guarda. El archivo comprimido se descomprime antes del análisis. Si la aplicación se bloquea al descomprimir el archivo comprimido, puede eliminar manualmente los archivos descomprimidos en la ruta siguiente: %systemroot %\temp. Los archivos tienen el prefijo PR.

Protección de datos personales en Internet

Esta sección proporciona información sobre cómo hacer su navegación en Internet segura y proteger sus datos contra robos.

En esta sección

Acerca de la protección de datos personales en Internet	69
Acerca del Teclado en pantalla	70
Inicio del Teclado en pantalla	72
Comprobación de seguridad de un sitio web	73

Acerca de la protección de datos personales en Internet

Kaspersky Anti-Virus le ayuda a proteger sus datos personales frente a robos:

- Contraseñas, nombres de usuario y otros datos de registro.
- Números de cuenta y de tarjetas bancarias.

Kaspersky Anti-Virus incluye componentes y herramientas que le permiten proteger sus datos personales frente a robos por parte de delincuentes que utilizan métodos como el phishing o la interceptación de los datos introducidos con el teclado.

La funcionalidad Anti-Phishing protege frente a las actividades fraudulentas y está implementada en los componentes Antivirus Internet y Antivirus para chat. Active estos componentes para garantizar una protección exhaustiva frente al fraude.

La protección frente a la interceptación de datos introducidos desde el teclado se realiza gracias a Teclado en pantalla.

El asistente de limpieza de rastros privados borra del equipo toda información sobre las actividades del usuario.

Acerca del Teclado en pantalla

Al navegar en Internet, a menudo tendrá que introducir sus datos personales o su nombre de usuario y contraseña. Esto sucede, por ejemplo, durante el registro de cuentas en sitios web y servicios bancarios o tiendas en línea.

Existe el peligro de que los datos personales puedan ser interceptados por herramientas de interceptación del teclado físico o lectores de teclado (keyloggers), es decir, programas que registran la pulsación de teclas. La herramienta Teclado en pantalla evita la interceptación de los datos que introduce por teclado.

Muchos programas clasificados como software espía pueden realizar capturas de pantalla, que se transmiten automáticamente a un intruso para su posterior análisis y para robar los datos personales del usuario. Teclado en pantalla protege los datos personales introducidos frente a los intentos de interceptarlos mediante capturas de pantalla.

El Teclado en pantalla tiene las funciones siguientes:

- Puede pulsar los botones del Teclado en pantalla con el ratón.
- A diferencia de los teclados físicos, es imposible presionar varias teclas simultáneamente en el Teclado en pantalla. Esta es la razón por la cual las combinaciones de teclas (como **ALT + F4**) requieren que haga clic en la primera tecla (por ejemplo, **ALT**), a continuación en la segunda (por ejemplo, **F4**) y, por último, la primera tecla otra vez. El segundo clic en la tecla funciona igual que la liberación de la tecla en un teclado físico.
- Puede cambiar el idioma del Teclado en pantalla utilizando el mismo acceso directo especificado en la configuración del sistema operativo para el teclado físico. Para ello, haga clic con el botón derecho del ratón en la otra tecla (por ejemplo, si se ha configurado el atajo **ALT IZQ + MAYÚS** en el sistema operativo para cambiar el idioma del teclado, haga clic con el botón izquierdo del ratón en la tecla **ALT IZQ** y, a continuación, haga clic con el botón derecho del ratón en la tecla **MAYÚS**).

Para garantizar la protección de los datos introducidos a través del Teclado en pantalla, reinicie el equipo después de instalar Kaspersky Anti-Virus.

El uso del Teclado en pantalla tiene las siguientes limitaciones:

- El Teclado en pantalla evita la interceptación de datos personales solamente cuando se utiliza con los navegadores Microsoft Internet Explorer, Mozilla Firefox o Google Chrome. Cuando utilice otros navegadores, el Teclado en pantalla no protegerá los datos personales que introduzca frente a su interceptación.
- El Teclado en pantalla no está disponible en el navegador Microsoft Internet Explorer (versiones 10 y 11) con la nueva interfaz de usuario de Windows. En este caso, se recomienda abrir el Teclado en pantalla desde la interfaz de Kaspersky Anti-Virus.
- El Teclado en pantalla no puede proteger sus datos personales si el sitio web que requiere la entrada de estos datos se piratea, porque en este caso la información la obtienen los intrusos directamente del sitio web.
- El Teclado en pantalla no evita las capturas de pantalla que se realizan pulsando la tecla **IMP PANT** u otras combinaciones de teclas especificadas en la configuración del sistema operativo.
- Al ejecutar el Teclado en pantalla, la función Autocompletar de Microsoft Internet Explorer deja de funcionar, ya que este sistema de entrada automática de datos puede permitir a los ciberdelincuentes interceptar los datos.

La lista anterior describe las principales restricciones de la funcionalidad para la protección de la entrada de datos. La lista completa de las restricciones se encuentra disponible en un artículo publicado en el sitio web de Soporte Técnico de Kaspersky Lab (<http://support.kaspersky.com/sp/12000>). Este artículo enumera restricciones en la Entrada segura desde el teclado en Kaspersky Internet Security, estas restricciones también se aplican al Teclado en pantalla en Kaspersky Anti-Virus.

Inicio del Teclado en pantalla

Puede abrir el Teclado en pantalla de las siguientes formas:

- En el menú contextual del icono de la aplicación en el área de notificaciones de la barra de tareas.
 - Desde la ventana de la aplicación
 - En la barra de herramientas de Microsoft Internet Explorer, Mozilla Firefox o Google Chrome
 - Presionando una combinación de teclas
- *Para abrir Teclado en pantalla desde el menú contextual del icono de la aplicación del área de notificaciones de la barra de tareas:*

Seleccione **Teclado en pantalla** (consulte la siguiente figura).




Figura 3. Menú contextual de Kaspersky Anti-Virus

- *Para abrir Teclado en pantalla desde la ventana de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón **Teclado en pantalla**

- *Para abrir el Teclado en pantalla desde la barra de herramientas de Google Chrome, Microsoft Internet Explorer o Mozilla Firefox:*

1. Haga clic en el botón  **Kaspersky Protection** en la barra de herramientas del navegador.
2. Seleccione el elemento **Teclado en pantalla** en el menú que se abre.

► *Para abrir Teclado en pantalla con el teclado físico:*




Pulse el atajo **CTRL+ALT+MAYÚS+P**.

Comprobación de seguridad de un sitio web

Kaspersky Anti-Virus permite comprobar la seguridad de un sitio web antes de que haga clic en un vínculo para abrirlo. Los sitios web se comprueban con el *Supervisor de direcciones URL*.

El Supervisor de direcciones URL no está disponible en el navegador Microsoft Internet Explorer (versiones 10 y 11) con la nueva interfaz de usuario de Windows.


El Supervisor de direcciones URL comprueba los vínculos de la página web que se abre con Microsoft Internet Explorer, Google Chrome y Mozilla Firefox. Kaspersky Anti-Virus muestra uno de los siguientes iconos al lado de cada vínculo comprobado:

-  : si la página web abierta por medio del vínculo es segura según Kaspersky Lab
-  : si no hay información sobre el estado de seguridad de la página web abierta por medio del vínculo
-  : si la página web abierta por medio del vínculo es peligrosa según Kaspersky Lab.

Para ver una ventana emergente con más detalles sobre el vínculo, coloque el cursor sobre el icono correspondiente.

De forma predeterminada, Kaspersky Anti-Virus comprueba solo los vínculos en los resultados de búsqueda. Puede activar la comprobación de vínculos en todos los sitios web.

► *Para permitir la comprobación de vínculos en sitios web:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la sección **Protección**, seleccione la subsección **Antivirus Internet**.

La ventana muestra la configuración de Antivirus Internet.

4. En la parte inferior de la ventana, haga clic en el vínculo **Configuración avanzada**. Se abrirá la ventana de configuración avanzada de Antivirus Internet.
5. En la sección **Supervisor de direcciones URL**, seleccione la casilla de verificación **Comprobar direcciones URL**.
6. Si desea que Kaspersky Anti-Virus analice el contenido de todos los sitios web, seleccione **En todos los sitios web excepto en aquellos especificados**.
7. Si es preciso, especifique las páginas web en las que confía en la ventana **Exclusiones**. Abra esta ventana haciendo clic en el vínculo **Administrar exclusiones**. Kaspersky Anti-Virus no analiza el contenido de las páginas web especificadas o de las conexiones cifradas con los sitios web especificados.
8. Si desea que Kaspersky Anti-Virus compruebe únicamente el contenido de páginas web específicas:
 - a. Seleccione **Solo en sitios web especificados**.
 - b. Haga clic en el vínculo **Configurar sitios web seleccionados** para abrir la ventana **Sitios web seleccionados**.
 - c. Haga clic en el botón **Agregar**.
 - d. Introduzca la dirección de la página web cuyo contenido desea comprobar.
 - e. Seleccione un estado de comprobación para la página web (si el estado es *Activo*, Kaspersky Anti-Virus comprobará el contenido de la página web).
 - f. Haga clic en el botón **Agregar**.

La página web especificada aparecerá en la lista de la ventana **Sitios web seleccionados**. Kaspersky Anti-Virus comprobará las URL de esta página web.

