

GUÍA DEL USUARIO

**KASPERSKY
INTERNET
SECURITY 2009
SPECIAL EDITION
FOR ULTRA-
PORTABLES**

¡Bienvenido a Kaspersky Internet Security 2009!

Gracias por haber elegido nuestro producto. Esperamos que esta documentación le ayude en su trabajo y responda a sus preguntas sobre el producto.

Advertencia. Este documento es propiedad de Kaspersky Lab: todos los derechos están reservados de acuerdo con las leyes de propiedad intelectual de la Federación Rusa y con los tratados internacionales. La reproducción o distribución ilícita de este documento, en parte o en totalidad, puede ser perseguida ante los tribunales civiles, administrativos o penales, en conformidad con las leyes de la Federación Rusa. Cualquier reproducción o distribución de estos materiales, inclusive su traducción, requiere autorización escrita de Kaspersky Lab. Este documento y las ilustraciones asociadas sólo pueden ser utilizados con fines de información no comercial o personal.

Este documento está sujeto a cambios sin previo aviso. Para la última versión de este documento, visite el sitio Web de Kaspersky Lab en la dirección <http://www.kaspersky.com/docs>. Kaspersky Lab no asume ninguna responsabilidad por el contenido, la calidad, la relevancia o la exactitud de los materiales utilizados en este documento cuyos derechos son propiedad de terceras partes, ni por los daños potenciales asociados al uso de estos documentos.

Este documento menciona marcas comerciales registradas o no. Todas las marcas comerciales pertenecen a sus propietarios respectivos.

© Kaspersky Lab, 1997-2009

+7 (495) 645-7939,
Tfno, fax: +7 (495) 797-8700,
+7 (495) 956-7000

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

Fecha de revisión: 08.04.2009

ÍNDICE

INSTALACIÓN DE KASPERSKY INTERNET SECURITY	6
Información acerca de la aplicación.....	6
Fuentes de información para búsquedas personalizadas	7
Contacto con el Departamento de Ventas.....	7
Contacto con el servicio de Soporte técnico	7
Foro Web sobre aplicaciones Kaspersky Lab	9
Presentación de la protección de la aplicación	9
Asistentes y herramientas	10
Características de soporte	11
Análisis heurístico	12
requisitos hardware y software del sistema	13
AMENAZAS A LA SEGURIDAD DEL EQUIPO	15
Amenazas software	15
Software malintencionado (malware)	16
Virus y gusanos	16
Troyanos.....	20
Herramientas malintencionadas	26
Programas potencialmente indeseados	30
Software publicitario (adware)	31
Software pornográfico (pornware)	31
Otros programas de riesgo	32
Métodos de detección de objetos infectados, sospechosos y potencialmente peligrosos por la aplicación.....	36
Amenazas Internet.....	37
Correo no solicitado (Spam).....	37
Fraudes por Internet (Phishing).....	38
Ataques de piratas	38
Banners.....	39
INSTALACIÓN DE LA APLICACIÓN.....	40
Paso 1. Descarga de versiones recientes de la aplicación	41
Paso 2. Comprobación de los requisitos de instalación en el sistema	42

Paso 3. Ventana de bienvenida del Asistente	42
Paso 4. Lectura del Contrato de licencia	43
Paso 5. Selección del tipo de instalación	43
Paso 6. Selección de la carpeta de instalación	44
Paso 7. Selección de los componentes de aplicación para instalar	44
Paso 8. Búsqueda de otro software antivirus	45
Paso 9. Preparación final de la instalación	46
Paso 10. Fin de la instalación	46
INTERFAZ DEL PROGRAMA	47
Icono del área de notificaciones.....	47
Menú contextual.....	48
Ventana principal de la aplicación.....	50
Notificaciones.....	53
Ventana de configuración de la aplicación.....	53
PRIMEROS PASOS	54
Selección del tipo de red.....	55
Actualización de la aplicación	56
Análisis de seguridad.....	56
Análisis antivirus del equipo.....	57
Administración de la licencia.....	58
Suscripción para la renovación automática de la licencia	59
Participación en el programa Kaspersky Security Network.....	61
Administración de la seguridad	62
Suspensión de la protección	64
VALIDACIÓN DE LOS PARÁMETROS DE LA APLICACIÓN.....	66
Prueba con el "virus" EICAR y sus modificaciones.....	66
Prueba de protección en el tráfico HTTP	70
Prueba de protección en el tráfico SMTP	70
Validación de los parámetros del componente Antivirus de archivos y memoria.....	71
Validación de los parámetros de la tarea de análisis antivirus.....	72
Validación de los parámetros del componente Anti-Spam.....	72

DECLARACIÓN DE RECOLECCIÓN DE DATOS DE KASPERSKY SECURITY NETWORK	74
KASPERSKY LAB	80
CRYPTOEX LLC	83
MOZILLA FOUNDATION	84
CONTRATO DE LICENCIA	85

INSTALACIÓN DE KASPERSKY INTERNET SECURITY

Es posible instalar Kaspersky Internet Security en uno de los dos modos siguientes:

- en modo interactivo, con el Asistente de instalación de la aplicación, que requiere la intervención del usuario durante el proceso;
- en modo no-interactivo, donde la instalación se realiza desde la línea de comandos, sin ninguna intervención del usuario.

Antes de instalar Kaspersky Internet Security, se recomienda cerrar todas las aplicaciones activas.

EN ESTA SECCIÓN:

Información acerca de la aplicación	6
Presentación de la protección de la aplicación.....	9
requisitos hardware y software del sistema.....	13

INFORMACIÓN ACERCA DE LA APLICACIÓN

Si tiene cualquier pregunta relativa a la compra, instalación o uso de la aplicación, puede obtener fácilmente respuestas.

Kaspersky Lab ofrece muchas fuentes de información entre las que puede elegir la que más le convenga, en función de la urgencia o importancia de su pregunta.

FUENTES DE INFORMACIÓN PARA BÚSQUEDAS PERSONALIZADAS

Puede utilizar el sistema de [Ayuda](#).

El sistema de Ayuda contiene información acerca de cómo administrar la protección del equipo: mostrar el estado de protección, analizar varias zonas del equipo y ejecutar otras tareas.

Para abrir la Ayuda, haga clic en el vínculo **Ayuda** de la ventana principal de la aplicación o haga clic en <F1>.

CONTACTO CON EL DEPARTAMENTO DE VENTAS

Si tiene alguna pregunta acerca de la elección o compra de la aplicación, de la ampliación del periodo de utilización, puede llamar por teléfono a nuestros especialistas del Departamento de ventas en nuestra sede central de Moscú:

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00.

El servicio se ofrece en los idiomas ruso e inglés.

Puede enviar sus preguntas al Departamento de venta en la dirección de correo electrónico sales@kaspersky.com.

CONTACTO CON EL SERVICIO DE SOPORTE TÉCNICO

Si ya ha adquirido la aplicación, puede obtener información acerca de la misma en el Servicio de soporte técnico de Kaspersky Lab por teléfono o por Internet.

Los especialistas del Servicio de Soporte técnico responderán a sus preguntas acerca de la instalación y uso de la aplicación y, si su equipo está infectado, le ayudarán a eliminar las consecuencias de las acciones del software malintencionado.

Antes de entrar en contacto con el Servicio de Soporte técnico, lea primero las reglas de consulta (<http://support.kaspersky.com/support/rules>).

Consultas por correo al Servicio de soporte técnico (sólo para usuarios registrados)

Puede consultar a los especialistas del Servicio de Soporte técnico completando el formulario Web del servicio de ayuda (Helpdesk) en la dirección (<http://support.kaspersky.com/helpdesk.html>).

Puede redactar su pregunta en cualquier de los idiomas alemán, español, francés, inglés o ruso.

Para enviar un mensaje de correo con su pregunta, debe comunicar el **número de cliente** recibido durante el registro en el sitio Web del Servicio de Soporte técnico junto con su **contraseña**.

Nota

Si todavía no es usuario registrado de aplicaciones Kaspersky Lab, puede completar un formulario de registro en (<https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/>). Durante el registro, deberá comunicar el código de activación o el nombre del archivo llave.

Recibirá la respuesta de un especialista del Servicio de Soporte técnico en su **Espacio personal** en la dirección <https://support.kaspersky.com/en/PersonalCabinet>, así como en la dirección de correo electrónico especificada en su consulta.

Describa en el formulario Web el problema encontrado con el máximo detalle posible. Especifique la información siguiente en los campos obligatorios:

- **Tipo de pregunta.** Las preguntas más frecuentes de los usuarios son agrupadas por temas genéricos, por ejemplo "Problema de instalación/desinstalación de productos" o "Problema con el Análisis antivirus/respaldo". Si no existe un tema apropiado para su pregunta, elija la entrada "Pregunta general".
- **Nombre y número de versión de la aplicación.**
- **Texto de la pregunta.** Describa el problema encontrado con el máximo detalle posible.

- **Número y contraseña de cliente.** Escriba el número y contraseña de cliente recibidos durante el registro en el sitio Web del Servicio de Soporte técnico.
- **Dir. de correo.** El servicio de Soporte técnico enviará la respuesta a esta dirección de correo electrónico.

Soporte técnico por teléfono

Si su problema requiere ayuda urgente, puede llamar al servicio de Soporte técnico de su ciudad. Deberá suministrar datos de identificación (<http://support.kaspersky.com/support/details>) cuando consulte el Soporte técnico ruso (http://support.kaspersky.com/support/support_local) o internacional (<http://support.kaspersky.com/support/international>). Esto facilitará a nuestros especialistas procesar su consulta lo antes posible.

FORO WEB SOBRE APLICACIONES KASPERSKY LAB

Si su consulta no requiere una respuesta urgente, puede exponerla ante los especialistas de Kaspersky Lab y otros usuarios en nuestro foro en la dirección <http://forum.kaspersky.com/>.

Este foro permite consultar temas existentes, dejar comentarios, crear temas nuevos y utilizar el motor de búsqueda.

PRESENTACIÓN DE LA PROTECCIÓN DE LA APLICACIÓN

Kaspersky Internet Security protege su equipo contra amenazas conocidas y desconocidas y otros datos indeseados. El procesamiento de cada tipo de amenaza corre a cargo de un componente individual de la aplicación. Esta organización flexible permite configurar con facilidad cualquiera de los componentes y ajustarlos a las necesidades específicas de un usuario en particular, o de toda una organización.

Kaspersky Internet Security incluye las siguientes características de protección:

- Vigilancia de las actividades de las aplicaciones de usuario, para evitar la ejecución de acciones peligrosas.
- Componentes de protección que ofrecen protección en tiempo real de las transferencias y de las rutas de entrada de todos los datos en su equipo.
- Componentes de protección que aseguran la protección de su equipo contra cualquier ataque o intrusión por red conocido en ese momento.
- Componentes de filtrado de datos indeseados que ahorran tiempo, tráfico Web y dinero.
- Tareas de análisis antivirus utilizadas para buscar virus en archivos, carpetas, unidades o zonas individuales, o para realizar un análisis completo del equipo. También es posible configurar las tareas de análisis para detectar vulnerabilidades en aplicaciones instaladas.
- Componente de actualización, que asegura el estado óptimo de los módulos internos de la aplicación modules y de las bases utilizadas para buscar programas malintencionados, detectar ataques de piratas y mensajes indeseados.
- Asistentes y herramientas que facilitan la ejecución de tareas durante el funcionamiento de Kaspersky Internet Security.
- Características de soporte que ofrecen asistencia para trabajar con la aplicación y ampliar sus posibilidades.

ASISTENTES Y HERRAMIENTAS

Asegurar la seguridad de su equipo es una tarea difícil que requiere conocimientos sobre las características del sistema operativo y los métodos empleados para aprovechar sus puntos débiles. Además, resulta difícil analizar y asimilar la cantidad y diversidad de la información existente sobre seguridad de sistemas.

Para facilitar la solución de tareas de seguridad específicas para el equipo, el paquete Kaspersky Internet Security incluye un conjunto de Asistentes y herramientas:

- El Asistente para el análisis de la seguridad realiza diagnósticos de seguridad del equipo y busca vulnerabilidades en el sistema operativo y programas instalados en el equipo.
- Asistente de configuración del navegador: analiza los parámetros de Microsoft Internet Explorer, en primer lugar, desde una perspectiva de seguridad.
- Asistente de restauración del sistema: elimina el rastro de las acciones de objetos malintencionados dentro del sistema.
- Asistente para la limpieza de los rastros de actividad: busca rastros de acciones del usuario dentro del sistema y en parámetros del sistema operativo, que puedan servir para recuperar información confidencial sobre la actividad del usuario.
- Análisis de paquetes de red: intercepta y muestra los detalles de los paquetes de red.
- Monitor de red: muestra información acerca de la actividad de red de su equipo.
- Teclado virtual: evita la captura de los datos introducidos por teclado.

CARACTERÍSTICAS DE SOPORTE

La aplicación incluye características de soporte diseñadas para mantener la protección del equipo actualizada, mejorar las prestaciones y ayudarle a utilizar la aplicación.

Kaspersky Security Network

Kaspersky Security Network es un sistema de transferencia automática de informes sobre amenazas detectadas y potenciales, a una base de datos centralizada. Con esta base de datos, Kaspersky Lab puede responder más rápidamente a las amenazas más difundidas y alertar a los usuarios cuando se producen epidemias víricas.

Licencia

Cuando adquiere Kaspersky Internet Security, acepta un contrato de licencia con Kaspersky Lab que regula la utilización de la aplicación así como su acceso a actualizaciones de las bases de datos y al Soporte técnico por un tiempo especificado. Los términos de uso y otros datos

necesarios para que la aplicación sea completamente funcional son suministrados por un archivo llave.

La entrada **Licencia** le permite consultar información detallada sobre su licencia así como adquirir o renovar la existente.

Soporte

Todos los usuarios registrados de Kaspersky Internet Security pueden beneficiarse de nuestro servicio de soporte técnico. Para ver la información acerca de cómo obtener soporte técnico, utilice la función **Soporte**.