9. Si desea definir la configuración avanzada para la comprobación de direcciones URL, en la ventana **Configuración avanzada de Antivirus Internet** de la sección **Supervisor de direcciones URL**, haga clic en el vínculo **Configurar Supervisor de direcciones URL** para abrir la ventana **Supervisor de direcciones URL**.
10. Si desea que Kaspersky Anti-Virus le advierta de la seguridad de los vínculos en todas las páginas web, en la sección **Direcciones URL comprobadas** seleccione **Todas las URL**.
11. Si desea que Kaspersky Anti-Virus muestre información sobre si un vínculo pertenece a una categoría específica de contenido de sitio web (por ejemplo, *Blasfemias y lenguaje obsceno*):
 - a. Seleccione la casilla de verificación **Mostrar información sobre las categorías de contenidos de sitios web**.
 - b. Seleccione las casillas de verificación junto a las categorías de contenido del sitio web cuya información desea que aparezca como comentario.

Kaspersky Anti-Virus comprueba los vínculos en las páginas web especificadas y muestra información sobre las categorías de los vínculos de acuerdo con la configuración actual.

Eliminación de rastros de actividad en el equipo y en Internet

Las acciones realizadas por los usuarios en un equipo se registran en el sistema operativo. Se guarda la siguiente información:

- Detalles acerca de las búsquedas realizadas por los usuarios y de los sitios web visitados
- Información sobre aplicaciones iniciadas, así como archivos abiertos y guardados.
- Entradas del registro de eventos de Microsoft Windows.
- Otra información sobre la actividad del usuario.

Los intrusos y las personas no autorizadas podrían acceder a los datos confidenciales contenidos en la información relativa a las acciones que haya realizado anteriormente el usuario.

Kaspersky Anti-Virus incluye el asistente de limpieza de rastros privados que limpia los rastros de actividad de usuario en el sistema operativo.

► *Para ejecutar el asistente de limpieza de rastros privados:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Limpieza de rastros privados** para ejecutar el asistente de limpieza de rastros privados.

El asistente consta de una serie de páginas (pasos) por los que usted puede navegar mediante los botones **Atrás** y **Siguiente**. Para cerrar el asistente cuando haya concluido, haga clic en el botón **Finalizar**. Para interrumpir el asistente en cualquier momento, utilice **Cancelar**.

Examinemos más detalladamente los pasos del asistente.

Paso 1. Inicio del asistente

Asegúrese de que la casilla de verificación **Buscar rastros de actividad de usuario** esté seleccionada. Haga clic en el botón **Siguiente** para iniciar el asistente.

Paso 2. Búsqueda de rastros de actividad

Este asistente busca rastros de actividad dentro de su equipo. La búsqueda puede tardar un momento. Cuando la búsqueda finaliza, el asistente procede automáticamente al paso siguiente.

Paso 3. Selección de acciones de limpieza de rastros privados

Cuando la búsqueda finalice, el asistente le informará sobre los rastros de actividad detectados y preguntará qué acciones se deben realizar para eliminarlos (consulte la siguiente figura).

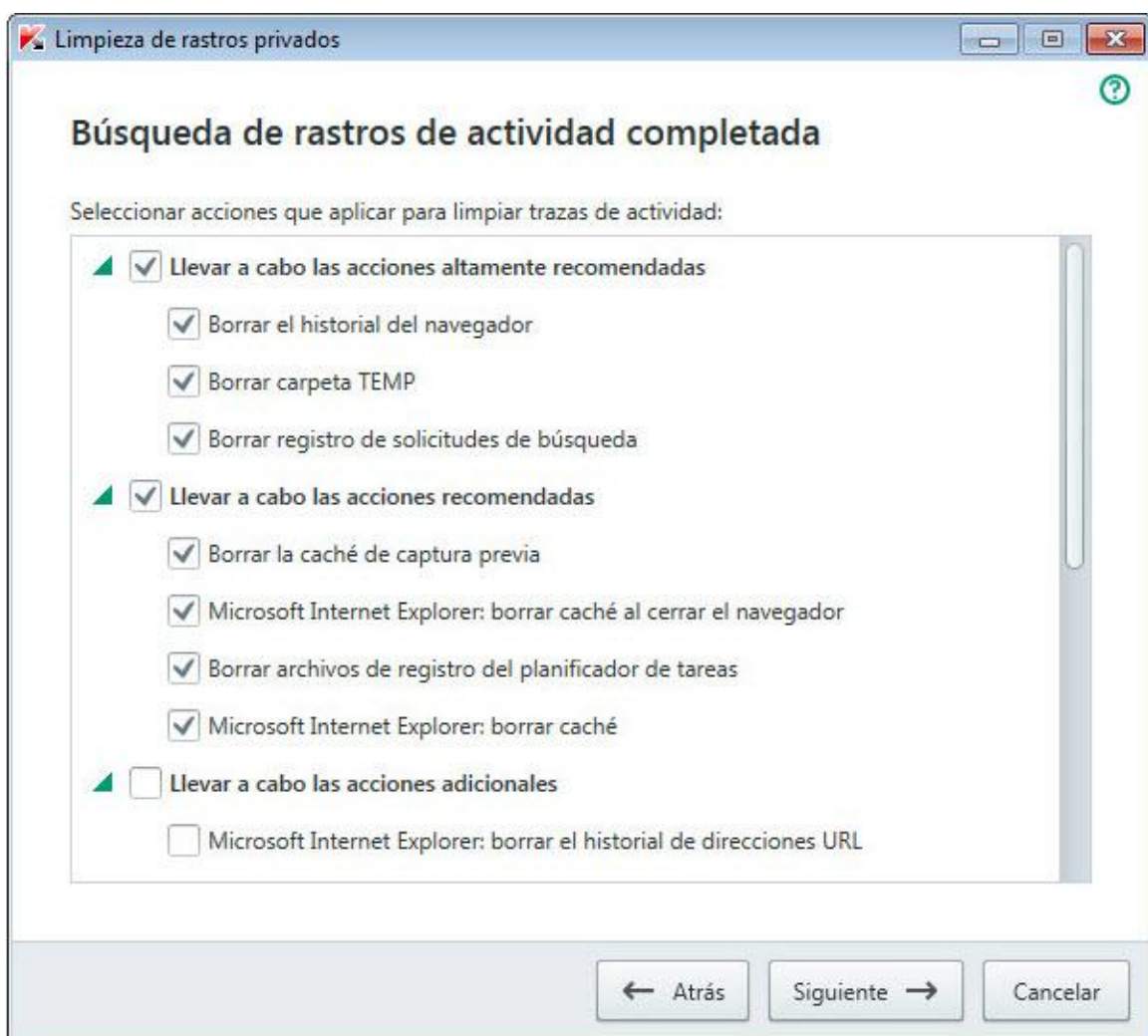


Figura 4. Rastros de actividad encontrados y recomendaciones para su eliminación

Para visualizar las acciones de un grupo, haga clic en el icono ►, a la izquierda del nombre del grupo.

Para que el asistente realice una acción determinada, a la izquierda de una acción, seleccione la casilla de verificación correspondiente. De forma predeterminada, el asistente realiza todas las acciones recomendadas y recomendadas fuertemente. Si no desea realizar una acción determinada, desactive la casilla de verificación asociada.

Se recomienda encarecidamente no desactivar las casillas seleccionadas de forma predeterminada; de lo contrario, su equipo quedará expuesto a amenazas.

Cuando haya definido las acciones que debe realizar el asistente, haga clic en el botón **Siguiente**.

Paso 4. Limpieza de rastros privados

El asistente llevará a cabo las acciones seleccionadas durante el paso anterior. La eliminación de rastros de actividad puede llevar cierto tiempo. Para limpiar ciertos rastros de actividad, puede ser necesario reiniciar el equipo. En ese caso, el asistente le informará de ello.

Cuando finalice la limpieza, el asistente procede automáticamente al paso siguiente.

Paso 5. Fin del asistente

Haga clic en **Finalizar** para cerrar el asistente.

Gestión remota de la protección del equipo

Esta sección describe cómo puede gestionar la protección de su equipo de forma remota con Kaspersky Anti-Virus instalado.

En esta sección

Información sobre la gestión remota de la protección del equipo	79
Acerca de My Kaspersky Account.....	80
Acceso a la gestión remota de la protección del equipo	81

Información sobre la gestión remota de la protección del equipo

Si un equipo tiene Kaspersky Anti-Virus instalado, puede gestionar la protección del equipo de forma remota. La protección del equipo se puede gestionar de forma remota mediante el portal de My Kaspersky. Para gestionar la protección del equipo de forma remota, regístrese en el portal My Kaspersky, inicie sesión en My Kaspersky y vaya a la sección **Mis dispositivos**.

El portal My Kaspersky le permite realizar las tareas siguientes relacionadas con la seguridad del equipo:

- Consultar la lista de problemas de seguridad del equipo y corríjalos de forma remota
- Analizar el equipo para detectar virus y otras amenazas
- Actualizar las bases de datos y los módulos de aplicación
- Configurar los componentes de Kaspersky Anti-Virus

Si se inicia un análisis del equipo desde el portal de My Kaspersky, Kaspersky Anti-Virus procesa los objetos detectados automáticamente sin que tenga que hacer nada. Al detectar un virus u otra

amenaza, Kaspersky Anti-Virus intenta realizar una desinfección sin reiniciar el equipo. Si la desinfección sin el reinicio del equipo no es posible, la lista de problemas de seguridad del equipo del portal de My Kaspersky muestra un mensaje acerca de que el equipo debe reiniciarse para llevar a cabo la desinfección.

Si la lista de objetos detectados en el portal de My Kaspersky incluye más de 10 elementos, estos se agruparán. En este caso, los objetos detectados solo se pueden procesar juntos mediante el portal sin la posibilidad de examinar cada objeto por separado. Para ver los objetos por separado en este caso, se recomienda usar la interfaz de la aplicación instalada en el equipo.