Los vínculos le dan acceso al foro de usuarios de Kaspersky Lab, le permiten enviar sugerencias al Soporte técnico o aportar comentarios sobre la aplicación mediante un formulario en línea especial.

También puede tener acceso al servicio de Soporte técnico en línea y a los servicios de su Espacio personal. Por supuesto, nuestro personal está siempre dispuesto a ayudarle por teléfono con la aplicación.

ANÁLISIS HEURÍSTICO

Algunos componentes de protección en tiempo real utilizan métodos heurísticos, como el Antivirus de archivos y memoria, el Antivirus de correo y chat, el Antivirus Internet y el análisis antivirus.

El análisis de objetos mediante el método de comparación de firmas, utilizando una base de datos con las descripciones de todas las amenazas conocidas, permite obtener una respuesta definitiva acerca de un objeto, si éste es malintencionado y su grado de peligrosidad. El método heurístico, a diferencia del método de comparación de firmas, intenta detectar comportamientos típicos de los objetos en lugar de analizar su contenido estático, pero no ofrece el mismo grado de aciertos.

La ventaja del análisis heurístico es que detecta software malintencionado que no está registrado en la base, por lo que no es necesario actualizar la base de datos antes del análisis. Por estas razones, consigue detectar nuevas amenazas antes de que los analistas antivirus las descubran.

Sin embargo, existen métodos que permiten engañar los métodos heurísticos. Por ejemplo, una de estas medidas defensivas del código malintencionado consiste en congelar su actividad cuando detecta que un análisis heurístico está en curso.

Nota

El uso combinado de varios métodos de análisis ofrece una mayor seguridad.

Al analizar un objeto, el analizador heurístico simula la ejecución del objeto dentro de un entorno virtual seguro administrado por la aplicación. Si descubre una actividad sospechosa durante la ejecución del objeto, la aplicación lo considera como dañino y no le permite ejecutarse en el equipo huésped, o presenta un mensaje al usuario solicitando instrucciones adicionales:

- Mover a cuarentena la nueva amenaza para ser analizada y procesada más tarde con bases actualizadas.
- Eliminar el objeto.
- Ignorar (si está seguro de que el objeto no puede ser dañino).

Para utilizar los métodos heurísticos, active la casilla **Utilizar el analizador heurístico** y desplace el cursor del nivel de detalle a una de las posiciones siguientes: Superficial, Medio o Avanzado. El nivel de detalle busca un equilibrio entre la minuciosidad y, por tanto, calidad del análisis contra nuevas amenazas, y el consumo de recursos del sistema, así como la duración del análisis. A mayor nivel heurístico, mayor cantidad de recursos del sistema se consume y mayor es el tiempo requerido.

Advertencia.

Las amenazas nuevas detectadas de forma heurística son rápidamente analizadas por Kaspersky Lab y los métodos para su desinfección se agregan en pocas horas a las actualizaciones de las bases.

Si actualiza regularmente sus bases de datos, podrá mantener el nivel óptimo de protección para su equipo.

REQUISITOS HARDWARE Y SOFTWARE DEL SISTEMA

Para operar normalmente, el equipo debe cumplir los requisitos siguientes:

Requisitos generales:

- 75 Mb de espacio libre en disco.
- Ratón (mouse).

- Microsoft Internet Explorer 5.5 o superior (para actualizar las bases y módulos de la aplicación por Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (SP2 o superior), Microsoft Windows XP Professional (SP2 o superior):

- Procesador Intel Atom, Intel Celeron-M o VIA C7-M.
- 256 Mb de memoria RAM libre.

AMENAZAS A LA SEGURIDAD DEL EQUIPO

Las aplicaciones malintencionadas suponen una amenaza considerable a la seguridad del equipo. Además, otras amenazas provienen del correo no deseado (spam), mensajes fraudulentos (phishing), efracciones de piratas así como software publicitario (adware) o pornográfico (pornware). Estas amenazas están asociadas al uso de Internet.

EN ESTA SECCIÓN:

Amenazas software	15
Amenazas Internet	37

AMENAZAS SOFTWARE

Kaspersky Internet Security puede detectar centenares de miles de programas malintencionados residentes en su equipo. Algunos de estos programas suponen una amenaza mayor para su equipo, mientras otros sólo son peligrosos bajo determinadas condiciones. Después de detectar una aplicación malintencionada, la clasifica y le atribuye un nivel de peligrosidad (alta o media).

Los analistas de Kaspersky Lab distinguen dos categorías principales de amenazas software: *programas malintencionados* y *programas potencialmente indeseados*.

Los programas malintencionados (Malware) (página 16) son diseñados para producir daños en el equipos y a su usuario: por ejemplo, robos, bloqueos, alteraciones o eliminaciones de datos, interrupciones en el funcionamiento de los equipos o de la red.

Los programas potencialmente indeseados (PUP) (página 30), a diferencia de los programas malintencionados, no están pensados sólo para producir daños, pero pueden ayudar a romper el sistema de seguridad del equipo.

La Enciclopedia del virus (<http://www.viruslist.com/en/viruses/encyclopedia>) contiene una descripción detallada de estos programas.

SOFTWARE MALINTENCIONADO (MALWARE)

Los programas malintencionados ("malware") son diseñados especialmente para producir daños en los equipos y a sus usuarios: robos, bloqueos, alteraciones o eliminaciones de datos, interrupciones en el funcionamiento de los equipos o de la red de equipos.

Los programas malintencionados se dividen en tres subcategorías: *virus y gusanos*, *caballos de Troya (troyanos)* y *herramientas malintencionadas*.

Los virus y gusanos (Viruses_and_Worms) (página 16) son capaces de crear copias de sí mismos y éstas, a su vez, también son capaces de reproducirse. Algunos de ellos se ejecutan sin conocimiento ni intervención del usuario, mientras otros requieren la actuación del usuario para poder ejecutarse. Estos programas realizan acciones malintencionadas cuando se ejecutan.

Los caballos de Troya (Trojan_programs) (página 20) no se autorepican, a diferencia de los gusanos y los virus. Se infiltran en el equipo, por ejemplo, a través del correo electrónico o de un navegador, cuando el usuario consulta un sitio Web "infectado". Para ejecutarse, requieren la acción del usuario antes de poder realizar sus acciones malintencionadas.

Las herramientas malintencionadas (Malicious_tools) (página 26) son herramientas creadas especialmente para producir daños. Sin embargo, a diferencia de otros programas malintencionados, no ejecutan acciones inmediatamente malintencionadas y pueden ser conservados y ejecutados sin riesgo en el equipo del usuario. Contienen funciones que permiten a los infractores crear virus, gusanos y troyanos, organizar ataques de red contra servidores remotos, piratear equipos o realizar otras acciones malintencionadas.

VIRUS Y GUSANOS

Subcategoría: virus y gusanos (Viruses_and_Worms)

Nivel de riesgo: máximo

Los virus y gusanos tradicionales realizan acciones no autorizadas en el equipo infectado, pueden autoreplicarse y propagarse por sí mismos.

Virus tradicionales

Después de infiltrar el sistema, un virus tradicional infecta un archivo, se autoactiva, realiza su acción malintencionada y agrega copias de sí mismo dentro de otros archivos.

Los virus tradicionales sólo se reproducen en los recursos locales de un determinado equipo, no pueden penetrar en otros equipos de forma independiente. La distribución hacia otros equipos sólo se produce si el virus agrega una copia de sí mismo a un archivo ubicado en una carpeta compartida o en un CD, o cuando el usuario reenvía un correo con un adjunto infectado.

El código de un virus tradicional suele especializarse en penetrar en varias zonas de su equipo, del sistema operativo o de una aplicación. En función del entorno, se hace una diferencia entre virus de *archivo*, de *arranque*, de *secuencia de comandos (script)* y de *macro*.

Los virus pueden infectar archivos de diferentes modos. *Los virus de sobreescritura* escriben su propio código para reemplazar el contenido del archivo infectado. El archivo infectado deja de funcionar y no es posible repararlo. *Los virus parasitarios* modifican los archivos, pero los dejan parcial o completamente operacionales. *Los virus compañeros* no modifican los archivos, sino que los duplican, de forma que al abrir el ejemplar de archivo infectado por el virus, éste se ejecuta. Existen otros tipos como los *virus vinculados*, los virus que infectan *módulos objeto (OBJ)* o *bibliotecas de compilación (LIB)*, los virus que *infectan el texto original de los programas*.

Gusano

Después de infiltrar el sistema, el código de un gusano de red, de forma similar al código de un virus tradicional, se ejecuta y realiza su acción malintencionada. Los gusanos de red se denominan así por su capacidad para aprovechar túneles de comunicación entre equipos para propagarse a sí mismos a través de varios canales de información.

Los gusanos se clasifican por su método principal de proliferación, descrito en la tabla siguiente:

Tabla 1. Gusanos clasificados por modo de proliferación

TIPO	NOMBRE	DESCRIPCIÓN
IM-Worm	Gusanos de mensajería instantánea	<p>Estos gusanos se propagan a través de clientes de mensajería instantánea (IM) como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ó Skype.</p> <p>Normalmente, estos gusanos utilizan listas de contactos para enviar mensajes con un vínculo hacia una copia del archivo con el gusano, ubicada en un sitio Web. Cuando un usuario descarga y abre el archivo, el gusano se activa.</p>
Email-Worm	Gusanos de correo	<p>Los gusanos de correo infectan los equipos a través del correo electrónico.</p> <p>El mensaje infectado contiene un archivo adjunto con una copia del gusano, o un vínculo a dicho archivo ubicado en un sitio Web. El sitio Web suele estar pirateado o pertenece al propio pirata. Cuando abre el adjunto, el gusano se activa; en otro caso, se activa cuando el usuario hace clic en el vínculo, descarga y abre el archivo con el gusano. Tras esto, el gusano sigue reproduciéndose mensajes con copias de sí mismo a otras direcciones de correo.</p>
IRC-Worm	Gusanos IRC	<p>Los gusanos de este tipo penetran en los equipos a través de sistemas IRC (Internet Relay Chat) que permiten comunicar con otras personas por Internet en tiempo real.</p> <p>Estos gusanos publican en el canal IRC una copia del archivo o un vínculo al archivo del gusano. Cuando un usuario descarga y abre el archivo, el gusano se activa.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Net-Worms	Gusanos de red (que operan en redes de equipos)	<p>Estos gusanos se reproducen a través de redes informáticas.</p> <p>A diferencia de los otros tipos, los gusanos de red se propagan sin la intervención del usuario. Buscan los equipos dentro de la red local a través de programas que presentan vulnerabilidades. Para ello utilizan el procedimiento de difusión un paquete de red especial (un "exploit") que contiene parte o la totalidad de su propio código. Si un equipo dentro de la red es vulnerable, será infiltrado por dicho paquete. Una vez dentro del equipo, el gusano se activa.</p>
P2P-Worm	Gusanos de intercambio de archivos	<p>Los gusanos P2P se propagan mediante las redes P2P, como Kazaa, Grokster, EDonkey, FastTrack o Gnutella.</p> <p>Para utilizar una red de intercambio de archivos, el gusano se duplica dentro de la carpeta de intercambio normalmente ubicada dentro del equipo del usuario. La red de intercambio de archivos difunde la información sobre su presencia y el usuario puede "buscar" el archivo infectado en la red y, como cualquier otro archivo, descargarlo y abrirlo.</p> <p>Otros gusanos más complejos imitan los protocolos de red de una determinada red de intercambio de archivos: responden de forma positiva a respuestas de la red y ofrecen sus propias copias para descarga.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Worm	Otros gusanos	<p>Otros gusanos de red incluyen:</p> <ul style="list-style-type: none">• Gusanos que distribuyen sus copias mediante recursos de red. Aprovechando las características del sistema operativo, atraviesan las carpetas de red compartidas, se conectan a equipos de la red externa global e intentan autorizar permisos de acceso completo a sus discos. A diferencia de otros gusanos de red, el usuario debe abrir un archivo con una copia del gusano para poder activarlo.• Gusanos que utilizan otros métodos de propagación no presentados aquí: por ejemplo, gusanos que se propagan a través de teléfonos móviles.

TROYANOS

Subcategoría: Troyanos (Trojan_programs)

Nivel de riesgo: máximo

A diferencia de los gusanos y los virus, los caballos de Troya (troyanos) no crean copias de sí mismos. Se filtran en el equipo, por ejemplo, a través de un adjunto de correo o de un navegador, cuando el usuario consulta un sitio Web "infectado". Los troyanos deben ser ejecutados por el usuario para poder realizar sus acciones malintencionadas.

Los caballos de Troya son capaces de realizar toda una gama de acciones malintencionadas. Las características principales de los troyanos son el bloqueo, modificación y eliminación de datos, así como la perturbación del funcionamiento de los equipos en redes informáticas. Además, los troyanos pueden recibir y enviar archivos, ejecutarlos, mostrar mensajes, conectarse a páginas Web, descargar e instalar programas y reiniciar el equipo infectado.

Los intrusos utilizan a menudo "conjuntos" que incluyen varios tipos de troyanos complementarios.

La tabla a continuación describe los diferentes tipos y comportamientos de los troyanos.

Tabla 2. Tipos de troyanos clasificados por su comportamiento en el equipo infectado

TIPO	NOMBRE	DESCRIPCIÓN
Trojan-ArcBomb	Archivos bomba	Archivos comprimidos que, cuando se descomprimen, aumentan de tamaño hasta impedir el funcionamiento del equipo. Cuando se intenta descomprimir el propio archivero, el equipo empieza a ralentizarse o se "congela" mientras el espacio disco puede saturarse con datos "vacíos". Los "archivos bomba" son especialmente peligrosos para los servidores de archivos y de correo. En un servidor donde se ejecute un sistema de procesamiento automático de información entrante, un "archivo bomba" puede llegar a detener el servidor.
Backdoor	Troyanos de administración remota (puerta trasera)	Estos programas se consideran los más peligrosos de los troyanos; por sus características, recuerdan programas de administración remota. Estos programas se instalan a sí mismos sin el conocimiento del usuario y facilitan a los intrusos medios de administración remota del equipo.

TIPO	NOMBRE	DESCRIPCIÓN
Trojans	Troyanos	<p>Los troyanos incluyen los siguientes programas malintencionados:</p> <ul style="list-style-type: none">• Trojanos tradicionales; sólo reproducen las características principales de los troyanos: bloqueo, modificación y eliminación de datos, la perturbación del funcionamiento de los equipos en redes informáticas. No disponen de ninguna de las características avanzadas propias de otros tipos de troyanos descritos en esta tabla;• Trojanos "polivalentes"; disponen de funciones adicionales, propias de varios tipos de caballos de Troya.
Trojan-Ransoms	Trojanos chantajistas	<p>Estas versiones "toman como rehén" la información del usuario dentro del equipo, modificando, bloqueando o perturbando el funcionamiento del equipo, de forma que el usuario es incapaz de utilizar los datos. A continuación, el pirata pide un rescate al usuario a cambio de proporcionarle un programa que restablecerá el funcionamiento normal del equipo.</p>
Trojan-Clickers	Trojanos generadores de clics	<p>Estos programas visitan páginas Web desde el equipo del usuario: envían un comando al navegador Web o sustituyen las direcciones Web almacenadas en los archivos del sistema.</p> <p>Gracias a estos programas, los intrusos organizan ataques por red o aumentan el tráfico hacia esos sitios, para mejorar la cantidad de ingresos por apariciones de banners publicitarios.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Trojan-Downloaders	Troyanos cargadores	Estos programas acceden a la página Web del intruso, descargan otros programas malintencionados y los instalan en el equipo del usuario. El nombre del archivo de software malintencionado que descargan, lo guardan en su código o lo obtienen de la página Web consultada.
Trojan-Droppers	Troyanos lanzadera	<p>Estos troyanos guardan en el disco del equipo otros troyanos y a continuación los instalan.</p> <p>Los intrusos pueden utilizar estos troyanos lanzadera de varias formas:</p> <ul style="list-style-type: none">• para instalar programas malintencionados sin el conocimiento de sus usuarios: los troyanos lanzadera no muestran ningún mensaje propio ni mensajes falsos, por ejemplo para informar acerca de un error de archivo o de una versión incorrecta del sistema operativo;• para evitar que otro programa malintencionado pueda ser detectado: no todos los programas antivirus son capaces de detectar un programa malintencionado alojado dentro de un troyano lanzadera.

TIPO	NOMBRE	DESCRIPCIÓN
Trojan-Notifiers	Troyanos informadores	<p>Informan al intruso de que el equipo infectado está conectado; a continuación le transfieren los datos de dicho equipo, en particular: la dirección IP, el número de un puerto abierto o la dirección de correo electrónico. Para comunicarse con el intruso, utilizan el correo electrónico, un servidor FTP o se conectan a la página Web del intruso.</p> <p>Los troyanos informadores se incluyen a menudo en conjuntos de varios troyanos complementarios. Informan al intruso que otros troyanos han sido instalados con éxito en el equipo del usuario.</p>
Trojan-Proxies	Trojans-Proxies	Permiten al intruso acceder de forma anónima a páginas Web bajo la identidad del equipo del usuario y sirven a menudo para enviar correo indeseado.
Trojan-PSWs	Ladrones de contraseñas	<p>Troyanos ladrones de contraseñas (PSW, Password Stealing Ware); roban cuentas de usuarios, por ejemplo, información de registro de software. Buscan información confidencial en los archivos del sistema y el Registro y para transmitirla utilizan el correo electrónico, un servidor FTP o se conectan a la página Web del intruso.</p> <p>Algunos de estos troyanos entran dentro de los tipos especiales descritos en esta tabla, como los tipos Trojan-Bankers, Trojan-IM y Trojan-GameThieves.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Trojan-Spies	Troyanos espía	Estos programas sirven para espiar al usuario: recopilan información sobre las acciones del usuario en el equipo: por ejemplo, interceptan datos introducidos con el teclado, capturan imágenes de la pantalla y generan listas de aplicaciones activas. Después de recuperar esta información, la transmiten al intruso, para ello utilizan el correo electrónico, un servidor FTP o se conectan a la página Web del intruso.
Trojans-DoS	Troyanos para ataques por red	Los programas de ataque DoS (Denial-of-Service) envían numerosas peticiones al servidor remoto desde el equipo del usuario. El servidor moviliza todos sus recursos para procesar las peticiones hasta que deja de funcionar. Estos programas sirven a menudo para infectar múltiples equipos desde los que atacan al servidor.
Trojan-IMs	Ladrones de datos en mensajerías instantáneas	Estos programas roban números y contraseñas de usuarios de clientes de mensajería instantánea (IM), como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ó Skype. Para transferir la información al intruso utilizan el correo electrónico, un servidor FTP o se conectan a la página Web del intruso.
Rootkits	Procesos ocultos	Estos programas ocultan la presencia y actividad de otros programas malintencionados, facilitando por tanto su actividad y propagación dentro del sistema. Ocultan archivos o procesos en la memoria de un equipo infectado, registran claves ejecutadas por los programas malintencionados, ocultan el intercambio de datos entre las aplicaciones instaladas en el equipo del usuario y otros equipos de la red.

TIPO	NOMBRE	DESCRIPCIÓN
Trojan-SMS	Troyanos de mensajes SMS	Estos programas infectan teléfonos móviles desde los que envían mensajes SMS a números de pago que se facturan al usuario.
Trojan-GameThieves	Ladrones de datos en juegos de red.	Estos programas roban los datos de la cuenta a usuarios de juegos en línea; a continuación, transmiten esta información al intruso por correo electrónico, mediante FTP, conectándose a la página Web del intruso o con otros métodos.
Trojans-Bankers	Ladrones de cuentas bancarias	Estos programas roban datos de cuentas bancarias o de cuentas de dinero electrónico; transmiten estos datos al intruso por correo electrónico, mediante FTP, conectándose a la página Web del intruso o con otros métodos.
Trojan-Mailfinders	Buscadores de direcciones electrónicas	Estos programas recuperan direcciones de correo electrónico en el equipo y las transmiten al intruso por correo electrónico, mediante FTP, conectándose a la página Web del intruso o con otros métodos. El intruso utiliza las direcciones recopiladas para enviar correo no deseado.

HERRAMIENTAS MALINTENCIONADAS

Subcategoría: herramientas malintencionadas (Malicious_tools)

Nivel de riesgo: Medio

Son herramientas diseñadas especialmente para producir daños. Sin embargo, a diferencia de otros programas malintencionados, son herramientas utilizadas principalmente para atacar otros equipos y pueden ser conservados y ejecutados sin riesgo en el equipo del usuario. Estos programas contienen funciones para crear virus, gusanos y troyanos, organizar ataques de red contra servidores remotos, piratear equipos o realizar otras acciones malintencionadas.

Existen varios tipos de herramientas para software malintencionado, con diferentes funciones, descritas en la tabla siguiente.

Tabla 3. Herramientas malintencionadas agrupadas por función

TIPO	NOMBRE	DESCRIPCIÓN
Constructor	Constructores	Los constructores sirven para generar virus, gusanos y caballos de Troya nuevos. Algunos constructores poseen una interfaz estándar con ventanas, que permite al pirata seleccionar el tipo de programa malintencionado creado, el método utilizado para resistir a los métodos de depuración así como otras propiedades.
DoS	Ataques de red	Los programas de ataque DoS (Denial-of-Service) envían numerosas peticiones al servidor remoto desde el equipo del usuario. El servidor paraliza sus recursos para procesar las peticiones hasta que deja de funcionar.

TIPO	NOMBRE	DESCRIPCIÓN
Exploit	Exploit/Hazaña	<p>Un exploit ("hazaña") es un conjunto de datos o un trozo de código que aprovecha las vulnerabilidades de la aplicación objetivo para realizar una acción malintencionada en el equipo. Por ejemplo, una hazaña puede escribir o leer archivos, o abrir páginas Web "infectadas".</p> <p>Las diferentes hazañas aprovechan las vulnerabilidades de diferentes aplicaciones o servicios de red. Una hazaña se transmite por la red a múltiples equipos como un paquete de red, para buscar equipos con servicios de red vulnerables. Por ejemplo, una hazaña incluida en un archivo DOC busca las vulnerabilidades de los procesadores de texto y, cuando el usuario abre un archivo infectado, ejecuta las funciones programadas por el intruso. Un hazaña contenida en un mensaje de correo busca vulnerabilidades dentro de los clientes de correo; es capaz de ejecutar su acción malintencionada tan pronto como el usuario abre el mensaje infectado dentro del programa.</p> <p>Las hazañas sirven para difundir gusanos de red (Net-Worm). Los Exploits-Nukers son paquetes de red que inutilizan los equipos.</p>
FileCryptors	Cifradores de archivos	Los cifradores de archivos procesan otros programas malintencionados para ocultarlos de las aplicaciones antivirus.

TIPO	NOMBRE	DESCRIPCIÓN
Flooders	Programas de saturación de redes	<p>Envían un gran número de mensajes a través de canales de comunicación por red, en canales IRC por ejemplo.</p> <p>Sin embargo, esta categoría de software malintencionado no incluye programas que saturen el tráfico de correo, canales de mensajería instantánea o envíen SMS, que ya están clasificados como tipos aparte en la tabla siguiente (Email-Flooder, IM-Flooder y SMS-Flooder).</p>
HackTools	Herramientas de efracción	<p>Las herramientas de efracción (hacking) sirven para piratear los equipos donde se encuentran instaladas, o para organizar ataques desde otro equipo. Estos ataques comprenden: agregar usuarios de sistema sin autorización; borrar los informes de sistema para ocultar cualquier rastro de su presencia en el sistema. Incluyen algunos "sniffers" (rastreadores de tráfico de red) que ejecutan funciones malintencionadas, como interceptar contraseñas, por ejemplo. Los rastreadores son programas que permiten examinar el tráfico de red.</p>
not-virus:Hoax	Bromistas	<p>Estos programas asustan al usuario con mensajes parecidos a virus: avisan de la "detección" de un virus dentro de un archivo sano, o informan con un mensaje del formateo del disco, sin que se produzca.</p>
Spoofers	Spoofers	<p>Estos programas envían mensajes y peticiones de red con una dirección de remite simulada. Los intrusos utilizan spoofers (simuladores), por ejemplo, para aparentar ser otro remitente.</p>
VirTools	Herramientas que modifican programas malintencionados	<p>Permiten modificar otros programas malintencionados para ocultarlos de las aplicaciones antivirus.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Email-Flooders	Programas de saturación para direcciones de correo	Estos programas envían numerosos mensajes a direcciones de correo electrónico (las inundan). Debido al amplio flujo de mensajes, los usuarios se vuelven incapaces de distinguir mensajes entrantes no deseados.
IM-Flooders	Programas de saturación para mensajería instantánea	Estos programas envían gran número de mensajes a usuarios de clientes de mensajería instantánea (IM), como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ó Skype. Debido al amplio flujo de mensajes, los usuarios se vuelven incapaces de distinguir mensajes entrantes no deseados.
SMS-Flooders	Programas de saturación con mensajes SMS	Estos programas envían numerosos mensajes SMS a teléfonos móviles.

PROGRAMAS POTENCIALMENTE INDESEADOS

Programas potencialmente indeseados: a diferencia de los programas malintencionados, no están pensados sólo para producir daños. Sin embargo, pueden servir para romper la seguridad del equipo.

Los programas potencialmente indeseados incluyen software publicitario (adware), los captadores pornográficos (pornware) y otros *programas potencialmente indeseados*.

Programas publicitarios o *Adware* (página 31) presentan información publicitaria ante el usuario.

Captadores pornográficos o *Pornware* (página 31) presentan información pornográfica ante el usuario.

Otros programas de riesgo o *riskware* (página 32) suelen ser programas útiles instalados por muchos usuarios informáticos. Sin embargo, si un intruso consigue introducirse o instalar dichos programas en el equipo del usuario, podrá explotar algunas de sus características para romper la seguridad del sistema.

Los programas potencialmente indeseados son instalados mediante uno de los siguientes métodos:

- Son instalados por el usuario, individualmente o junto con otro programa. Por ejemplo, los desarrolladores de software incluyen programas publicitarios dentro sus programas freeware o shareware.
- También son instalados por los intrusos. Por ejemplo, vienen incluidos en paquetes de otros programas malintencionados, aprovechan "vulnerabilidades" del navegador Web o utilizan cargadores o lanzaderas de troyanos, cuando el usuario visita un sitio Web "infectado".

SOFTWARE PUBLICITARIO (ADWARE)

Subcategoría: Software publicitario (adware)

Nivel de riesgo: Medio

Los programas publicitarios (Adware) implican la presentación de publicidad ante el usuario. Muestran pancartas publicitarias en la interfaz de otros programas y redireccionan las consultas de búsqueda hacia sitios Web de publicidad. Algunos programas publicitarios coleccionan y envían a sus desarrolladores los datos del usuario para uso comercial: por ejemplo, qué sitios visita, qué búsquedas hace. A diferencia de los troyanos espía, estos programas transfieren la información con autorización del usuario.

SOFTWARE PORNOGRÁFICO (PORNWARE)

Subcategoría: Software pornográfico (pornware)

Nivel de riesgo: Medio

Normalmente, son los usuarios los que instalan estos programas para buscar o descargar pornografía.

Los intrusos también pueden instalar estos programas en el equipo del usuario para mostrar publicidad de sitios y servicios comerciales pornográficos, sin haber sido autorizados para ello. Para instalarlos, aprovechan vulnerabilidades del sistema operativo o del navegador Web y son distribuidos normalmente por cargadores o lanzaderas de troyanos.

Existen tres tipos de captadores pornográficos, descritos en la tabla a continuación.