Existe información de uso del portal detallada disponible en la ayuda del portal de My Kaspersky (<https://help.kaspersky.com/KPC/1.0/es-ES/index.htm>).

Acerca de cuenta My Kaspersky

Se requiere una *My Kaspersky Account* para iniciar sesión en el portal My Kaspersky <https://center.kaspersky.com> y poder utilizarlo, así como ciertas aplicaciones de Kaspersky Lab.

Si aún no tiene una cuenta My Kaspersky, la puede crear en el portal o mediante aplicaciones compatibles con este. También puede usar cuentas empleadas para otros recursos de Kaspersky Lab para iniciar sesión en el portal.

Al crear una cuenta de My Kaspersky, debe especificar una dirección de correo electrónico válida y configurar una contraseña. La contraseña debe contener al menos 8 caracteres, un número, una letra mayúscula y una letra latina minúscula. No se admiten espacios en blanco.

Si la contraseña es demasiado poco segura o común, no se creará la cuenta.

Al crear una cuenta, podrá especificar una pregunta secreta. Esta pregunta proporciona seguridad adicional cuando se recupera una contraseña olvidada.

Una vez creada su cuenta My Kaspersky, recibirá un mensaje de correo electrónico con un vínculo para activarla.

Active su cuenta My Kaspersky en el plazo de una semana con el enlace del correo electrónico o se eliminará la cuenta.

Acceso a la gestión remota de la protección del equipo

► *Para continuar con la gestión remota de la protección del equipo, realice lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Gestión en línea**.
3. En la ventana **Gestión en línea**, haga clic en el botón **Conectar el equipo con My Kaspersky**.

El formulario de inicio de sesión del portal de My Kaspersky se carga en la ventana **Gestión en línea**, a menos que ya haya iniciado sesión. Complete los campos e inicie sesión en el portal My Kaspersky.

La conexión al portal de My Kaspersky puede fallar debido a un mal funcionamiento del portal. Cuando esto sucede, Kaspersky Anti-Virus muestra una notificación sobre los problemas experimentados por el portal de My Kaspersky que está solucionando el personal de Kaspersky Lab. Si no se puede conectar al portal de My Kaspersky porque el portal no funciona correctamente, intente volver a conectarse más tarde.

La página del portal de My Kaspersky con la sección **Mis dispositivos** se abre en la ventana del navegador de forma predeterminada.


Reserva de los recursos del sistema operativo para videojuegos

Cuando se ejecuta Kaspersky Anti-Virus en modo de pantalla completa con otras aplicaciones (en particular, juegos) de forma simultánea, se pueden producir los siguientes problemas:

- El rendimiento de la aplicación o del juego disminuye debido a la falta de recursos de sistema
- Las ventanas de notificación de Kaspersky Anti-Virus distraen al usuario del juego

Para evitar cambiar la configuración de Kaspersky Anti-Virus manualmente cada vez que cambie al modo de pantalla completa, puede utilizar el perfil para juegos. Cuando se activa el perfil para juegos, al cambiar al modo de pantalla completa, se cambian automáticamente los ajustes de todos los componentes de Kaspersky Anti-Virus para asegurar un funcionamiento óptimo del sistema en ese modo. Cuando salga del modo de pantalla completa, los ajustes de la aplicación vuelven a los valores iniciales que se utilizaban antes de activar el modo de pantalla completa.

► *Para activar el Perfil para juegos:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la parte izquierda de la ventana, seleccione la sección **Rendimiento**.

La ventana mostrará los ajustes de rendimiento de Kaspersky Anti-Virus.

4. En la sección **Perfil para juegos**, seleccione la casilla de verificación **Usar Perfil para juegos**.


Acceso protegido con contraseña a las opciones de administración de Kaspersky Anti-Virus

Varios usuarios con distintos niveles de experiencia y conocimientos informáticos pueden compartir un mismo equipo. Un acceso sin restricciones de distintos usuarios a Kaspersky Anti-Virus y su configuración podría poner en peligro el nivel de seguridad del equipo.

Para restringir el acceso a la aplicación, puede establecer una contraseña de administrador y especificar las acciones para las cuales se debe introducir esta contraseña:

- Configuración de los parámetros de la aplicación
- Salir de la aplicación
- Eliminación de la aplicación

► *Para proteger con contraseña el acceso al control de Kaspersky Anti-Virus:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la parte izquierda de la ventana, seleccione la sección **General** y haga clic en el vínculo **Configurar protección con contraseña** para abrir la ventana **Protección con contraseña**.
4. En la ventana que se abre, rellene los campos **Nueva contraseña** y **Confirmar la contraseña**.
5. En el grupo de configuración **Cobertura de la contraseña**, especifique las acciones de la aplicación a las que desea restringir el acceso.

No se pueden recuperar las contraseñas olvidadas. Si ha olvidado su contraseña, póngase en contacto con el servicio de Soporte técnico para recuperar el acceso a la configuración de Kaspersky Anti-Virus.

Suspensión y reanudación de la protección del equipo

La suspensión de la protección implica desactivar temporalmente todos los componentes.

Cuando se suspende la protección o Kaspersky Anti-Virus no se está ejecutando, se supervisa la actividad de las aplicaciones que se ejecutan en el equipo. La información sobre los resultados de la supervisión de la actividad de las aplicaciones se guarda en el sistema operativo. Cuando se reinicia Kaspersky Anti-Virus o se reanuda la protección, Kaspersky Anti-Virus usa esta información para proteger el equipo de las acciones maliciosas que puedan haberse realizado cuando la protección se suspendió o cuando Kaspersky Anti-Virus no estaba en ejecución. La información sobre los resultados de la supervisión de la actividad de las aplicaciones se almacena de forma indefinida. Esta información se eliminará si se quita Kaspersky Anti-Virus del equipo.

► *Para suspender la protección de su equipo:*

1. En el menú contextual del icono de la aplicación situado en el área de notificaciones de la barra de tareas, seleccione el elemento **Pausar la protección**.

Se abrirá la ventana **Pausar la protección** (consulte la figura siguiente).



Figura 5. Ventana Pausar la protección

2. En la ventana **Pausar la protección**, seleccione el intervalo de tiempo tras el cual se debe reanudar la protección:

- **Pausar durante el tiempo especificado:** La protección se activará cuando finalice el intervalo de tiempo seleccionado en la lista desplegable.
- **Pausar hasta el reinicio del equipo:** La protección se activará cuando se vuelva a iniciar el sistema operativo o la aplicación (siempre y cuando esté habilitado el parámetro de inicio automático de la aplicación).
- **Pausar:** La protección se reanudará cuando el usuario lo decida.

3. Haga clic en el botón **Pausar la protección** y confirme su elección en la ventana que se abrirá.

► *Para reanudar la protección del equipo:*


En el área de notificaciones de la barra de tareas, en el menú contextual del icono de la aplicación, seleccione **Reanudar la protección**.

Restablecimiento de los parámetros predeterminados de la aplicación

Puede restaurar en cualquier momento la configuración recomendada por Kaspersky Lab para Kaspersky Anti-Virus. Los parámetros se pueden restaurar utilizando el *asistente de configuración de la aplicación*.

Cuando el asistente concluye su operación, el nivel de seguridad **Recomendado** se establece para todos los componentes de protección.

► *Para ejecutar el asistente de configuración de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. Seleccione la sección **General**.

La ventana mostrará la configuración de Kaspersky Anti-Virus.

4. En la parte inferior de la ventana, en la lista desplegable **Administrar configuración**, seleccione **Restaurar configuración**.

Examinemos más detalladamente los pasos del asistente.

Paso 1. Inicio del asistente

Haga clic en **Siguiente** para continuar con el asistente.

Paso 2. Restaurar la configuración

En este paso, la configuración de la aplicación se restablece a la configuración predeterminada de Kaspersky Lab.

Paso 3. Finalización de la restauración

Para cerrar el asistente cuando haya completado su tarea, haga clic en el botón **Finalizar**.

Visualización del informe acerca del funcionamiento de una aplicación

Kaspersky Anti-Virus mantiene informes de funcionamiento para cada uno de los componentes de protección. Con un informe, puede obtener información estadística sobre el funcionamiento de la aplicación (por ejemplo, saber cuántos objetos maliciosos se han detectado y neutralizado durante un período de tiempo específico, cuántas veces se han actualizado las bases de datos y los módulos de la aplicación en el mismo período y mucho más).

► *Para ver el informe acerca del funcionamiento de una aplicación:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón **Informes**.

La ventana **Informes** muestra informes sobre el funcionamiento de la aplicación durante el día actual (en la parte izquierda de la ventana) y durante un período de tiempo en particular (en la parte derecha de la ventana).

3. Si desea consultar un informe detallado sobre el funcionamiento de la aplicación, en la parte superior de la ventana **Informes**, haga clic en el vínculo **Informes detallados**. Se abrirá la ventana **Informes detallados**.

La ventana **Informes detallados** mostrará los datos en forma de tabla. Para ver los informes de manera cómoda, puede seleccionar varias opciones de filtrado.

Aplicación de la configuración de la aplicación en otro equipo


Una vez que haya configurado la aplicación, podrá aplicar los parámetros en una copia de Kaspersky Anti-Virus instalada en otro equipo. Como consecuencia, la aplicación se configurará de forma idéntica en ambos equipos.

La configuración de la aplicación se guardará en un archivo de configuración que podrá mover de un equipo a otro.