Tabla 4. Tipos de captadores pornográficos, clasificados por función

TIPO	NOMBRE	DESCRIPCIÓN
Porn-Dialers	Marcadores automáticos	Estos programas marcan automáticamente los teléfonos de servicios pornográficos que incorporan; a diferencia de los troyanos marcadores, informan al usuario de su acción.
Porn-Downloaders	Programas de descarga de archivos por Internet	Estos programas descargan información pornográfica en el equipo del usuario; a diferencia de los troyanos marcadores, informan al usuario de su acción.
Porn-Tools	Herramientas	Permiten buscar y visualizar contenidos pornográficos; este tipo incluye barras de herramientas especiales para navegadores y reproductores de vídeo.

OTROS PROGRAMAS DE RIESGO

Subcategoría: otros programas de riesgo

Nivel de riesgo: Medio

La mayoría de estos programas son herramientas legítimas utilizadas por muchos usuarios. Se incluyen los clientes IRC, marcadores telefónicos, programas de descarga de archivos, monitores de actividad del sistema, herramientas para trabajar con contraseñas, servidores Internet FTP, HTTP ó Telnet.

Sin embargo, si un intruso consigue introducirse o instalar dichos programas en el equipo del usuario, sus características permiten romper la seguridad del sistema.

La tabla siguiente describe programas de riesgo agrupados por característica:

Tabla 5. Otros tipos de software de riesgo agrupados por característica

TIPO	NOMBRE	DESCRIPCIÓN
Client-IRC	Programas clientes de Internet chat	Los usuarios instalan estos programas para comunicarse por IRC. Los intrusos los utilizan para propagar programas malintencionados.
Dialers	Programas de marcación automática	Estos programas establecen conexiones telefónicas "ocultas" por módem.
Downloaders	Descargadores de archivos	Estos programas descargan en secreto archivos desde sitios Web.
Monitors	Supervisores	Estos programas supervisan la actividad de los equipos donde se encuentran instalados, incluido el rendimiento de las aplicaciones y los intercambios de datos con aplicaciones de otros equipos.
PSWTools	Herramientas de recuperación de contraseñas	Estos programas sirven para mostrar y recuperar contraseñas olvidadas. Los intrusos los utilizan del mismo modo cuando se instalan en los equipos de los usuarios.

TIPO	NOMBRE	DESCRIPCIÓN
RemoteAdmin	Programas de administración remota	<p>Estos programas son utilizados a menudo por administradores de sistema; dan acceso a la interfaz del equipo remoto con el fin de monitorizarla y controlarla. Los intrusos los utilizan del mismo modo cuando se instalan en los equipos de los usuarios.</p> <p>Los programas de riesgo destinados a la administración remota son diferentes de los troyanos de administración remota, o puertas traseras (Backdoor en inglés). Los troyanos disponen de funciones que les permiten infiltrarse e instalarse en el sistema de forma independiente; los programas legítimos no presentan estas características.</p>
Server-FTP	Servidores FTP	Estos programas ofrecen funciones propias de servidores FTP. Los intrusos los instalan en los equipos de los usuarios para tener acceso remoto a través del protocolo FTP.
Server-Proxy	Servidores proxy	Estos programas ofrecen funciones propias de servidores proxy. Los intrusos se instalan en el equipo para enviar correo no deseado utilizando la identidad del usuario.
Server-Telnet	Servidores Telnet	Estos programas ofrecen funciones propias de servidores Telnet. Los intrusos los instalan en los equipos de los usuarios para tener acceso remoto a través del protocolo Telnet.
Server-Web	Servidores Web	Estos programas ofrecen funciones propias de servidores Web. Los intrusos los instalan en los equipos de los usuarios para tener acceso remoto a través del protocolo HTTP.

TIPO	NOMBRE	DESCRIPCIÓN
RiskTool	Herramientas locales del equipo	Estas herramientas proporcionan características avanzadas que se utilizan tan sólo en el equipo del usuario. Permiten al intruso ocultar archivos o ventanas de aplicaciones activas, o cerrar procesos activos.
NetTool	Herramientas de red	Estas herramientas permiten al usuario de un equipo controlar otros equipos en la red: por ejemplo, para reiniciarlos, encontrar puertos abiertos o ejecutar programas instalados en esos equipos.
Client-P2P	Cientes P2P	Estos programas son utilizados en redes punto a punto (P2P). Los intrusos pueden utilizarlos para propagar programas malintencionados.
Client-SMTP	Cientes SMTP	Estos programas envían mensajes de correo y ocultan sus actividades. Los intrusos se instalan en el equipo para enviar correo no deseado utilizando la identidad del usuario.
WebToolbar	Barras de herramientas Web	Estos programas agregan sus propias barras de herramientas a las de otras aplicaciones.
FraudTool	Programas fraudulentos	Estos programas se presentan como si fuesen otros programas auténticos. Por ejemplo, existen programas antivirus fraudulentos que muestran mensajes acerca de la detección de programas malintencionados, pero no encuentran ni neutralizan nada.

MÉTODOS DE DETECCIÓN DE OBJETOS INFECTADOS, SOSPECHOSOS Y POTENCIALMENTE PELIGROSOS POR LA APLICACIÓN

Kaspersky Internet Security detecta los programas malintencionados utilizando dos métodos: el método reactivo (mediante bases de datos) y el método proactivo (mediante análisis heurístico).

Las bases de datos de la aplicación contienen registros utilizados para identificar centenares de miles de amenazas conocidas en los objetos analizados. Los registros contienen información sobre los segmentos de control en el código de los programas malintencionados así como sobre los algoritmos utilizados para desinfectar los objetos que contienen estos programas. Los analistas antivirus de Kaspersky Lab analizan a diario centenares de nuevos programas malintencionados, crean registros que los identifican y los incluyen en actualizaciones a la base de datos.

Si Kaspersky Internet Security detecta en un objeto examinado segmentos de código que coinciden exactamente con las secciones de control de un programa malintencionado, gracias a la información disponible en la base, determinará que se trata de un objeto *infectado*: si sólo coincide en parte, su estado se define como *sospechoso*.

Con el método proactivo, la aplicación consigue detectar nuevos programas malintencionados, que no aparecen en la base de datos.

La aplicación es capaz de detectar objetos que contienen nuevos programas malintencionados, en función de su comportamiento. El código de un nuevo objeto puede no coincidir en parte o en totalidad con el de un programa malintencionado conocido, pero contiene secuencias de comandos características, como la apertura o escritura de un archivo, o la interceptación de vectores de interrupción. La aplicación determina por ejemplo que un archivo puede estar infectado por un virus de arranque desconocido.

Los objetos detectado por el método proactivo son designados como *potencialmente peligrosos*.

AMENAZAS INTERNET

La aplicación Kaspersky Lab utiliza tecnologías especiales para evitar las siguientes amenazas a la seguridad de su equipo:

- Correo entrante no solicitado o spam (página 37);
- Fraudes de phishing (página 38);
- Ataques de piratas (página 38);
- banners publicitarios (página 39).

CORREO NO SOLICITADO (SPAM)

La aplicación Kaspersky Lab protege a los usuarios contra el correo no solicitado. El Spam son mensajes entrantes no solicitados, a menudo con contenido publicitario. El correo no solicitado supone una carga adicional para la red y los servidores del proveedor de correo. El destinatario paga por el tráfico no deseado generado y los mensajes normales se transmiten con retraso. Por esta razón, el correo no solicitado se considera ilegal en muchos países.

Kaspersky Internet Security se integra en clientes de correo (Microsoft Office Outlook, Microsoft Outlook Express y The Bat!) y analiza los mensajes entrantes. Los mensajes identificados como no deseados son procesados de acuerdo con acciones definidas por el usuario: por ejemplo, el posible mover el mensaje a una carpeta especial, o eliminarlo.

Kaspersky Internet Security detecta el correo no deseado con un grado elevado de precisión. Aplica numerosas tecnologías de filtrado antispam, incluido: análisis de la dirección del remitente, de palabras y frases presentes en el asunto; reconoce mensajes gráficos no deseados y ejecuta un algoritmo de autoaprendizaje para mejorar su detección antispam a partir del texto del mensaje.

Las bases antispam contienen listas "negra" y "blanca" de direcciones de remite, así como listas de palabras y frases relacionadas con varias categorías de correo no deseado, como publicidad, medicamentos y salud o apuestas en línea.

FRAUDES POR INTERNET (PHISHING)

El Phishing (aproximadamente, un "anzuelo") es un tipo de fraude por Internet que intenta "pescar" números de tarjetas de crédito, códigos PIN y otra información personal, con el fin de robar dinero.

Los anzuelos se asocian a menudo con entidades financieras en Internet. Los intrusos crean un réplica exacta del banco objetivo y envían mensajes a sus clientes sin su conocimiento. Los clientes son informados de que, debido a ciertos cambios o fallos en el software bancario, se han perdido las cuentas de los usuarios, por lo que éstos deben confirmar o modificar sus datos en el sitio Web de su banco. El usuario se conecta al sitio Web del intruso, donde comunica sus datos personales.

Las bases del componente Anti-Phishing contienen una lista de direcciones URL de sitios Web conocidos por ser origen de fraudes.

Kaspersky Internet Security analiza los mensajes entrantes de clientes compatibles (Microsoft Office Outlook y Microsoft Outlook Express), y si encuentra un vínculo a una dirección URL presente lista de sitios fraudulentos, lo clasifica como no deseado. Si el usuario abre el mensaje e intenta seguir el vínculo, la aplicación bloquea la conexión con el sitio Web.

ATAQUES DE PIRATAS

Un ataque de red es una intrusión destinada a tomar el control de un sistema informático remoto, normalmente para provocar su caída o para obtener acceso a información protegida.

Los ataques de red pueden ser acciones intrusivas (por ejemplo, exploración de puertos, intentos de robo de contraseñas) o programas malintencionados que ejecutan comandos en nombre del usuario para, por ejemplo, transmitir la información al programa "maestro" remoto. Entre estos programas, se encuentran troyanos, ataques DoS (denegación de servicio), scripts malintencionados y algunos tipos de gusanos de red.

Los ataques de red penetran en la red local y las redes globales aprovechando vulnerabilidades de los sistemas operativos y aplicaciones. Pueden transferirse como paquetes de datos IP durante las conexiones de red.

Kaspersky Internet Security bloquea los ataques de red sin perturbar las conexiones, mediante una base de datos especial del componente Firewall. Estas bases de datos contienen registros que identifican los paquetes de datos

IP característicos de varios programas intrusivos. La aplicación analiza las conexiones de red y bloquea cualquier paquete IP peligroso.

BANNERS

Los *banners* o publicidades emergentes son vínculos al sitio Web del anunciante, presentadas la mayoría de las veces como imágenes. La aparición de pancartas en el sitio Web no supone ninguna amenaza para la seguridad del equipo, pero se considera una interferencia dentro del funcionamiento normal del equipo. Las pancartas intermitentes en pantalla perturban las condiciones y reducen la eficiencia del trabajo. El usuario está distraído por información irrelevante y la visita de los vínculos de publicidad aumenta el tráfico Internet.

Muchas organizaciones prohíben la presentación de publicidad en sus interfaces, dentro de sus directivas de seguridad de datos.

Kaspersky Internet Security bloquea los banners en función de la dirección URL del sitio Web al que apunta la publicidad. Utiliza una base antibanner actualizable con una lista de direcciones URL de publicidad rusas e internacionales. La aplicación examina los vínculos del sitio Web visitado, los compara con las direcciones en la base y si alguna corresponde, elimina el vínculo hacia dicha dirección y sigue cargando la página.

INSTALACIÓN DE LA APLICACIÓN

El Asistente de instalación deja la aplicación instalada en el equipo en modo interactivo.

Advertencia.

Le recomendamos cerrar todos los programas en ejecución antes de continuar la instalación.

Para instalar la aplicación en su equipo, ejecute el archivo de distribución (con extensión *.exe).

Tras esto, el programa busca el paquete de instalación de la aplicación (con extensión *.msi) y, si lo encuentra, busca una versión nueva en los servidores Internet de Kaspersky Lab. Si no encuentra ningún paquete de instalación, ofrece descargarlo. Después de terminar la descarga, comienza la instalación de Kaspersky Internet Security. Si no acepta la descarga, la instalación de la aplicación continúa en el modo estándar.

El programa de instalación está diseñado como un Asistente. Cada ventana contiene un conjunto de botones para desplazarse por el proceso de instalación. A continuación aportamos una breve descripción del uso de cada botón:

- **Siguiente:** acepta la acción y pasa a la etapa siguiente de la instalación.
- **Anterior:** regresa al paso anterior del proceso de instalación.
- **Cancelar:** cancela la instalación.
- **Terminar:** termina la instalación de la aplicación.

Damos a continuación una explicación detallada de cada etapa de la instalación del paquete.

EN ESTA SECCIÓN:

Paso 1. Descarga de versiones recientes de la aplicación.....	41
Paso 2. Comprobación de los requisitos de instalación en el sistema	42
Paso 3. Ventana de bienvenida del Asistente	42
Paso 4. Lectura del Contrato de licencia	43
Paso 5. Selección del tipo de instalación	43
Paso 6. Selección de la carpeta de instalación	44
Paso 7. Selección de los componentes de aplicación para instalar	44
Paso 8. Búsqueda de otro software antivirus	45
Paso 9. Preparación final de la instalación.....	46
Paso 10. Fin de la instalación.....	46

PASO 1. DESCARGA DE VERSIONES RECIENTES DE LA APLICACIÓN

Antes de instalar la aplicación en su equipo, el Asistente busca en los servidores de actualización de Kaspersky Lab si existe una nueva versión de la aplicación que va a instalar.

Si no detecta la presencia de una versión nueva en los servidores de actualización de Kaspersky Lab, el Asistente de instalación continua para instalar la versión actual.

Si encuentra una versión más reciente de la aplicación en los servidores, el Asistente le ofrece descargarla. Si cancela la descarga, el Asistente de instalación se reanuda para instalar la versión actual. Si decide instalar una versión más reciente, los archivos de instalación son descargados en su equipo y el Asistente de instalación comienza automáticamente a instalar la versión más

reciente. Para más detalles acerca de la instalación de una versión más reciente, consulte la documentación de la versión correspondiente.