Para mover la configuración de Kaspersky Anti-Virus de un equipo a otro, siga estos tres pasos:

1. Guarde la configuración de la aplicación en un archivo de configuración.
2. Mueva el archivo de configuración al otro equipo (por ejemplo, por correo electrónico o con una unidad extraíble).
3. Importe los parámetros del archivo de configuración a la copia de la aplicación instalada en el otro equipo.

► *Para exportar la configuración de la aplicación, haga lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la ventana **Configuración**, seleccione la sección **General**.
4. En la lista desplegable de **Administrar configuración**, seleccione **Exportar configuración**.


Se abrirá la ventana **Guardar como**.

5. Especifique un nombre para el archivo de configuración y haga clic en el botón **Guardar**.

La configuración de la aplicación se guardará en el archivo de configuración.

También puede exportar la configuración de la aplicación en la línea de comandos con el siguiente comando: `avp.com EXPORT <nombre_archivo>`.

► *Para importar la configuración en una copia de la aplicación instalada en otro equipo, haga lo siguiente:*

1. En el otro equipo, abra la ventana principal de la aplicación de Kaspersky Anti-Virus.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la ventana **Configuración**, seleccione la sección **General**.
4. En la lista desplegable de **Administrar configuración**, seleccione **Importar configuración**.

Se abrirá la ventana **Abrir**.

5. Especifique un archivo de configuración y haga clic en el botón **Abrir**.

La configuración se importará a la aplicación instalada en el otro equipo.

Participación en Kaspersky Security Network (KSN)

Kaspersky Anti-Virus utiliza la protección en la nube para mejorar la eficacia de la protección de su equipo. La protección en la nube se implementa con la infraestructura de Kaspersky Security Network, que utiliza los datos recibidos de usuarios de todo el mundo.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky Lab, que contiene información sobre la reputación de archivos, recursos web y software. El uso de datos de Kaspersky Security Network garantiza tiempos de respuesta más rápidos de Kaspersky Anti-Virus frente a nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce la posibilidad de falsos positivos.

La participación de los usuarios en Kaspersky Security Network permite a Kaspersky Lab recibir rápidamente información sobre tipos y fuentes de nuevas amenazas, desarrollar soluciones para neutralizarlas y minimizar el número de falsos positivos. La participación en Kaspersky Security Network permite acceder a las estadísticas de reputación de aplicaciones y sitios web.

Si participa en Kaspersky Security Network, enviará automáticamente a Kaspersky Lab información sobre la configuración de su sistema operativo y de las horas de inicio y de finalización de los procesos de Kaspersky Anti-Virus.


En esta sección

Activar y desactivar la participación en Kaspersky Security Network.....	90
Comprobación de la conexión a Kaspersky Security Network.....	91

Activar y desactivar la participación en Kaspersky Security Network

La participación en Kaspersky Security Network es voluntaria. Puede activar o desactivar el uso de Kaspersky Security Network (KSN) cuando instale Kaspersky Anti-Virus o en cualquier momento después de instalar la aplicación.

► *Para activar o desactivar la participación en Kaspersky Security Network:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abrirá la ventana **Configuración**.

3. En la sección **Adicional**, seleccione **Herramientas de protección y administración adicionales**.

La ventana muestra los detalles de Kaspersky Security Network y la configuración de la participación en Kaspersky Security Network.

4. Active o desactive la participación en Kaspersky Security Network mediante los botones **Activar** o **Desactivar**:

- Si desea participar en Kaspersky Security Network, haga clic en el botón **Activar**.

Se abrirá una ventana con el texto de la Declaración de Kaspersky Security Network. Si acepta los términos de la declaración, haga clic en el botón **Acepto**.

- Si no desea participar en Kaspersky Security Network, haga clic en el botón **Desactivar**.

Comprobación de la conexión a Kaspersky Security Network

La conexión a Kaspersky Security Network se puede perder por los siguientes motivos:

- Usted no participa en Kaspersky Security Network.
- Su equipo no está conectado a Internet.
- El estado de la clave actual no permite la conexión a Kaspersky Security Network.

El estado actual de la clave aparece en la ventana **Licencia**.

► *Para comprobar la conexión a Kaspersky Security Network:*

1. Abra la ventana principal de la aplicación.
2. En la lista desplegable **Más herramientas**, seleccione **Protección en la nube**.

La ventana **Protección en la nube** muestra el estado de conexión a Kaspersky Security Network.

Participación en el programa Proteger a un amigo

Con el programa Proteger a un amigo, puede obtener puntos de bonificación y cambiarlos por un código de activación para Kaspersky Anti-Virus. Para ello, debe publicar un vínculo de descarga en Twitter y en sus páginas de otras redes sociales. Este vínculo permite a sus amigos descargar el paquete de instalación de Kaspersky Anti-Virus con un período de evaluación ampliado. Cuando uno de sus amigos de Twitter o de otra red social descarga el paquete de instalación de Kaspersky Anti-Virus haciendo clic en el vínculo que ha publicado y, a continuación, activa la aplicación, usted recibe puntos de bonificación.

El número de puntos de bonificación depende de la versión de la aplicación.

Tenga en cuenta que la opción de la participación en el programa de protección de amigos podría no estar disponible para todos los usuarios.

Para iniciar sesión en su perfil dentro del programa Proteger a un amigo, debe usar el nombre de usuario y la contraseña de su cuenta My Kaspersky (consulte la sección "Acerca de cuenta My Kaspersky" en la página [80](#)). Si aún no tiene una cuenta My Kaspersky, puede crear una cuando abra su perfil de Proteger a un amigo por primera vez.

Un código de activación de bonificación también puede estar especificado en la aplicación como el nuevo código de activación.

Se puede usar un código de activación de bonificación para activar la aplicación en otro equipo (por ejemplo, puede regalárselo a otro usuario).

Los códigos de activación de bonificación no se pueden utilizar en los casos siguientes:

- La aplicación se usa bajo suscripción. En este caso, puede utilizar el código de activación de bonificación cuando caduque la suscripción. También puede aplicar su código de activación de bonificación en otro equipo.
- Ya hay un código de activación establecido como el nuevo código. En este caso, puede utilizar el código de activación de bonificación cuando caduque la licencia.

En esta sección

Crear una cuenta en portal My Kaspersky	94
Iniciar sesión en su perfil del programa Proteger a un amigo	95

Crear una cuenta en portal My Kaspersky

Para participar en el programa Proteger a un amigo, debe crear una cuenta en el portal My Kaspersky.

► *Para crear su cuenta de My Kaspersky:*

1. Abra la ventana principal de la aplicación y, en la parte inferior de la ventana, haga clic en el vínculo **My Kaspersky**.
2. Cree y active su cuenta de My Kaspersky:
 - a. En la parte derecha de la página web, introduzca una dirección de correo electrónico en el campo **Correo electrónico**.
 - b. Introduzca una contraseña y a continuación introdúzcala de nuevo para confirmarla en los campos **Contraseña** y **Confirme contraseña**. La contraseña debe contener, al menos, ocho caracteres.
 - c. Haga clic en el botón **Registrarse**.

La página web mostrará un mensaje que le informa de que su cuenta de My Kaspersky se ha registrado correctamente. Recibirá un correo electrónico con un vínculo en el que tendrá que hacer clic para activar la cuenta de My Kaspersky.

- d. Haga clic en el vínculo para activar su cuenta de My Kaspersky.

La página web mostrará un mensaje que le informa de que su cuenta de My Kaspersky se ha activado correctamente. Puede utilizar su cuenta de My Kaspersky recién creada para iniciar sesión en su perfil de Proteger a un amigo.

Iniciar sesión en su perfil del programa Proteger a un amigo

► *Para iniciar sesión en la página web con su perfil del programa Proteger a un amigo:*

1. Abra la ventana principal de la aplicación y, en la parte inferior de la ventana, haga clic en el vínculo **My Kaspersky**.

Se abrirá la página web, que contiene los campos para registrarse o iniciar sesión en portal My Kaspersky.

2. En la parte derecha de la página web, rellene los campos con la dirección de correo electrónico y la contraseña que especificó durante el registro de la cuenta de My Kaspersky.
3. Haga clic en el botón **Iniciar sesión**.
4. Vaya a la **sección Proteger a un amigo**.

Más información sobre las reglas de participación en el programa Proteger a un amigo en portal My Kaspersky.

Uso de la aplicación desde la línea de comandos

Puede utilizar Kaspersky Anti-Virus en la línea de comandos.

Sintaxis de la línea de comandos:

```
avp.com <command> [settings]
```

Para mostrar la ayuda sobre la sintaxis de la línea de comandos, introduzca el siguiente comando:

```
avp.com [ /? | HELP ]
```

Este comando le permite obtener la lista completa de los comandos que están disponibles para administrar Kaspersky Anti-Virus mediante la línea de comandos.

Para obtener ayuda sobre la sintaxis de un comando concreto, puede introducir alguno de los siguientes comandos:

```
avp.com <command> /?  
avp.com HELP <command>
```

En la línea de comandos, puede consultar la aplicación tanto desde la carpeta de instalación de la aplicación como especificando la ruta completa a avp.com.

Cómo ponerse en contacto con el servicio de Soporte técnico

Esta sección describe las formas de obtener soporte técnico y las condiciones según las cuales está disponible.

En esta sección

Cómo conseguir soporte técnico	97
Soporte técnico por teléfono	98
Obtención de soporte técnico en el portal de My Kaspersky	98
Recopilación de información para Soporte técnico	99

Cómo conseguir soporte técnico

Si no encuentra una solución para el problema en la documentación de la aplicación o en una de las fuentes de información acerca de la aplicación, le recomendamos que se ponga en contacto con el Soporte técnico de Kaspersky Lab. Los especialistas de Soporte técnico responderán a sus preguntas acerca de la instalación y el uso de la aplicación.

Antes de ponerse en contacto con el Soporte Técnico, lea las reglas de soporte (<http://support.kaspersky.com/sp/support/rules>).

Puede ponerse en contacto con el servicio de Soporte técnico de cualquiera de las siguientes maneras:

- Por teléfono. Este método le permite consultar a nuestros especialistas desde Soporte técnico en lengua rusa o internacional.
- Envíe la solicitud desde el portal de My Kaspersky. Este método le permite ponerse en contacto con nuestros especialistas a través de la solicitud de consulta.

El soporte técnico solo está disponible para usuarios que hayan comprado una licencia para usar la aplicación. No se proporcionará soporte técnico a los usuarios de versiones de evaluación.

Soporte técnico por teléfono

Puede llamar al servicio de soporte técnico de cualquier zona del mundo. Puede encontrar información acerca de las formas de recibir soporte técnico en su región y los datos de contacto de Soporte técnico en el sitio web del Soporte técnico de Kaspersky Lab (<http://support.kaspersky.com/sp/b2c>).

Antes de ponerse en contacto con el Soporte Técnico, lea las reglas de soporte (<http://support.kaspersky.com/sp/support/rules>).

Obtención de soporte técnico en el portal de My Kaspersky

My Kaspersky (<https://my.kaspersky.com/en/index.html?LANG=sp>) es un recurso en línea universal para administrar la protección de sus dispositivos y los códigos de activación de las aplicaciones de Kaspersky Lab, así como para solicitar soporte técnico.

Para acceder al portal de My Kaspersky, se tiene que registrar. Para ello, indique su dirección de correo electrónico y cree una contraseña.

Puede recibir soporte técnico mediante el portal de My Kaspersky de las formas siguientes:

- Enviar solicitudes por correo electrónico al servicio de Soporte técnico
- Contactar con Soporte técnico sin necesidad de utilizar el correo electrónico
- Realizar un seguimiento del estado de sus solicitudes en tiempo real

También puede consultar el historial completo de sus solicitudes de soporte técnico.

Envío de solicitudes por correo electrónico al servicio de Soporte técnico

Tiene que especificar la información siguiente en la solicitud por correo electrónico al servicio de Soporte técnico:

- Asunto del mensaje
- Nombre de aplicación y número de versión

- Nombre del sistema operativo y número de versión
- Descripción del problema

Un especialista del servicio de Soporte técnico enviará una respuesta a su pregunta al portal de My Kaspersky y a la dirección de correo electrónico que haya especificado al registrarse.

Recopilación de información para Soporte técnico

Después de notificar un problema a los especialistas de Soporte técnico, estos podrían solicitarle que cree un informe que contenga información sobre su sistema operativo y lo envíe a Soporte técnico. Los especialistas de Soporte técnico también podrían pedir que cree un archivo de depuración. El archivo de depuración permite un seguimiento paso a paso de la ejecución de comandos de la aplicación y determinar el momento en el funcionamiento de la aplicación en el que se produce el error.

Una vez que los especialistas de Soporte técnico hayan analizado los datos enviados, pueden crear un script de AVZ y enviárselo. La ejecución de scripts de AVZ le permite analizar procesos activos y el sistema en busca de código malintencionado, desinfectar o borrar archivos infectados, y crear informes sobre los resultados de los análisis del sistema.

Con el fin de proporcionar una mejor asistencia sobre los problemas relacionados con el funcionamiento de la aplicación, los especialistas de Soporte técnico pueden pedirle que cambie de forma temporal la configuración de la aplicación para fines de depuración mientras se realiza el diagnóstico. Para ello, puede que deba realizar las siguientes acciones:

- Activar la recopilación de información de diagnóstico ampliada
- Configurar componentes individuales de la aplicación cambiando parámetros especiales a los que no se puede acceder mediante la interfaz de usuario estándar
- Volver a configurar el almacenamiento y el envío de la información de diagnóstico recopilada
- Configurar la interceptación de tráfico de red y el guardado del tráfico de red en un archivo

Los especialistas de Soporte técnico le proporcionarán toda la información necesaria para realizar estas acciones (instrucciones paso a paso, parámetros que cambiar, scripts, funciones adicionales de la línea de comandos, depuración de módulos, herramientas especiales, etc.) y le informarán sobre qué datos se recopilarán para fines de depuración. Una vez recopilada la información de diagnóstico ampliada, se guarda en el equipo del usuario. Los datos recopilados no se envían automáticamente a Kaspersky Lab.


Se recomienda realizar las acciones anteriores únicamente con la orientación de un especialista de Soporte técnico y cuando haya recibido las instrucciones para hacerlo. La modificación de parámetros de la aplicación por su cuenta de una forma que no se haya descrito en la guía del administrador o que no hayan recomendado los especialistas de Soporte técnico puede causar ralentización y bloqueos del sistema operativo, reducir el nivel de protección del equipo y dañar la disponibilidad e integridad de la información procesada.

En esta sección

Creación de un informe de estado del sistema.....	100
Envío de archivos de datos	101
Contenido y almacenamiento de archivos de depuración.....	102
Ejecución de scripts de AVZ	103

Creación de un informe de estado del sistema

► *Para crear un informe de estado del sistema:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abre la ventana **Soporte**.

3. En la ventana que se abre, haga clic en el vínculo **Herramientas de soporte** para abrir la ventana **Herramientas de soporte**.


4. En la ventana que se abre, haga clic en el vínculo **Cómo crear un informe de estado del sistema operativo** para abrir un artículo de la Base de conocimientos que explica cómo crear un informe de estado del sistema operativo.
5. Siga las instrucciones del artículo de la Base de conocimientos.

Envío de archivos de datos

Después de crear los archivos de depuración y el informe de estado del sistema, debe enviarlos a los especialistas de Soporte técnico de Kaspersky Lab.

Tendrá que utilizar un número de solicitud para transferir archivos al servidor de Soporte Técnico (consulte la sección "Obtención de soporte técnico en el portal de My Kaspersky" en la página [98](#)). Este número estará disponible en el portal de My Kaspersky cuando tenga una solicitud activa.

► Para transferir archivos de datos al servidor de Soporte técnico:


1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abre la ventana **Soporte**.
3. Haga clic en el vínculo **Herramientas de soporte** para abrir la ventana **Herramientas de soporte**.
4. En la ventana que se abre, haga clic en el vínculo **Enviar informe a Soporte técnico** para abrir la ventana **Enviar informe**.
5. Seleccione las casillas de verificación junto a los datos que desee enviar a Soporte técnico.
6. Introduzca el número que Soporte técnico ha asignado a su solicitud.
7. Haga clic en el botón **Enviar informe**.

Los archivos de datos seleccionados se comprimen y se envían al servidor de Soporte técnico.

Si no podía enviar los archivos por algún motivo, puede almacenar los archivos de datos en su equipo y enviarlos más tarde desde el portal de My Kaspersky.

► *Para guardar los archivos de datos al disco duro:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abre la ventana **Soporte**.

3. En la ventana que se abre, haga clic en el vínculo **Herramientas de soporte** para abrir la ventana **Herramientas de soporte**.
4. En la ventana que se abre, haga clic en el vínculo **Enviar informe a Soporte técnico** para abrir la ventana **Enviar informe**.
5. Seleccione los tipos de datos que desea guardar en el disco:
 - **Información del sistema operativo**. Seleccione esta casilla de verificación para guardar en el disco información sobre el sistema operativo de su equipo.
 - **Datos recibidos para análisis**. Seleccione esta casilla de verificación para guardar en el disco los archivos de depuración de la aplicación. Haga clic en el vínculo **<number of files>**, **<data volume>** para abrir la ventana **Datos recibidos para análisis**. Seleccione las casillas de verificación correspondientes a los archivos de depuración que desea guardar.
6. Haga clic en el vínculo **Guardar informe** para abrir la ventana mediante la cual podrá guardar un archivo comprimido con los archivos de datos.
7. Especifique el nombre del archivo y confirme el guardado.

El archivo creado puede enviarse a Soporte técnico desde el portal de My Kaspersky.

Contenido y almacenamiento de archivos de depuración

Los archivos de depuración se almacenan en el equipo abiertamente durante siete días tras desactivar la escritura de archivos de depuración. Los archivos de depuración se eliminan permanentemente al cabo de siete días.

Los archivos de depuración se almacenan en la carpeta ProgramData\Kaspersky Lab.

El formato de los nombres de los archivos de depuración es el siguiente:


KAV<versión_fechaXX.XX_horaXX.XX_pidXXX.><tipo de archivo de depuración>.log.

Los archivos de depuración pueden contener datos confidenciales. Puede ver el contenido de un archivo de depuración abriéndolo en un editor de texto (como, por ejemplo, el Bloc de notas).

Ejecución de scripts de AVZ

No se recomienda modificar el contenido del script AVZ entregado por los expertos de Kaspersky Lab. Si se produce algún problema durante la ejecución de un script, póngase en contacto con Soporte técnico.

► *Para ejecutar un script de AVZ:*

1. Abra la ventana principal de la aplicación.
2. Haga clic en el botón , situado en la parte inferior de la ventana.

Se abre la ventana **Soporte**.
3. En la ventana que se abrirá, haga clic en el vínculo **Herramientas de soporte**.

Se abre la ventana **Herramientas de soporte**.
4. En la ventana que se abre, haga clic en el vínculo **Ejecutar script** para abrir la ventana **Ejecución de script**.
5. Copie el texto del script enviado por los especialistas de Soporte técnico, cópielo en el campo de entrada de la ventana que se abre y haga clic en el botón **Ejecutar**.