PASO 2. COMPROBACIÓN DE LOS REQUISITOS DE INSTALACIÓN EN EL SISTEMA

Antes de instalar la aplicación en su equipo el Asistente comprueba que el equipo cumple con los requisitos mínimos (sección "Requisitos hardware y software del sistema" en la página 13). También comprueba que dispone de los permisos necesarios para instalar el software.

En caso de no cumplirse estos requisitos, aparecerá un aviso correspondiente en pantalla. Le recomendamos instalar los programas y las actualizaciones requeridas con el servicio **Windows Update**, antes de intentar de nuevo instalar Kaspersky Internet Security.

PASO 3. VENTANA DE BIENVENIDA DEL ASISTENTE

Si su sistema cumple todos los requisitos (sección "Requisitos hardware y software del sistema" en la página 13), si no existe una versión nueva en los servidores de actualización de Kaspersky Lab o si cancela la instalación de ésta, el Asistente de instalación se reanuda para instalar la versión actual de la aplicación.

Se muestra en pantalla el primer cuadro de diálogo del Asistente, indicando el inicio de la instalación.

Para continuar con la instalación, haga clic en **Siguiente**. Para cancelar la instalación, haga clic en **Cancelar**.

PASO 4. LECTURA DEL CONTRATO DE LICENCIA

El cuadro de diálogo siguiente incluye el Contrato de licencia entre Usted y Kaspersky Lab. Léalo con atención y si está de acuerdo con todos los términos y condiciones del contrato, seleccione **Acepto los términos del Contrato de Licencia** y haga clic en **Siguiente**. La instalación continúa.

Para cancelar la instalación, haga clic en **Cancelar**.

PASO 5. SELECCIÓN DEL TIPO DE INSTALACIÓN

En este paso, puede seleccionar el tipo de instalación que mejor se adapta a sus necesidades:

- **Instalación rápida.** Si selecciona esta opción, se instalará la aplicación completa en su equipo, con los parámetros de protección recomendados por Kaspersky Lab. Después de completar la instalación, se abre el Asistente de configuración de la aplicación.
- **Instalación personalizada.** En este paso, podrá: seleccionar los componentes de la aplicación que desea instalar; especificar la carpeta de destino de la instalación (sección "Paso 6. Selección de la carpeta de instalación" en la página 44); activar y configurar la aplicación con el Asistente de configuración de la aplicación.

Si la primera opción, el Asistente de instalación de la aplicación pasa directamente al Paso 8 (sección "Paso 8. Búsqueda de otro software antivirus" en la página 45). En otro caso, será necesario especificar su decisión en cada paso de la instalación.

PASO 6. SELECCIÓN DE LA CARPETA DE INSTALACIÓN

Nota

Este paso del Asistente de instalación sólo se produce si selecciona la opción de instalación personalizada (sección "Paso 5. Selección del tipo de instalación" en la página 43).

Este paso permite indicar una carpeta en su equipo en la que se instalará la aplicación. La ruta predeterminada es:

- <Unidad> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009 Special Edition for Ultra-Portables : para sistemas de 32 bits.

Para especificar una carpeta diferente haga clic en el botón **Examinar** y seleccione ésta en el cuadro de diálogo estándar de selección de carpetas, o escriba la ruta de la carpeta en el campo de entrada.

Advertencia.

Recuerde que si especifica manualmente la ruta completa de la carpeta de instalación, su nombre no debe superar 200 caracteres ni la ruta debe incluir caracteres especiales.

Para continuar con la instalación, haga clic en **Siguiente**.

PASO 7. SELECCIÓN DE LOS COMPONENTES DE APLICACIÓN PARA INSTALAR

Nota. Este paso del Asistente de instalación sólo se produce si selecciona la opción de instalación personalizada (sección "Paso 5. Selección del tipo de instalación" en la página 43).

Durante una instalación personalizada, debe seleccionar los componentes de la aplicación que desea instalar en su equipo. De forma predeterminada, todos los componentes están seleccionados: componentes de protección, análisis y actualización.

Para ayudarle a elegir los componentes, dispone de información acerca de cada uno: seleccione el componente en la lista y lea la descripción asociada en el campo inferior. La información contiene una breve descripción del componente y los requisitos de espacio libre en disco para su instalación.

Para evitar la instalación de cualquier componente, abra el menú contextual con un clic en el icono junto al nombre del componente y seleccione la opción **Componente no disponible**. Observe que si cancela la instalación de algún componente, no estará protegido contra un cierto número de programas peligrosos.

Para seleccionar la instalación de un componente, abra el menú contextual con un clic en el icono junto al nombre del componente y seleccione la opción **Se instalará en la unidad de disco duro local**.

Después de seleccionar los componentes para instalar, haga clic en **Siguiente**. Para regresar a la lista predeterminada de componentes de instalación, haga clic en **Borrar**.

PASO 8. BÚSQUEDA DE OTRO SOFTWARE ANTIVIRUS

En este paso, el Asistente busca otros programas antivirus, inclusive programas Kaspersky Lab que puedan entrar en conflicto con la aplicación una vez instalada.

Si se detectan en su equipo, la lista de estos programas se muestra en pantalla. Podrá eliminarlos antes de continuar con la instalación.

Puede decidir si los elimina automáticamente o manualmente con los controles ubicados debajo de la lista de programas antivirus detectados.

Para continuar con la instalación, haga clic en **Siguiente**.

PASO 9. PREPARACIÓN FINAL DE LA INSTALACIÓN

Este paso completa la preparación de la instalación de la aplicación en su equipo.

Durante la instalación inicial y personalizada de la aplicación (sección "Paso 5. Selección del tipo de instalación" en la página 43) recomendamos no desactivar la casilla **Activar la Autoprotección antes de instalar** durante la instalación inicial. Si la opción de protección del módulo está activada y ocurre un error durante la instalación, se asegura así una posible anulación correcta del procedimiento de instalación. Cuando vuelve a intentar la instalación, recomendamos desactivar esta casilla.

Nota

En caso de instalar de forma remota de la aplicación con **Escritorio remoto**, recomendamos desactivar la casilla **Activar la Autoprotección antes de instalar**. Si activa la casilla, la instalación puede desarrollarse incorrectamente o no realizarse en absoluto.

Para continuar con la instalación, haga clic en **Siguiente**. Comenzará la copia de los archivos de instalación en su equipo.

Advertencia.

Durante el proceso de instalación, la conexión de red actual se interrumpirá si el paquete de aplicación incluye los componentes que interceptan el tráfico de red. La mayoría de las conexiones interrumpidas serán restauradas automáticamente en su debido tiempo.

PASO 10. FIN DE LA INSTALACIÓN

La ventana **Instalación terminada** informa del fin del proceso de instalación de la aplicación en su equipo.

La ventana indica, por ejemplo, si es necesario reiniciar el equipo para completar correctamente la instalación. Después de reiniciar, el Asistente de instalación se reanudará automáticamente.

Si no es necesario reiniciar el sistema, haga clic en **Siguiente** para iniciar el Asistente de configuración de la aplicación.

INTERFAZ DEL PROGRAMA

La aplicación posee una interfaz sencilla e intuitiva. Este capítulo describe sus características básicas en detalle.

Además de la interfaz principal del programa, existen complementos para Microsoft Office Outlook, The Bat! y el Explorador de Microsoft Windows. Los complementos amplían las funciones de estos programas al permitir administrar y configurar los componentes de Kaspersky Internet Security desde la interfaz del programa cliente.



EN ESTA SECCIÓN:

Icono del área de notificaciones	47
Menú contextual	48
Ventana principal de la aplicación	50
Notificaciones	53
Ventana de configuración de la aplicación	53

ICONO DEL ÁREA DE NOTIFICACIONES

Inmediatamente después de instalar la aplicación, su icono aparece en el área de notificaciones de la barra de tareas de Microsoft Windows.

Este icono es un indicador de la operación actual de la aplicación. También refleja el estado de protección y muestra un número de funciones básicas realizadas por el programa.

Si el icono está activo  (color), todos o algunos componentes de protección de la aplicación están en ejecución. Si el icono se encuentra inactivo  (blanco y negro), todos los componentes están desactivados.

El icono de la aplicación cambia en función de la operación realizada:



– Análisis en curso del correo.



– Actualización de las bases y módulos de programa de la aplicación.



– Es necesario reiniciar para aplicar las actualizaciones.




– Ocurrió un error en alguno de los componentes de Kaspersky Internet Security.

El icono también facilita el acceso a las funciones básicas de la interfaz de la aplicación, incluyendo el menú contextual (sección "Menú contextual" en la página 48) y la ventana principal de la aplicación (sección "Ventana principal de la aplicación" en la página 50).

Para abrir el menú contextual, haga clic con el botón derecho en el icono de la aplicación.

Para abrir la ventana principal de la aplicación, haga doble clic en el icono de la aplicación. La ventana principal siempre se abre en la sección **Protección**.

Si hay noticias disponibles desde Kaspersky Lab, el icono de noticias aparece en el área de notificaciones de la barra de tareas . Haga doble clic en el icono para mostrar las noticias en la ventana de respuesta.

MENÚ CONTEXTUAL

Puede ejecutar tareas de protección básica desde el menú contextual, que incluye estos elementos:

- **Actualizar:** ejecuta la actualización de las bases y módulos de la aplicación y los instala en su equipo.
- **Análisis completo:** ejecuta un análisis completo del equipo en busca de objetos peligrosos. Se analizan los archivos de todas las unidades, incluso en los medios extraíbles.
- **Análisis antivirus:** selecciona objetos y ejecuta un análisis antivirus. De forma predeterminada la lista contiene varios objetos, como la carpeta **Mis documentos** y los buzones de correo. Puede completar esta lista con la selección de otros objetos para analizar.

- **Monitor de red:** muestra la lista de conexiones de red establecidas, los puertos abiertos y el tráfico.
- **Teclado virtual:** cambia al teclado virtual.
- **Kaspersky Internet Security:** abre la ventana principal de la aplicación (sección "Ventana principal de la aplicación" en la página 50).
- **Configuración:** ver y modificar los parámetros de aplicación.
- **Activar la aplicación:** activa el programa. Para beneficiarse de la condición de usuario registrado, debe activar su aplicación. Esta opción de menú sólo está disponible si la aplicación no ha sido activada.
- **Acerca de:** abre una ventana con información acerca de la aplicación.
- **Suspender / Reanudar la protección:** desactiva temporalmente o activa los componentes de protección en tiempo real. Esta opción del menú no afecta a las actualizaciones de la aplicación ni a las tareas de análisis antivirus.
- **Bloquear el tráfico de red:** bloquea temporalmente todas las conexiones de red del equipo. Si desea autorizar el acceso del equipo a la red, utilice de nuevo este comando desde el menú contextual.
- **Salir:** termina y descarga la aplicación de la memoria del equipo.



Figura 1: Menú contextual

Si una tarea de análisis antivirus está en ejecución, su nombre aparece en el menú contextual con una barra de progreso (porcentaje terminado). Si

selecciona la tarea, podrá abrir la ventana de informe para conocer los resultados de ejecución actuales de la tarea.

VENTANA PRINCIPAL DE LA APLICACIÓN

La ventana principal de la aplicación puede dividirse en tres partes:

- La parte superior de la ventana le informa sobre el estado actual de la protección de su equipo.



Figura 2: Estado actual de la protección del equipo

Existen tres estados de protección posibles: cada uno viene indicado por un color similar al que se utiliza en los semáforos. El color verde significa que el nivel de protección del equipo es el correcto, mientras los colores amarillo y rojo avisan de la presencia de amenazas de seguridad en la configuración o en el funcionamiento de la aplicación. Además de programas malintencionados, también se consideran amenazas bases de aplicación desfasadas, componentes de protección desactivados o la selección de parámetros mínimos.

Las amenazas a la seguridad deben eliminarse en cuanto aparecen. Para obtener información detallada y sobre su eliminación rápida, utilice el vínculo **Reparar ahora** (figura anterior).

- La parte izquierda de la ventana, la barra de exploración, ofrece acceso rápido a cualquier función de la aplicación, incluyendo las tareas de búsqueda antivirus o de actualización.



Figura 3: Parte izquierda de la ventana principal

- La parte derecha de la ventana contiene información acerca de la función seleccionada en la parte izquierda, permite configurar dichas funciones y ofrece herramientas para tareas de análisis antivirus, descarga de actualizaciones, etc.



Figura 4: Sección informativa de la ventana principal

También puede utilizar los botones:

- **Configuración:** abre la ventana de configuración de la aplicación.
- **Ayuda:** abre el sistema de ayuda de la aplicación.
- **Detectados:** abre la lista de objetos dañinos detectados por cualquiera de los componentes o tareas de análisis antivirus, y permite visualizar estadísticas detalladas de la actividad de la aplicación.
- **Informes:** abre la lista de eventos ocurridos durante el funcionamiento de la aplicación.
- **Soporte:** abre la ventana con información acerca del sistema y vínculos hacia recursos de información de Kaspersky Lab (sitio del Servicio de Soporte técnico, foro).

Nota

Para modificar la apariencia de la aplicación, puede crear y utilizar sus propias combinaciones gráficas y de color.

NOTIFICACIONES

Si se producen eventos durante el funcionamiento de la aplicación, aparecen en pantalla notificaciones especiales con forma de mensajes emergentes por encima del icono de la aplicación en la barra de tareas de Microsoft Windows.

En función del grado de gravedad del evento, en relación con la seguridad del equipo, puede recibir los siguientes tipos de notificaciones:

- **Alerta.** Se ha producido un evento crítico; por ejemplo, se detectó la presencia de un virus o una actividad peligrosa en su sistema. Debe decidir inmediatamente cómo responder a esta amenaza. Este tipo de notificación aparece en rojo.
- **Advertencia.** Se ha producido un evento potencialmente peligroso. Por ejemplo, se detectó la presencia de archivos potencialmente infectados o una actividad sospechosa en su sistema. Debe instruir al programa en función del peligro relacionado con este evento. Este tipo de notificación aparece en amarillo.
- **Nota.** Esta notificación le ofrece información acerca de eventos sin gravedad. Este tipo, por ejemplo, incluye notificaciones relativas al funcionamiento del componente **Filtrado de contenidos**. Las notificaciones informativas están en verde.

VENTANA DE CONFIGURACIÓN DE LA APLICACIÓN

Es posible abrir la ventana de configuración de la aplicación desde la ventana principal (sección "Ventana principal de la aplicación" en la página 50) o el menú contextual (sección "Menú contextual" en la página 48). Para abrir esta ventana, haga clic en el vínculo **Configuración** en la parte superior de la ventana principal o seleccione la opción apropiada en el menú contextual de la aplicación.

La ventana de configuración consta de dos partes:

- La parte izquierda de la ventana da acceso a los componentes de la aplicación, como tareas de análisis antivirus, y de actualización;
- La parte derecha de la ventana contiene la lista de parámetros del componente o tarea seleccionados en la izquierda de la ventana.

PRIMEROS PASOS

Uno de los principales objetivos de los expertos de Kaspersky Lab al diseñar Kaspersky Internet Security fue ofrecer una configuración óptima de todas las opciones del programa. Se posibilita así que incluso un usuario no familiarizado con su equipo pueda protegerlo inmediatamente después de su instalación, sin dedicarle horas a ajustar la configuración.

Para comodidad del usuario, hemos agrupado los pasos iniciales de configuración dentro de un mismo Asistente de primera configuración que se inicia tan pronto como se instala la aplicación. Siguiendo las instrucciones del Asistente, podrá activar el programa, configurar los parámetros de actualización, restringir el acceso al programa con una contraseña y ajustar otros parámetros.

Su equipo puede estar infectado por software malintencionado antes de instalar la aplicación. Para detectar los programas malintencionados existentes, ejecute un análisis del equipo (sección "Análisis antivirus del equipo" en la página 57).

Como consecuencia de una infección por software malintencionado o de fallos en el sistema, la configuración de su equipo puede estar dañada. Ejecute el Asistente de análisis de seguridad para encontrar vulnerabilidades en el software instalado o anomalías en la configuración del sistema.

Las bases de aplicación incluidas en el paquete de instalación estarán probablemente desfasadas. Actualice la aplicación (página 56), si no lo hizo el Asistente de instalación o automáticamente, inmediatamente después de instalar la aplicación.

El componente Anti-Spam incluido dentro de la aplicación utiliza un algoritmo de aprendizaje automático para detectar mensajes no deseados. Ejecute el Asistente de aprendizaje antispam para configurar el componente a partir de su propia correspondencia.

Después de completar las acciones en esta sección, la aplicación estará lista para proteger su equipo. Para evaluar el nivel de protección de su equipo, utilice el Asistente de administración de la seguridad (sección "Administración de la seguridad" en la página 62).

EN ESTA SECCIÓN:

Selección del tipo de red	55
Actualización de la aplicación.....	56
Análisis de seguridad	56
Análisis antivirus del equipo	57
Administración de la licencia	58
Suscripción para la renovación automática de la licencia	59
Participación en el programa Kaspersky Security Network	61
Administración de la seguridad.....	62
Suspensión de la protección.....	64

SELECCIÓN DEL TIPO DE RED

Después de instalar la aplicación, el componente Firewall analizará las conexiones de red activas en su equipo. Cada conexión de red se ve atribuir un estado que determina qué actividades de red son autorizadas.

Si seleccionó el modo interactivo de funcionamiento, Kaspersky Internet Security abrirá notificaciones cada vez que se establezca una conexión de red. Seleccione el estado de las nuevas redes en la ventana de notificaciones:

- **Red pública:** el acceso a su equipo desde el exterior así como a las carpetas públicas e impresoras está bloqueado. Este es el estado recomendado para conexiones a la red Internet.
- **Red local:** el acceso a carpetas públicas e impresoras está autorizado. Le recomendamos asociar este estado a las redes locales protegidas, por ejemplo, una red corporativa.
- **Redes de confianza:** cualquier actividad está autorizada. Le recomendamos asociar este estado tan sólo a zonas absolutamente seguras.

Para cada estado de red, Kaspersky Internet Security incluye un conjunto de reglas de administración de las actividades de red. Más tarde, puede cambiar el estado especificado para la red, después de su primera detección.

ACTUALIZACIÓN DE LA APLICACIÓN

Advertencia.

Necesita una conexión Internet para actualizar Kaspersky Internet Security.

Kaspersky Internet Security incluye bases de datos con firmas de amenazas, ejemplos de frases típicas del correo no deseado y descripciones de ataques de red. Sin embargo, cuando instale la aplicación, es posible que las bases de datos hayan quedado obsoletas, ya que Kaspersky Lab las actualiza regularmente, junto con los módulos de aplicación.

Puede especificar cómo se ejecuta la tarea de actualización durante la ejecución del Asistente de configuración de la aplicación. De forma predeterminada, Kaspersky Internet Security busca automáticamente actualizaciones en los servidores de Kaspersky Lab. Si el servidor contiene actualizaciones recientes, la aplicación las descarga e instala en segundo plano.

Para mantener siempre actualizada la protección de su equipo, le recomendamos actualizar Kaspersky Internet Security inmediatamente después de su instalación.

► *Para actualizar Kaspersky Internet Security,*

1. Abra la ventana principal de la aplicación.
2. Seleccione la entrada **Actualizar** en la parte izquierda de la ventana.
3. Haga clic en **Iniciar la actualización**.

ANÁLISIS DE SEGURIDAD

La configuración de su sistema operativo puede quedar dañada por fallos en el sistema o por la actuación de programas malintencionados. Adicionalmente, las aplicaciones instaladas en su equipo pueden contener vulnerabilidades que los intrusos pueden aprovechar para causar daños a su equipo.

Para detectar y eliminar estos problemas de seguridad, le recomendamos ejecutar el *Asistente para el análisis de la seguridad* después de instalar la aplicación. El Asistente busca vulnerabilidades en aplicaciones instaladas así como daños o anomalías en la configuración del sistema operativo y del navegador.

► *Para iniciar el asistente:*

1. Abra la ventana principal de la aplicación.
2. En la parte izquierda de la ventana seleccione **Vigilancia de aplicaciones**.
3. Inicie la tarea **Análisis de seguridad**.

ANÁLISIS ANTIVIRUS DEL EQUIPO

Debido a que los autores de software malintencionado se esfuerzan en disimular las acciones de sus programas, es posible que no se dé cuenta de su presencia dentro del equipo.

Una vez instalado en el equipo, Kaspersky Internet Security ejecuta automáticamente un **Análisis rápido** en su equipo. Esta tarea busca y neutraliza los programas dañinos presentes en los objetos que se cargan al arrancar el sistema operativo.

Los especialistas de Kaspersky Lab le recomiendan además ejecutar la tarea **Análisis completo**.

► *Para iniciar / detener una tarea de análisis antivirus:*

1. Abra la ventana principal de la aplicación.
2. En la parte izquierda de la ventana seleccione la entrada **Analizar (Análisis completo, Análisis rápido)**.
3. Haga clic en **Iniciar análisis** para iniciar el análisis. Si necesita detener la ejecución de la tarea, haga clic en **Detener análisis** durante el funcionamiento de la tarea.

ADMINISTRACIÓN DE LA LICENCIA

La aplicación requiere una llave de licencia para funcionar. Recibe una llave cuando adquiere el programa. Le da derecho a utilizar el programa a partir del día en que adquiere e instala la llave.

Sin una llave de licencia, a menos que la versión de evaluación del programa esté activada, la aplicación se ejecuta en modo limitado a una sola actualización. La aplicación no descargará ninguna nueva actualización.

Si activó la versión de evaluación del programa, tras este plazo, la aplicación dejará de funcionar.

Cuando la llave de licencia caduque, el programa seguirá funcionando, pero no podrá actualizar las bases de aplicación. Como antes, podrá analizar su equipo en busca de virus y utilizar los componentes de protección, pero sólo con las bases de aplicación disponibles cuando caducó la licencia. No podemos garantizarle la protección contra virus que aparezcan después de caducar su licencia.

Para proteger su equipo contra la infección de nuevos le recomendamos renovar la llave de la aplicación. El programa le notificará con dos semanas de antelación de la expiración de su licencia. Durante ese tiempo, un mensaje recordatorio se visualizará cada vez que inicie la aplicación.

Los datos de la llave actual se muestran en la entrada **Licencia** de la ventana principal de la aplicación: identificador de la llave, su tipo (comercial, evaluación, prueba beta), el número de equipos en los que puede instalarla, la fecha de caducidad y el número de días pendientes. Los datos de caducidad no aparecerán si instaló una licencia comercial con suscripción (sección "Suscripción para la renovación automática de la licencia" en la página 59).

Para examinar los términos del contrato de licencia, haga clic en **Ver el contrato de licencia de usuario final**. Para eliminar una llave de la lista, haga clic en **Eliminar**.

Para comprar o renovar una llave:

1. Adquirir una nueva llave. Para ello haga clic en **Adquirir una licencia** (si la aplicación no ha sido activada) o **Renovar la licencia**. La página Web abierta contiene toda la información sobre la compra de una llave en la tienda en línea de Kaspersky Lab o de sus empresas colaboradoras. Si su compra se realiza en línea, después de realizar el

pago, recibirá un archivo llave o un código de activación en la dirección indicada en el formulario de pedido.

2. Instale la llave. Para ello haga clic en **Instalar llave** en la sección **Licencia** de la ventana principal de la aplicación o utilice el comando **Activación** desde el menú principal de la aplicación. Se abrirá el Asistente de activación.

Nota. Kaspersky Lab ofrece regularmente amplios descuentos para renovar las licencias de nuestros productos. Compruebe las ofertas en el sitio Internet de Kaspersky Lab, en la zona **Products → Sales and special offers** (Venta de productos y ofertas especiales).

SUSCRIPCIÓN PARA LA RENOVACIÓN AUTOMÁTICA DE LA LICENCIA

Si adquiere su licencia mediante suscripción, la aplicación se pone automáticamente en contacto con el servidor de activación cada cierto tiempo para reactivar su licencia durante el plazo de suscripción.

Si la llave actual ha caducado, Kaspersky Internet Security comprueba en segundo plano la disponibilidad de una llave actualizada en el servidor. Si encuentra la llave, la aplicación la descarga e instala reemplazando la llave anterior. De este modo, es posible renovar la licencia sin necesidad de intervenir. Si el periodo de renovación de la licencia por la propia aplicación también ha caducado, es posible renovar la licencia manualmente. Durante el periodo de renovación manual de la licencia, se mantienen las características de la aplicación. Al finalizar este periodo, si no renovó la licencia, no se producirán nuevas actualizaciones de las bases de datos. Para rechazar la suscripción para la renovación automática de la licencia, póngase en contacto con la tienda en línea donde compró la aplicación.

Advertencia.

Si cuando activa la aplicación, ésta ya estaba activada con una llave comercial, dicha llave será reemplazada por la llave de suscripción. Si desea volver a utilizar la llave comercial, debe eliminar la llave de suscripción y activar de nuevo la aplicación con el código de activación que recibió junto con la llave comercial.

Las condiciones de la suscripción se ajustan a las cláusulas siguientes:

1. *Dañado*. Su solicitud de activación de suscripción no ha sido procesada todavía (es necesario un cierto tiempo para procesar la solicitud en el servidor). Kaspersky Internet Security opera en modo completamente funcional. Si después de un cierto tiempo, la solicitud de suscripción no ha sido procesada, una notificación le informará de ello. En este caso las bases de la aplicación no se actualizarán de nuevo.
2. *Activación*. La suscripción para la renovación automática de la licencia estaba activa por un plazo no limitado de tiempo (no se especifica fecha) o por un plazo determinado (fecha de final de la suscripción especificada).
3. *Renovado*. La suscripción fue renovada automática o manualmente por un plazo no limitado de tiempo (no se especifica fecha) o por un plazo determinado (se indica la fecha de final de la suscripción).
4. *Error*. La renovación de la suscripción produjo un error.
5. *Caducado*. El periodo de suscripción ha terminado. Puede utilizar otro código de activación o renovar su suscripción poniéndose en contacto con la tienda en línea donde adquirió la aplicación.
6. *Cancelación de la suscripción*. Puede cancelar su suscripción para la renovación automática de la licencia.
7. *La actualización es obligatoria*. No se recibió a tiempo la llave para renovar la suscripción por alguna razón. Utilice **Renovar el estado de suscripción** para renovar la suscripción.

Si el periodo de validez de la suscripción ha terminado, así como el periodo adicional durante el cual se puede renovar la licencia (estado de suscripción - *Terminado*), la aplicación emite una notificación y deja de intentar obtener una llave actualizada desde el servidor. Las funciones de la aplicación se mantendrán, con excepción de la característica de actualización de las bases de aplicación.

Si, por cualquier motivo, no se renovó la licencia (estado de suscripción - *Actualización necesaria*) en el plazo previsto (el equipo estaba apagado durante el periodo de renovación de la licencia, por ejemplo), puede actualizar el estado de la licencia manualmente. Para ello, utilice **Renovar el estado de suscripción**. Mientras no se renueva la suscripción, Kaspersky Internet Security deja de actualizar las bases de aplicación.

Mientras está vigente la suscripción, no puede instalar llaves de otro tipo ni utilizar otros códigos de activación para renovar la licencia. Sólo es posible utilizar otro código de activación después de terminar el periodo de suscripción (el estado de suscripción es *Caducado*).

Advertencia.

Observe que mientras utiliza una suscripción para renovar automáticamente la licencia, si reinstala la aplicación en su equipo, deberá activar de nuevo el producto manualmente, con el código de activación recibido al comprar la aplicación.

PARTICIPACIÓN EN EL PROGRAMA KASPERSKY SECURITY NETWORK

Todos los días, aparece un gran número de nuevas amenazas en todo el mundo. Para facilitar la recolección de estadísticas sobre los tipos y el origen de nuevas amenazas y desarrollar la forma de eliminarlas, Kaspersky Lab le invita a utilizar el programa Kaspersky Security Network.