El script se ejecuta.

Si el script se ejecuta con éxito, el asistente se cerrará automáticamente. Si se produce un error durante la ejecución del script, el asistente muestra el mensaje correspondiente.

Limitaciones y advertencias

Kaspersky Anti-Virus presenta ciertas limitaciones que no suponen ningún impedimento para el funcionamiento de la aplicación.

Limitaciones al actualizar desde una versión anterior de la aplicación

Se podrá actualizar la aplicación si las siguientes versiones de Kaspersky Anti-Virus están instaladas en el equipo:

- Kaspersky Anti-Virus 2013
- Kaspersky Anti-Virus 2014
- Kaspersky Anti-Virus 2015
- Kaspersky Anti-Virus 2016

No se admiten las actualizaciones de la aplicación realizadas a partir de versiones anteriores.

Después de realizar una actualización desde una versión anterior de la aplicación, Kaspersky Anti-Virus se inicia automáticamente aunque el inicio automático de la aplicación esté desactivado en la configuración guardada. Posteriormente, cuando se reinicie el sistema operativo, Kaspersky Anti-Virus no si iniciará automáticamente si el inicio automático de la aplicación está desactivado en la configuración guardada.

Cuando se actualiza a partir de una versión anterior de Kaspersky Anti-Virus, se sustituirá los siguientes parámetros de configuración de la aplicación por los parámetros predeterminados:

- Configuración de visualización de Kaspersky Anti-Virus
- Planificación de análisis
- Participación en Kaspersky Security Network
- Nivel de protección de Antivirus de archivos
- Nivel de protección de Antivirus del correo

- Orígenes de actualizaciones
- Lista de direcciones web de confianza
- Configuración de Supervisor de direcciones URL

Limitaciones en el funcionamiento de determinados componentes y en el procesamiento automático de archivos

Los archivos infectados se procesan automáticamente según las reglas creadas por los especialistas de Kaspersky Lab. No puede modificar estas reglas manualmente. Las reglas se pueden actualizar después de una actualización de las bases de datos y módulos de la aplicación.

Limitaciones en la comprobación de certificados de sitios web y en los análisis de archivos

Cuando analice un archivo, la aplicación puede conectarse a Kaspersky Security Network para buscar información sobre el archivo. Si los datos de Kaspersky Security Network no pudieran recuperarse, la aplicación decide si el archivo está infectado en función de las bases de datos antivirus locales.

Limitaciones de la funcionalidad System Watcher

La protección contra herramientas de cifrado (software malicioso que cifra los archivos del usuario) tiene las siguientes limitaciones:

- La carpeta Temp del sistema se emplea como apoyo para esta funcionalidad. Si la unidad del sistema de la carpeta Temp no dispone espacio en disco suficiente para crear archivos temporales, no se ofrecerá protección contra herramientas de cifrado. En ese caso, la aplicación no muestra ninguna notificación acerca de que no se están creando copias de seguridad de los archivos, es decir, que no se ofrece protección.
- Los archivos temporales se eliminan automáticamente cuando se cierra Kaspersky Anti-Virus o se desactiva el componente System Watcher.
- En caso de un cierre de emergencia de Kaspersky Anti-Virus, los archivos temporales no se eliminan automáticamente. Para eliminar los archivos temporales, quite la carpeta Temp de forma manual. Para ello, abra la ventana **Ejecutar** (comando **Ejecutar** en Windows XP) y, en el campo **Abrir**, escriba %TEMP%. Haga clic en **Aceptar**.

Limitaciones del análisis de conexiones cifradas

Debido a las limitaciones técnicas de la implantación de algoritmos de análisis, el análisis de conexiones cifradas no admite ciertas extensiones del protocolo TLS 1.0 y versiones posteriores (en particular, NPN y ALPN). Las conexiones mediante estos protocolos pueden estar limitadas. Los navegadores compatibles con el protocolo SPDY usan el protocolo HTTP en TLS en lugar del SPDY aunque el servidor con el que se haya establecido la conexión admita SPDY. Esto no afecta al nivel de seguridad de la conexión. Si el servidor admite solamente el protocolo SPDY y no se puede establecer la conexión mediante el protocolo HTTPS, la aplicación no supervisa la conexión establecida.

Kaspersky Anti-Virus no admite el procesamiento de tráfico de proxy HTTPS/2. La aplicación no procesa el tráfico transmitido mediante las extensiones del protocolo HTTP/2.

Kaspersky Anti-Virus solo supervisa las conexiones protegidas que puede descifrar. La aplicación no supervisa las conexiones agregadas a la lista de exclusiones (vínculo **Sitios web** de la ventana **Configuración de red**). Los componentes siguientes descifran y analizan el tráfico cifrado de forma predeterminada:

- Antivirus Internet
- Supervisor de direcciones URL

Kaspersky Anti-Virus descifra el tráfico cifrado cuando el usuario está usando el navegador Google Chrome si se ha desactivado la extensión Kaspersky Protection en este navegador.

Información sobre el procesamiento de archivos infectados por parte de los componentes de la aplicación

De forma predeterminada, Kaspersky Anti-Virus puede eliminar archivos infectados que no se pueden desinfectar. Esto se puede realizar durante el procesamiento de archivos por parte de aplicaciones como Antivirus de correo, Antivirus de archivos, durante tareas de análisis y cuando System Watcher detecta actividad malintencionada de las aplicaciones.

Advertencia sobre cambios en la funcionalidad de Antivirus para chat

A partir de la versión de 2016 de Kaspersky Anti-Virus, el componente Antivirus para chat no analizará los mensajes transmitidos mediante el protocolo IRC.

Acerca de los datos personales contenidos en los archivos de informes

Los archivos de informes se almacenan localmente en su equipo.

Ruta de los archivos de informes: %allusersprofile%\Kaspersky Lab\AVP16.0.0\Report\Database.

Los informes se almacenan en los archivos siguientes:

- reports.db
- reports.db-wal
- reports.db-shm (no contiene datos personales)

Los archivos de informes se protegen contra accesos no autorizados si se activa la autoprotección en Kaspersky Anti-Virus. Si la autoprotección está desactivada, los archivos de informes no se protegen.

Los archivos de informes pueden contener datos personales obtenidos durante el funcionamiento de los componentes de protección como, por ejemplo, Antivirus de archivos, Antivirus de correo y Antivirus Internet.

Los archivos de informes pueden contener los datos personales siguientes:

- La dirección IP del dispositivo del usuario
- El historial de navegación en línea
- Las versiones del navegador y el sistema operativo
- Los nombres de las cookies, así como otros archivos y rutas que permitan acceder a ellas
- Dirección de correo electrónico, remitente, asunto del mensaje

La información sobre el funcionamiento del proceso de autoejecución

El proceso de autoejecución registra sus resultados. Los datos se registran en archivos de texto llamados "kl-autorun-**<date><time>.log**". Para ver los datos, abra la ventana **Ejecutar** (comando **Ejecutar** en Windows XP) y, en el campo **Abrir**, escriba %TEMP% y haga clic en **Aceptar**.

Todos los archivos de depuración se guardan en esta ruta para configurar los archivos que se descargaron durante el proceso de autoejecución. Los datos se almacenan durante el proceso de autoejecución y se eliminan permanentemente cuando finaliza dicho proceso. Los datos no se envían a ninguna parte.

Limitaciones de Kaspersky Anti-Virus en Microsoft Windows 10 con el modo de protección de dispositivos activado:

La siguiente funcionalidad está parcialmente limitada:

- Búsqueda y desinfección de rootkits (desinfección de archivos pospuesta para después del reinicio del equipo; detección de software malicioso que crea claves de autoejecución en el registro)
- Análisis heurístico (emulación del inicio de aplicaciones sospechosas)

Acerca del registro de eventos en el registro del evento de Windows relacionados con el Contrato de licencia y Kaspersky Security Network

Los eventos que implican aceptar y rechazar las condiciones del Contrato de licencia, y también aceptar y rechazar la participación en Kaspersky Security Network, se registran en el registro del evento de Windows.

Comprobaciones de las limitaciones de la reputación de las direcciones locales en Kaspersky Security Network

Los vínculos a recursos locales no se analizan en Kaspersky Security Network.

Glosario

A

Activación de la aplicación

Cambio de la aplicación al modo completamente funcional. El usuario lleva a cabo la activación de la aplicación durante la instalación de la aplicación o después de esta. Para activar la aplicación, el usuario debe tener un código de activación.

Actualización

El procedimiento de sustituir/agregar archivos nuevos (bases de datos o módulos de la aplicación) recuperados de los servidores de actualización de Kaspersky Lab.

Actualización disponible

Un conjunto de actualizaciones para los módulos de las aplicaciones de Kaspersky Lab, incluidas las actualizaciones críticas acumuladas durante un determinado período de tiempo y los cambios en la arquitectura de la aplicación.

Análisis del tráfico

Análisis en tiempo real que utiliza información de la versión actual (más reciente) de las bases de datos de objetos transmitidos a través de todos los protocolos (por ejemplo, HTTP, FTP y otros protocolos).

Analizador heurístico

Tecnología de detección de amenazas cuya información no se ha añadido todavía a las bases de datos de Kaspersky Lab. El analizador heurístico detecta los objetos cuyas actividades en el sistema pueden suponer una amenaza para la seguridad. Los objetos que detecta el analizador heurístico se consideran posiblemente infectados. Por ejemplo, un objeto puede considerarse posiblemente infectado si contiene secuencias de comando típicas de los objetos maliciosos (abrir archivo o escribir en archivo).