La utilización de Kaspersky Security Network supone el envío de la información siguiente a Kaspersky Lab:

- Un identificador único atribuido a su equipo por la aplicación. Se trata de un identificador de la configuración hardware de su equipo y no contiene otra información.
- Información sobre amenazas detectadas por la aplicación. La estructura y contenido de la información depende del tipo de amenaza detectada.
- Información del sistema: versión del sistema operativo, Service Pack instalados, servicios y controladores descargados, versiones de clientes de correo y navegadores, extensiones del navegador, número de la versión instalada de Kaspersky Internet Security.

Kaspersky Security Network también recopila estadísticas ampliadas con información acerca de:

- archivos ejecutables y aplicaciones firmadas, descargadas en su equipo;
- aplicaciones en ejecución en su equipo.

La información estadística se envía cuando termina la actualización de la aplicación.

Advertencia.

Kaspersky Lab garantiza que dentro de Kaspersky Security Network, no se recolecta ni redistribuye ningún dato personal del usuario.

- ▶ Para configurar el envío de estadísticas:
 1. Abra la ventana de configuración de la aplicación.
 2. Seleccione la entrada **Comentarios** en la parte izquierda de la ventana.
 3. Active la casilla **Acepto participar en Kaspersky Security Network**, para confirmar su participación en el programa Kaspersky Security Network. Active la casilla **Acepto enviar estadísticas avanzadas dentro del programa Kaspersky Security Network**, para confirmar su aceptación antes de transmitir estadísticas ampliadas.

ADMINISTRACIÓN DE LA SEGURIDAD

Los problemas en la protección del equipo son indicados por el cambio de color del icono indicador del estado de la protección y del propio panel donde se encuentra el icono. En cuanto aparezca algún problema en el sistema de protección, recomendamos corregirlo inmediatamente.



Figura 5: estado actual de la protección del equipo

Puede ver la lista de problemas actuales, su descripción y sus soluciones posibles en la ficha **Estado** (figura siguiente) que se abre desde el vínculo **Reparar ahora** (figura anterior).

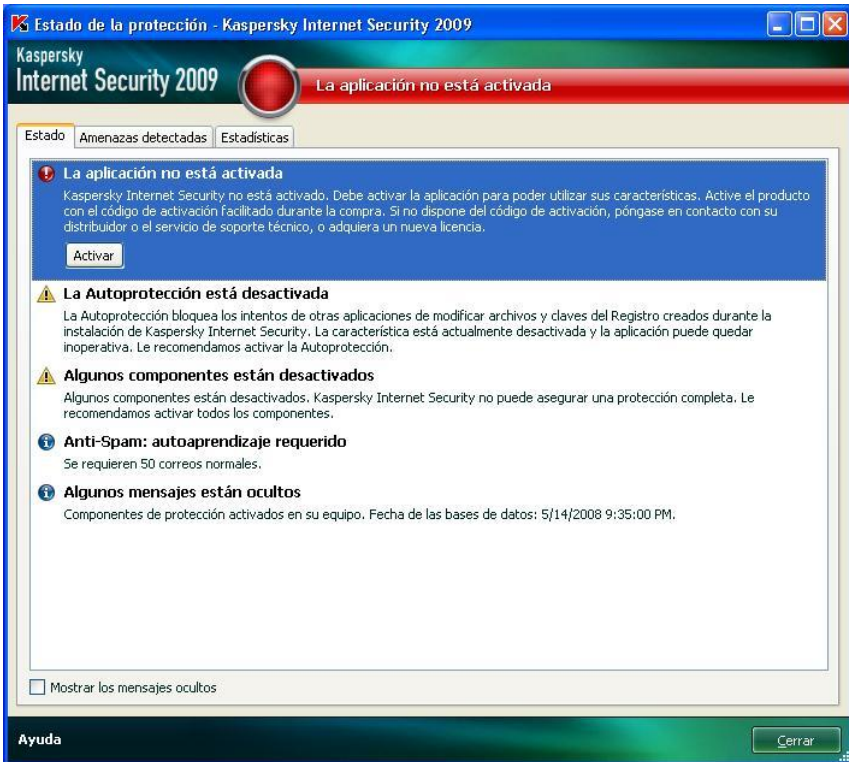


Figura 6: Solución de problemas de seguridad

La ficha muestra la lista de problemas existentes. Los problemas son presentados por orden de prioridad: aparecen en primer lugar los problemas más graves, con un icono rojo; siguen los problemas menos importantes con un icono amarillo y para terminar, los mensajes de información con un icono verde. Se proporciona una descripción detallada de cada problema y las siguientes acciones están disponibles:

- **Eliminar inmediatamente.** Con los botones correspondientes, puede corregir el problema aplicando la acción recomendada.
- **Posponer la eliminación.** Si por cualquier razón no puede eliminar la amenaza inmediatamente, puede posponer esta acción para más tarde. Para posponer la eliminación, haga clic en **Ocultar mensaje**.

Observe que esta opción no está disponible para problemas graves. Estos problemas incluyen, por ejemplo, objetos malintencionados que no fueron desinfectados, el bloqueo de alguno o de varios componentes o los daños en archivos de la aplicación.

Para volver a mostrar los mensajes ocultos en la lista general, active la casilla **Mostrar los mensajes ocultos**.

SUSPENSIÓN DE LA PROTECCIÓN

La suspensión de la protección implica desactivar temporalmente todos los componentes durante un cierto tiempo.

► *Para suspender la protección de su equipo:*

1. Seleccione la entrada **Suspender la protección** en el **menú contextual** (sección "Menú contextual" en la página 48).
2. En la ventana abierta **Suspender la protección**, seleccione el tiempo durante el cual desea suspender la protección:
 - **En <intervalo de tiempo>**: la protección se activará después de transcurrido el tiempo indicado. Utilice el menú desplegable para seleccionar el intervalo de tiempo.
 - **Después de reiniciar**: la protección se activará después de reiniciar el sistema, en el supuesto de que tenga activado el inicio de la aplicación junto con el equipo.
 - **Manualmente**: la protección sólo se activará si lo hace manualmente. Para activar la protección, seleccione Reanudar la protección en el menú contextual de la aplicación.

Como resultado de la desactivación temporal de la protección, todos los componentes de protección quedarán suspendidos. Esto queda indicado por:

- Los nombres deshabilitados (en gris) de los componentes desactivados en la entrada **Protección** de la ventana principal.
- Icono deshabilitado (en gris) de la aplicación (sección "Icono del área de notificaciones" en la página 47) en la barra de sistema.
- Color rojo del icono indicador de estado y del panel de la ventana principal de la aplicación.

Si se establecieron nuevas conexiones de red mientras la protección estaba suspendida, aparecerá una notificación informando de la interrupción de dichas conexiones


VALIDACIÓN DE LOS PARÁMETROS DE LA APLICACIÓN

Después de instalar y configurar la aplicación, para verificar que funciona correctamente puede utilizar un "virus" de prueba y sus variantes. Es necesario realizar una prueba separada para cada componente de protección o protocolo.

EN ESTA SECCIÓN:

Prueba con el "virus" EICAR y sus modificaciones	66
Prueba de protección en el tráfico HTTP	70
Prueba de protección en el tráfico SMTP	70
Validación de los parámetros del componente Antivirus de archivos y memoria	71
Validación de los parámetros de la tarea de análisis antivirus	72
Validación de los parámetros del componente Anti-Spam	72

PRUEBA CON EL "VIRUS" EICAR Y SUS MODIFICACIONES

Este "virus" ha sido especialmente diseñado por el organismo  (European Institute for Computer Anti) con el fin de realizar pruebas con productos antivirus.

El virus de prueba NO ES UN VIRUS porque no contiene código que pueda dañar su equipo. Sin embargo, la mayoría de los fabricantes de productos antivirus identifican este archivo como un virus.

Advertencia.

¡No utilice nunca un virus real para comprobar el funcionamiento de su antivirus!

Puede descargar el "virus" de prueba desde el sitio oficial del **EICAR** en la dirección: http://www.eicar.org/anti_virus_test_file.htm.

Nota

Antes de descargar el archivo, debe desactivar la protección antivirus ya que de otro modo la aplicación identificaría y procesaría el archivo *anti_virus_test_file.htm* como objeto infectado transmitido por el protocolo HTTP.

No olvide activar la protección antivirus en su equipo inmediatamente después de descargar el virus de prueba.

La aplicación identifica el archivo descargado del sitio **EICAR** como un objeto infectado que contiene un virus **que no se puede desinfectar** y ejecuta las acciones especificadas contra dicho objeto.

También puede utilizar variantes modificadas del "virus" de prueba estándar para comprobar el buen funcionamiento de la aplicación contra otros tipos de archivos. Una variante se consigue cambiando el contenido del "virus" estándar: para ello, agregue alguno de los prefijos siguientes (ver cuadro a continuación). Para crear variantes modificadas del "virus" de prueba, puede utilizar cualquier editor de texto simple o de hipertexto, por ejemplo **Bloc de notas Microsoft, UltraEdit32**, etc.

Advertencia.

Puede comprobar el funcionamiento correcto de la aplicación antivirus con el "virus" modificado EICAR tan sólo si la última actualización de su base antivirus es posterior al 24 de octubre de 2003, (actualizaciones acumuladas de octubre 2003).

La primera columna de la tabla siguiente contiene los prefijos que debe incluir delante de la cadena del virus de prueba estándar. La segunda columna enumera los posibles valores de estado que el antivirus atribuye al objeto, de acuerdo con los resultados del análisis. La tercera columna indica cómo la procesa los objetos con el estado especificado. Observe que las acciones realmente aplicadas a los objetos son determinados por los parámetros de la aplicación.

Después de agregar el prefijo al "virus" de prueba, guarde el archivo con un nombre nuevo, por ejemplo: *ecar_dele.com*. Atribuya nombres similares a todos los "virus" modificados.

Tabla 6. Modificaciones del "virus" de prueba"

Prefijo	Estado del objeto	Información de procesamiento del objeto
Sin prefijo, virus de prueba estándar	Infectado. Objeto infectado que contiene el código de un virus conocido. No se puede neutralizar.	La aplicación identifica el objeto como un virus que no se puede desinfectar. Ocurre un error al intentar desinfectar el objeto; se aplica la acción asociada para objetos no neutralizables.
CORR-	Dañado.	La aplicación tiene acceso al objeto pero no puede analizarlo, porque está dañado (la estructura del archivo está dañada o tiene un formato de archivo incorrecto, por ejemplo). Encontrará información acerca del procesamiento del objeto en el informe de actividad de la aplicación.
WARN-	Sospechoso. Objeto sospechoso que contiene código de un virus desconocido. No se puede neutralizar.	El analizador de código heurístico detecta el objeto como sospechoso. En el momento de la detección, las bases de aplicación no contienen una descripción que permita procesar este objeto. Recibirá una notificación cuando se detecte un objeto de este tipo.
SUSP-	Sospechoso. Objeto sospechoso que contiene código modificado de un virus conocido. No se puede neutralizar.	La aplicación ha detectado en una sección de código del objeto una correspondencia parcial con el código de otro virus conocido. En el momento de la detección, las bases de aplicación no contienen una descripción que permita procesar este objeto. Recibirá una notificación cuando se detecte un objeto de este tipo.

Prefijo	Estado del objeto	Información de procesamiento del objeto
ERRO-	Error de análisis.	Ocurrió un error mientras procesaba el objeto. La aplicación no consigue tener acceso al objeto: la integridad del objeto está dañada (por ejemplo, no se encuentra el final de un archivo multivolumen) o no es posible conectar con él (si el objeto analizado se encuentra en una unidad de red). Encontrará información acerca del procesamiento del objeto en el informe de actividad de la aplicación.
CURE-	Infectado. Objeto infectado que contiene el código de un virus conocido. Desinfectable.	El objeto contiene un virus que es posible neutralizar. La aplicación neutralizará el objeto; el contenido del cuerpo del "virus" será reemplazado por la palabra CURE. Recibirá una notificación cuando se detecte un objeto de este tipo.
DELE-	Infectado. Objeto infectado que contiene el código de un virus conocido. No se puede neutralizar.	La aplicación identifica el objeto como un virus que no se puede desinfectar. Ocurre un error al intentar desinfectar el objeto; se aplica la acción asociada para objetos no neutralizables. Recibirá una notificación cuando se detecte un objeto de este tipo.

PRUEBA DE PROTECCIÓN EN EL TRÁFICO HTTP

- ▶ *Para comprobar la detección de virus en flujos de datos transmitidos por protocolo HTTP, haga lo siguiente:*

Intente descargar un "virus" de prueba desde el sitio oficial de la organización EICAR en la dirección: http://www.eicar.org/anti_virus_test_file.htm.

Cuando el equipo intenta descargar el virus de prueba, Kaspersky Internet Security lo detecta e identifica como un objeto infectado que no se puede reparar, y aplica la acción especificada en los parámetros del tráfico HTTP para este tipo de objetos. De forma predeterminada, cuando intenta descargar el "virus" de prueba, la conexión con el sitio Web se interrumpe y el navegador muestra un mensaje informando al usuario que este objeto está infectado por el virus EICAR-Test-File.

PRUEBA DE PROTECCIÓN EN EL TRÁFICO SMTP

Para detectar virus dentro de flujos de datos transmitidos a través del protocolo SMTP, debe utilizar un sistema de correo compatible con este protocolo para transmitir datos.

Nota

Le recomendamos comprobar cómo Kaspersky Internet Security controla los mensajes de correo entrantes y salientes, incluyendo el cuerpo de los mensajes y los adjuntos. Para probar la detección de virus en el cuerpo de los mensajes, copie el texto del "virus" de prueba estándar o modificado dentro del cuerpo de un mensaje.

- ▶ *Para probar la detección de virus en los flujos de datos SMTP:*

1. Cree un mensaje en formato de **texto plano** con un cliente de correo ya instalado en su equipo.

Nota

El mensaje que contiene el virus de prueba no será analizado si lo crea en formato RTF o HTML.

2. Copie el texto de un "virus" de prueba estándar o modificado al principio del mensaje o adjunte un archivo que contenga el "virus" de prueba.
3. Envíe el mensaje al administrador.