Aplicación incompatible

Una aplicación de antivirus de otro desarrollador o una aplicación de Kaspersky Lab que no admite la administración a través de Kaspersky Anti-Virus.

Archivo comprimido

Un archivo comprimido que contiene un programa de descompresión e instrucciones para que lo ejecute el sistema operativo.

Archivo infectable

Un archivo que, debido a su estructura o formato, los delincuentes pueden utilizar como "recipiente" para almacenar y para difundir código malintencionado. En general, son archivos ejecutables (por ejemplo, archivos con las extensiones COM, EXE, DLL, etc.). El riesgo de activación de código malicioso en estos archivos es bastante alto.

B

Base de datos de direcciones web fraudulentas

Lista de direcciones web, definidas como fraudulentas por los especialistas de Kaspersky Lab. Las bases de datos se actualizan con regularidad y forman parte de la aplicación de Kaspersky Lab.

Base de datos de direcciones web maliciosas

Una lista de direcciones web cuyo contenido puede considerarse como peligroso. Creada por los especialistas de Kaspersky Lab, la lista se actualiza periódicamente y se incluye en el paquete de la aplicación de Kaspersky Lab.

Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas de seguridad del equipo conocidas por Kaspersky Lab en el momento de la publicación de las bases de datos antivirus. Las entradas de las bases de datos antivirus permiten la detección de código malicioso en los objetos analizados. Los autores de estas bases de datos antivirus son especialistas de Kaspersky Lab, que las actualizan cada hora.

Bloqueo de objetos

Denegación del acceso a un objeto de aplicaciones de terceros. Los objetos bloqueados no se pueden leer, ejecutar, modificar ni eliminar.

Brote de virus

Una serie de intentos deliberados de infectar un equipo con un virus.

C

Clasificación del usuario

El índice de la actividad del usuario que utiliza Kaspersky Anti-Virus. La clasificación del usuario aparece en el perfil del programa Proteger a un amigo y depende de la configuración y de la versión de la aplicación.

Código de activación

Un código que recibe al comprar una licencia de Kaspersky Anti-Virus. Este código es necesario para activar la aplicación.

El código de activación es una secuencia exclusiva de veinte caracteres alfanuméricos con el formato xxxxx-xxxxx-xxxxx-xxxxx.

Código de activación de bonificación

Un código de activación de Kaspersky Anti-Virus proporcionado al usuario a cambio de puntos de bonificación.

Componentes de protección

Partes integrantes de Kaspersky Anti-Virus (por ejemplo, Anti-Phishing) pensadas para ofrecer protección contra tipos de amenazas específicos. Todos los componentes son, hasta cierto punto, independientes entre sí, por lo que pueden desactivarse o configurarse de forma individual.

Configuración de tareas

Parámetros de la aplicación específicos de un tipo de tarea.

Correo basura

Envíos masivos de correo no solicitado, que la mayoría de las veces incluye publicidad.

Cuarentena

Almacenamiento dedicado en el que la aplicación coloca copias de seguridad de archivos modificados o eliminados durante el proceso de desinfección. Las copias de los archivos se almacenan en un formato especial que no es peligroso para el equipo.

pase

D

Depuración

Ejecución de la aplicación en modo de depuración; después de ejecutar cada comando, la aplicación se detiene y se muestra el resultado de este paso.

F

Falso positivo

Una situación en la que una aplicación de Kaspersky Lab considera un objeto no infectado como infectado porque el código del objeto es similar al de un virus.

Firma digital

Bloque cifrado de datos incrustados en un documento o una aplicación. Una firma digital se utiliza para identificar al autor del documento o de la aplicación. Para crear una firma digital, el autor del documento o de la aplicación debe tener un certificado digital que proporcione la identidad del autor.

Una firma digital le permite verificar el origen y la integridad de los datos, además de permitirle protegerse de falsificaciones.

G

Grupo de confianza

Un grupo en donde Kaspersky Anti-Virus asigna una aplicación o un proceso dependiendo de los criterios siguientes: la presencia de una firma digital, la reputación en Kaspersky Security Network, el nivel de confianza del origen de la aplicación y el peligro potencial de las acciones realizadas por la aplicación o su proceso. En función del grupo de confianza al que pertenezca una aplicación, Kaspersky Anti-Virus puede restringir las acciones que puede llevar a cabo en el sistema operativo.

En Kaspersky Anti-Virus, todas las aplicaciones pertenecen a uno de los grupos siguientes: De confianza, Restricción baja, Restricción alta o No fiable.

K

Kaspersky Security Network (KSN)

Es una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky Lab, que contiene información actualizada sobre la reputación de archivos, recursos web y software. El uso de datos de Kaspersky Security Network garantiza tiempos de respuesta más rápidos de Kaspersky Lab frente a amenazas, mejora el rendimiento de algunos componentes de protección y reduce el número de falsos positivos.

Keylogger

Programa diseñado para registrar de forma oculta información sobre las teclas que pulsa el usuario. Los keyloggers funcionan como interceptores de las pulsaciones del teclado.

M

Máscara de archivo

Representación del nombre de un archivo utilizando caracteres genéricos. Los dos caracteres genéricos estándar utilizados en máscaras de archivo son * y ?; donde * representa un número cualquiera de caracteres, y ? representa un único carácter.

Módulos de aplicación

Archivos incluidos en el paquete de instalación de Kaspersky Lab encargados de realizar las tareas principales de la aplicación correspondiente. A cada tipo de tarea llevada a cabo por la aplicación (protección, análisis, actualizaciones de módulos de la aplicación y de las bases de datos) le corresponde un módulo de la aplicación concreto.

N

Nivel de amenaza

Un índice que muestra la probabilidad de que una aplicación suponga una amenaza para el sistema operativo. El nivel de amenaza se calcula utilizando el análisis heurístico en función de dos tipos de criterios:

- Estáticos (como información sobre el archivo ejecutable de una aplicación: tamaño, fecha de creación, etc.).
- Dinámicos, que se utilizan durante la simulación del funcionamiento de la aplicación en un entorno virtual (análisis de las solicitudes del sistema de la aplicación).

El nivel de amenaza permite detectar comportamientos típicos del software malicioso. Cuanto menor sea el nivel de amenaza, mayor será el número de acciones que podrá realizar la aplicación en el sistema operativo.

Nivel de seguridad

El nivel de seguridad se define como el conjunto predefinido de configuraciones de un componente de aplicación.

O

Objeto infectado

Un objeto que contiene una porción de código que coincide totalmente con parte del código de software malintencionado conocido. Kaspersky Lab no recomienda acceder a tales objetos.

Objeto posiblemente infectado

Un objeto cuyo código contiene porciones de código modificado de una amenaza conocida o un objeto cuyo comportamiento es similar al de una amenaza.

Objetos del inicio

El conjunto de programas necesarios para iniciar y utilizar correctamente el sistema operativo y el software instalado en el equipo. Estos objetos se ejecutan cada vez que se inicia el sistema operativo. Existen virus capaces de infectar estos objetos autoejecutables específicamente, lo que puede provocar, por ejemplo, el bloqueo del inicio del sistema operativo.

P

Paquete de actualización

Paquete de archivos diseñado para actualizar los módulos de aplicaciones y bases de datos. Una aplicación de Kaspersky Lab copia los paquetes de actualización de los servidores de actualización de Kaspersky Lab y, a continuación, los instala y aplica.

Perfil en el programa Proteger a un amigo

Resumen de la participación del usuario en el programa Proteger a un amigo. El perfil contiene el número de puntos de bonificación recopilados, vínculos a la página para descargar Kaspersky Anti-Virus y los códigos de activación de bonificación concedidos al usuario.

Período de validez de la licencia

El período de tiempo durante el cual tiene acceso a las funciones de la aplicación y derecho para utilizar los servicios adicionales.

Phishing

Un tipo de fraude en Internet, en el que se envían mensajes de correo electrónico con el fin de robar datos confidenciales, a menudo datos financieros.

Probablemente correo no deseado

Mensaje que no se puede considerar claramente como correo basura, pero que cuenta con algunas propiedades de spam (por ejemplo, ciertos tipos de cadenas de mensajes y mensajes publicitarios).

Proceso de confianza

Proceso de software cuyas operaciones de archivos no están restringidas por la aplicación de Kaspersky Lab en el modo de protección en tiempo real. Cuando se detecta una actividad sospechosa en un proceso de confianza, Kaspersky Anti-Virus elimina el proceso de la lista de procesos de confianza y bloquea sus acciones.

Protocolo

Conjunto de reglas estandarizadas y perfectamente definidas que regulan la interacción entre un cliente y un servidor. Entre los protocolos más famosos y los servicios asociados a ellos se incluyen HTTP, FTP y NNTP.

Puntos de bonificación

Los puntos de bonificación son los puntos que Kaspersky Lab concede a los usuarios que participen en el programa Proteger a un amigo. Los puntos de bonificación se otorgan al usuario si publica un vínculo a la aplicación de Kaspersky Lab en redes sociales o pega el vínculo en un mensaje de correo electrónico y el amigo del usuario descarga el paquete de instalación de la aplicación a través de este vínculo y activa la aplicación.

R

Rootkit

Aplicación o conjunto de aplicaciones desarrollados para la ocultación de los rastros de un intruso o software malicioso en el sistema operativo.

En sistemas basados en Windows, normalmente los rootkits hacen referencia a programas que penetran en el sistema e interceptan funciones del sistema (API de Windows). Los principales métodos que logran que la presencia de estos programas en el sistema operativo sea tan imperceptible son la interceptación y la modificación de las funciones de API de bajo nivel. Un rootkit también puede enmascarar la presencia de cualquier proceso, carpeta y archivo que se haya almacenado en una unidad de disco duro, además de las claves de registro; en caso de que se describan en la configuración del rootkit. Muchos rootkits instalan sus propios controladores y servicios en el sistema operativo (también son "invisibles").

S

Script

Pequeño programa informático, o una parte de programa independiente (función), que, de forma general, se ha desarrollado para realizar una tarea específica. Se suele utilizar con programas incrustados en hipertexto. Los scripts se ejecutan, por ejemplo, al abrir determinados sitios web.

Si está activada la protección en tiempo real, la aplicación rastrea la ejecución de scripts, los intercepta y los analiza en busca de virus. En función de los resultados del análisis, puede prohibir o autorizar la ejecución de un script.

Sector de arranque del disco

Un sector de arranque es un área concreta del disco duro de un equipo, disquete o cualquier otro dispositivo de almacenamiento de datos. El sector contiene información sobre el sistema de archivos del disco y un programa de carga de arranque, que es responsable de iniciar el sistema operativo.

Existen varios virus que infectan sectores de arranque y que, por tanto, se conocen como virus de arranque. La aplicación de Kaspersky Lab permite analizar sectores de arranque en busca de virus y desinfectarlos en caso de que se encuentre alguna infección.

Servidores de actualización de Kaspersky Lab

Servidores HTTP de Kaspersky Lab desde los que se descargan las actualizaciones de los módulos de software y de bases de datos.

T

Tarea

Las funciones de la aplicación de Kaspersky Lab se implementan en forma de tareas como, por ejemplo: tarea de análisis completo o tarea de actualización.

Tecnología iChecker

Tecnología que permite aumentar la velocidad de análisis del antivirus al excluir objetos no modificados desde el análisis anterior, siempre que los parámetros de análisis (las bases de datos y la configuración) no hayan cambiado. La información de cada archivo se conserva en una base especial. Esta tecnología se utiliza tanto en los modos de protección en tiempo real como en el análisis bajo demanda.

Por ejemplo, tiene un archivo que analizó una aplicación de Kaspersky Lab y al que se le asignó el estado *no infectado*. La próxima vez, la aplicación omitirá el archivo a menos que se haya modificado o se haya cambiado la configuración del análisis. Si se modificó el contenido de un archivo agregando un objeto nuevo, se cambiaron los parámetros de análisis o se actualizaron las bases de datos de la aplicación, el archivo se volverá a analizar.

Limitaciones de la tecnología iChecker:

- Esta tecnología no funciona con archivos de gran tamaño, ya que es más rápido analizar un archivo que comprobar si se ha modificado desde el análisis anterior.
- Esta tecnología es compatible con un número limitado de formatos.

V

Virus

Programa que infecta a otros agregándoles su código con el fin de hacerse con el control cuando se ejecutan archivos infectados. Esta simple definición permite identificar la acción principal que realiza cualquier virus (infección).

Virus desconocido

Un nuevo virus sobre el que no hay información en las bases de datos. Generalmente, la aplicación detecta los virus desconocidos en objetos mediante el analizador heurístico. Estos objetos se clasifican como posiblemente infectados.

Vulnerabilidad

Fallo en un sistema operativo o una aplicación que puede aprovechar cualquier creador de software malicioso para penetrar en el sistema operativo o la aplicación y dañar su integridad. La presencia de un número elevado de vulnerabilidades en un sistema operativo lo convierte en un sistema no fiable. Esto se debe a que los virus que penetran el sistema pueden provocar interrupciones en el propio sistema operativo y en las aplicaciones instaladas.

AO Kaspersky Lab

Kaspersky Lab es un proveedor de renombre mundial que ofrece sistemas de protección de equipos contra varias amenazas, como virus y otro software malicioso, correo electrónico no solicitado (correo no deseado) y ataques de red y de piratas informáticos.

En 2008, Kaspersky Lab se clasificó entre los mejores cuatro vendedores de soluciones de software para la seguridad de la información de usuarios finales (estudio IDC Worldwide Endpoint Security Revenue de Vendor). Kaspersky Lab es el proveedor de sistemas de protección de equipos de usuarios particulares favorito en Rusia ("IDC Endpoint Tracker 2014").

Kaspersky Lab se creó en Rusia en 1997. Se ha convertido desde entonces en un grupo internacional de empresas con 34 oficinas en 31 países. La empresa cuenta con más de 3.000 profesionales cualificados.

PRODUCTOS. Los productos de Kaspersky Lab proporcionan protección para todos los sistemas, desde equipos domésticos a grandes redes corporativas.

La gama de productos personales incluye aplicaciones de seguridad para equipos de escritorio, portátiles, tabletas, teléfonos inteligentes y otros dispositivos móviles.

La empresa ofrece soluciones de protección y control y tecnologías para estaciones de trabajo y dispositivos móviles, máquinas virtuales, servidores de archivos y web, puertas de enlace de correo y firewalls. La cartera de la empresa también presenta productos especializados que ofrecen protección contra ataques de denegación de servicio (DDoS), protección para sistemas de control industriales y prevención del fraude financiero. En combinación con el sistema de administración centralizada de Kaspersky Lab, estas soluciones garantizan una protección automatizada eficaz para empresas y organizaciones frente a amenazas informáticas de cualquier envergadura. Los productos de Kaspersky Lab están certificados por importantes laboratorios de prueba, son compatibles con software de diversos proveedores y están optimizados para funcionar en muchas plataformas de hardware.

Los analistas antivirus de Kaspersky Lab no cesan de trabajar. Cada día descubren cientos de miles de nuevas amenazas informáticas, crean herramientas para detectarlas y desinfectarlas, e incluyen las firmas de dichas amenazas en las bases de datos utilizadas por las aplicaciones de Kaspersky Lab.

TECNOLOGÍAS. Numerosas tecnologías que hoy forman parte de las herramientas antivirus más modernas fueron desarrolladas originalmente por Kaspersky Lab. No es casualidad que muchos otros programadores utilicen el núcleo de Kaspersky Anti-Virus en sus productos, como los siguientes: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Muchas de las tecnologías más innovadoras de la empresa están patentadas.

LOGROS. A lo largo de los años, Kaspersky Lab ha obtenido cientos de galardones por sus servicios frente a las amenazas informáticas. Tras las pruebas y el estudio realizado por el reputado laboratorio de pruebas austriaco AV-Comparatives en 2014, Kaspersky Lab se clasificó entre los dos primeros proveedores en número de certificados Advanced+ obtenidos y consiguió el certificado de primer clasificado. Sin embargo, el mayor logro de Kaspersky Lab es la lealtad de sus usuarios en todo el mundo. Los productos de la empresa y sus tecnologías protegen a más de 400 millones de usuarios, y el número de clientes corporativos supera los 270 000.

Sitio web de Kaspersky Lab:

<http://www.kaspersky.es>

Enciclopedia del virus:

<http://securelist.com>

Virus Lab:

<http://newvirus.kaspersky.com/es> (para analizar archivos y sitios web sospechosos)

Foro web de Kaspersky Lab:

<http://forum.kaspersky.com/index.php?showforum=45>

Información sobre el código de terceros

La información sobre el código de terceros se incluye en el archivo legal_notices.txt, en la carpeta de instalación de la aplicación.

Información de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos propietarios.

Google Chrome y Chrome son marcas comerciales de Google, Inc.

Intel, Celeron y Atom son marcas comerciales de Intel Corporation en EE. UU. u otros países.

Internet Explorer, Microsoft, Windows y Windows Vista son marcas registradas de Microsoft Corporation en Estados Unidos y otros países.

Mozilla y Firefox son marcas comerciales de Mozilla Foundation.

Índice

A

Activación de la aplicación	51
código de activación	47
licencia	44
versión de evaluación	27
Actualización.....	59
Administración remota de la aplicación	79
Amenazas de seguridad	58
Análisis de seguridad	58
Análisis de vulnerabilidades	65
AO Kaspersky Lab	120

B

Bases de datos de la aplicación.....	59
--------------------------------------	----

C

Código	
código de activación	47
Contrato de licencia de usuario final	43
Cuarentena	
restauración de un objeto	66
Cuenta My Kaspersky	98

D

Depuración

transferencia de los resultados de depuración..... 101

Diagnóstico58

E

Eliminar la aplicación39

Estadísticas87

Estado de la protección.....58

H

Herramientas adicionales

Solución de problemas de Microsoft Windows.....53

I

Informes.....87

Instalación de la aplicación22

K

Kaspersky Security Network90

Keyloggers

Teclado virtual.....70

L

Licencia

código de activación.....47

Limpieza de rastros privados76

M

Modo de funcionamiento de la aplicación en pantalla completa	82
--	----

N

Notificaciones	57
----------------------	----

O

Objeto desinfectado	66
---------------------------	----

Origen de actualizaciones	59
---------------------------------	----

P

Perfil para juegos	82
--------------------------	----

Problemas de seguridad	58
------------------------------	----

Protección web	73
----------------------	----

Proteger a un amigo	93
---------------------------	----

clasificación	93
---------------------	----

cuenta	94
--------------	----

R

Recuperación de objetos	66
-------------------------------	----

Requisitos de hardware y software	20
---	----

Requisitos de software	20
------------------------------	----

Restablecimiento de los parámetros predeterminados	86
--	----

Restricción del acceso a la aplicación	83
--	----

S

Solución de problemas de Microsoft Windows	54
--	----

Supervisor de direcciones URL	
Antivirus Internet	73

T

Teclado en pantalla.....	70
Teclado virtual	70

V

Vulnerabilidad	65
----------------------	----