La aplicación detecta el objeto, lo identifica como infectado y bloquea el mensaje.

VALIDACIÓN DE LOS PARÁMETROS DEL COMPONENTE ANTIVIRUS DE ARCHIVOS Y MEMORIA

► *Para comprobar que la configuración del componente Antivirus de archivos y memoria es correcta:*

1. Cree una carpeta en disco, copie en ella el virus de prueba EICAR descargado, así como las modificaciones que haya creado.
2. Active el registro de todos los eventos para que el archivo de informe muestre información acerca de los objetos dañados o no analizados por causa de errores.
3. Ejecute el "virus" de prueba o alguna versión modificada.

El componente Antivirus de archivos y memoria interceptará la petición de ejecución del archivo, analizará éste último y aplicará la acción especificada en los parámetros para objetos con este estado. Si selecciona varias acciones para aplicarlas al objeto detectado, podrá realizar una comprobación completa del funcionamiento del componente.

Puede examinar los resultados de la actuación del componente Antivirus de archivos y memoria en el informe correspondiente.

VALIDACIÓN DE LOS PARÁMETROS DE LA TAREA DE ANÁLISIS ANTIVIRUS

- ▶ *Para comprobar que la configuración de la tarea de análisis antivirus es correcta:*
 1. Cree una carpeta en disco, copie en ella el virus de prueba EICAR descargado, así como las modificaciones que haya creado.
 2. Cree una nueva tarea de análisis antivirus y seleccione la carpeta con el conjunto de "virus" de prueba como objetivo del análisis.
 3. Active el registro de todos los eventos para que el archivo de informe muestre información acerca de todos los objetos dañados o no analizados por causa de errores.
 4. Ejecute la tarea de análisis antivirus.

Cuando ejecuta la tarea de análisis, las acciones especificadas en los parámetros de tarea se aplican a los objetos sospechosos o infectados detectados. Si selecciona varias acciones para aplicarlas a los objetos detectados, podrá realizar una comprobación completa del funcionamiento del componente.

Puede examinar todos los resultados relativos a la actuación de la tarea en el informe de actividad del componente.

VALIDACIÓN DE LOS PARÁMETROS DEL COMPONENTE ANTI-SPAM

Utilice un mensaje de prueba identificado como SPAM para poner a prueba la protección antispam.

El cuerpo del mensaje de prueba debe incluir la línea siguiente:

```
Spam is bad do not send it (El spam es malo no lo envíes)
```

Después de recibir este mensaje en el equipo, la aplicación lo analiza, le atribuye el estado de correo no deseado ("spam") y aplica la acción especificada para objetos de este tipo.

DECLARACIÓN DE RECOLECCIÓN DE DATOS DE KASPERSKY SECURITY NETWORK

INTRODUCCIÓN

LEA CON ATENCIÓN ESTE DOCUMENTO. CONTIENE INFORMACIÓN IMPORTANTE QUE DEBE CONOCER ANTES DE SEGUIR UTILIZANDO NUESTROS SERVICIOS O NUESTRO SOFTWARE. AL SEGUIR UTILIZANDO EL SOFTWARE Y LOS SERVICIOS DE KASPERSKY LAB, SIGNIFICA QUE ACEPTA LA PRESENTE DECLARACIÓN DE RECOLECCIÓN DE DATOS DE KASPERSKY LAB. Nos reservamos el derecho de modificar esta Declaración de recolección de datos en todo momento, previa publicación de las modificaciones en esta misma página. Compruebe la fecha de revisión a continuación para determinar si este acuerdo ha sido modificado desde la última vez que lo leyó. La utilización continuada de cualquiera de los Servicios de Kaspersky Lab después de la publicación de modificaciones a la Declaración de recolección de datos significa su aceptación de estas modificaciones.

Kaspersky Lab y sus filiales (colectivamente "**Kaspersky Lab**") ha redactado esta Declaración de recolección de datos con el fin de informar y dar a conocer su política de recuperación e intercambio de datos para Kaspersky Anti-Virus y Kaspersky Internet Security.

Acerca de Kaspersky Lab

Kaspersky Lab tiene el fuerte compromiso de ofrecer servicios de calidad a todos sus clientes y en particular, en relación con la recolección de datos. Comprendemos sus posibles interrogantes acerca del modo de recolección y utilización de la información y datos por parte de Kaspersky Security Network, por lo que hemos preparado este reglamento para informarle acerca de los principios de recolección de datos que regulan Kaspersky Security Network ("**Declaración de recolección de datos**" o "**Declaración**").

Esta Declaración de recolección de datos contiene numerosos detalles de orden general y técnico acerca de las medidas tomadas para responder a sus preocupaciones acerca de la recolección de sus datos. La presentación de esta Declaración está organizada por tipo de tratamiento y cobertura, con el fin de que pueda encontrar rápidamente la información que más le interese. La satisfacción de sus necesidades y expectativas es la línea directriz de nuestra

actuación y el fundamento de cuanto hacemos, incluyendo la protección de sus datos recolectados.

Los datos y la información son recolectados por Kaspersky Lab, por tanto, si después de leer esta Declaración de recolección de datos tiene preguntas o le quedan dudas, envíe un correo electrónico a la dirección support@kaspersky.com.

¿Qué es Kaspersky Security Network?

El servicio Kaspersky Security Network permite a cualquier usuario de productos de seguridad de Kaspersky Lab en todo el mundo contribuir a identificar y reducir el tiempo necesario para asegurar su protección contra los nuevos riesgos de seguridad (incontrolados) que asedian su equipo. Para poder identificar las amenazas nuevas y su origen, para contribuir a mejorar la seguridad de los usuarios y las prestaciones de sus productos, Kaspersky Security Network recolecta una selección de datos sobre la seguridad y las aplicaciones, relativos a riesgos potenciales que amenazan su equipo, y transfiere estos datos a Kaspersky Lab para su análisis. **Esta información no contiene ningún dato personal que permita identificar al usuario y Kaspersky Lab la utiliza únicamente para mejorar la seguridad de sus productos y desarrollar soluciones contra amenazas y virus malintencionados. En caso de transmisión accidental de cualquier dato personal del usuario, Kaspersky Lab lo mantendrá protegido de acuerdo con esta Declaración de recolección de datos.**

Al aceptar participar en Kaspersky Security Network, Usted y los demás usuarios de productos de seguridad Kaspersky Lab en todo el mundo contribuyen de forma significativa a convertir Internet en un entorno más seguro.

Cuestiones legales

Kaspersky Security Network está sometido a las leyes de múltiples jurisdicciones, porque sus servicios pueden ser utilizados en cualquiera de ellas, en particular en los Estados Unidos de América. Kaspersky Lab podrá comunicar su información personal sin su consentimiento cuando así lo exija la ley o en el convencimiento razonable de que dicha actuación es necesaria para la investigación de actividades peligrosas o protección de huéspedes, visitantes, colaboradores, propiedades de Kaspersky Lab, u otros. Como mencionado anteriormente, las leyes relativas a la protección de los datos recolectados por Kaspersky Security Network pueden variar según los países. Por ejemplo, en la Unión Europea y sus Estados miembros, la recolección de determinados datos personales identificables están sometidos a Directivas Europeas relativas a tratamiento de datos personales, privacidad y comunicaciones electrónicas. En particular, la Directiva 2002/58/CE del 12 de julio de 2002 del Parlamento y Consejo Europeos, relativa al tratamiento de datos personales y protección de la privacidad en el sector de las comunicaciones; la Directiva 95/46/CE del 24 de octubre 1995 del Parlamento y Consejo Europeos, relativa a la protección de las personas frente al tratamiento y libre comunicación de datos personales, con las consiguientes Leyes adoptadas por los Estados miembros de la UE; la Decisión 497/2001/CE de la Comisión Europea sobre cláusulas contractuales (datos

personales transferidos a terceros países), con las consiguientes Leyes adoptadas por los Estados miembros de la UE.

Kaspersky Security Network informará debidamente a los usuarios antes de iniciar cualquier recolección y tratamiento compartido de datos antes mencionados, en especial con fines de desarrollo comercial. Asimismo ofrecerá a estos usuarios de Internet la correspondiente **opción de entrada** (en los Estados miembros de la UE y en otros países que exigen un procedimiento previo de aceptación "opt-in") u opción de salida (procedimiento de "opt-out" practicado en otros países), disponible en línea, contra cualquier uso o comunicación de estos datos a terceras partes, con fines comerciales.

Kaspersky Lab puede ser requerido por Ley o por autoridades judiciales para aportar información de identificación personal a las autoridades gubernamentales pertinentes. En caso de requerimiento legal o judicial, aportaremos esta información tras recibir la documentación apropiada. Kaspersky Lab también puede aportar información para asegurarse legalmente de la protección de su propiedad así como de la salud y protección de los particulares, de acuerdo con la ley.

Se depositarán declaraciones de registro de datos personales ante las Agencias de protección de datos de los Estados miembros, de acuerdo con la legislación vigente de cada Estado miembro de la UE. Información sobre dichas declaraciones estará disponible en los servicios de Kaspersky Security Network.

INFORMACION RECOLECTADA

Datos recolectados

El servicio Kaspersky Security Network recolecta y transmite información básica y ampliada a Kaspersky Lab relacionada con los riesgos potenciales de seguridad que asedian su equipo. Los datos recolectados incluyen:

Datos básicos

- Información del hardware y software de su equipo, incluyendo: sistema operativo; actualizaciones instaladas; objetos del núcleo; controladores; extensiones para Internet Explorer, servicios impresión y el Explorador de Windows; archivos de programa descargados; archivos de instalación activa; subprogramas del panel de control; entradas Host y Registro; direcciones IP; tipos de navegadores; clientes de correo así como número de versión del producto Kaspersky Lab, que normalmente no permite la identificación personal;
- Identificador exclusivo generado por el producto Kaspersky Lab para identificar equipos individuales sin identificar al usuario y que no contiene ningún dato de carácter personal;
- Información de estado sobre la protección antivirus de su equipo, así como datos sobre cualquier archivo o actividad sospechosa de ser un

programa malintencionado (nombre de archivo, fecha y hora de la detección, nombres, rutas y tamaños de los archivos infectados, direcciones IP y puertos de ataques de red, nombre de la aplicación sospechosa de ser malintencionada). Observe que los datos recolectados antes enumerados no contienen ninguna información que permita la identificación personal.

Datos ampliados

- Información de aplicaciones firmadas descargadas por el usuario (dirección URL, tamaño del archivo, nombre del firmante)
- Información de aplicaciones ejecutables (tamaño, atributos, fecha de creación, información de encabezados PE, región, nombre, ubicación y herramienta de compresión utilizada).

Seguridad en transferencias y almacenamiento de datos

Kaspersky Lab está comprometido con la seguridad de la información recolectada. La información recolectada se almacena en equipos servidores de acceso limitado y restringido. Kaspersky Lab opera en redes de datos protegidas por cortafuegos de calidad industrial y sistemas de protección con contraseña. Kaspersky Lab utiliza una amplia gama de tecnologías y procedimientos de seguridad con el fin de proteger la información recolectada contra amenazas no autorizadas, tales como operaciones de acceso, utilización o divulgación de datos. Nuestras directivas de seguridad son revisadas de forma periódica, ampliadas en caso necesario, y tan sólo personas autorizadas tienen acceso a los datos recolectados. Kaspersky Lab toma todas las medidas para asegurar un tratamiento seguro de su información, de acuerdo con esta Declaración. Desgraciadamente, no es posible garantizar la seguridad de las transmisiones de datos. Por ello, aunque nos esforcemos en proteger sus datos, no podemos garantizar la seguridad de todos los datos transmitidos, ni de nuestros productos o servicios, sin excluir el propio servicio Kaspersky Security Network: todos estos servicios se proporcionan por su cuenta y riesgo.

Los datos recolectados pueden ser transferidos a los servidores de Kaspersky Lab, donde hemos tomado las precauciones necesarias para asegurarnos que esta información, en caso de ser transferida, recibirá un nivel de protección adecuado. Los datos recolectados son considerados información confidencial, es decir, son procesados de acuerdo y en conformidad con los procedimientos de seguridad y las directivas aplicables a la protección y utilización de información confidencial en vigor en nuestra organización. Tras su recepción en Kaspersky Lab, los datos recolectados son almacenados en un servidor con características de seguridad físicas y electrónicas habituales en la industria, incluyendo la utilización de procedimientos de autenticación por usuario y contraseña así como cortafuegos electrónicos diseñados para bloquear cualquier acceso no autorizado desde el exterior de Kaspersky Lab. Los datos recolectados por Kaspersky Security Network cubiertos por esta Declaración son procesados y almacenados en los Estados Unidos y pueden serlo también en

otras jurisdicciones donde Kaspersky Lab ejerce su actividad. Todo el personal de Kaspersky Lab está capacitado al uso de nuestras directivas de seguridad. El acceso a sus datos sólo está disponible para aquellos empleados que lo necesiten para realizar sus tareas. Ningún dato almacenado estará asociado con ninguna información personal que permita la identificación personal. Kaspersky Lab no combina los datos almacenados en Kaspersky Security Network con ningún otro dato, lista de contactos o información de suscripción registrada por Kaspersky Lab con fines promocional u otros.

UTILIZACIÓN DE LOS DATOS RECOLECTADOS

Cómo se utiliza su información personal

Kaspersky Lab recolecta datos con el fin de analizar e identificar el origen de riesgos potenciales de seguridad, así como mejorar la capacidad de los productos Kaspersky Lab para detectar comportamientos malintencionados, sitios Web fraudulentos, software criminal u otros tipos de amenazas de seguridad Internet, asegurando de este modo el mayor nivel de protección posible en el futuro para los clientes de Kaspersky Lab.

Comunicación de información a terceras partes

Kaspersky Lab podrá comunicar cualquier información recolectada en caso de requerimiento oficial previsto o autorizado por ley, en respuesta a una citación o cualquier otro procedimiento legal, o en la convicción razonable de estar obligado a ello para respetar una ley, reglamento o citación aplicable, o cualquier procedimiento o requerimiento gubernamental con fuerza de obligar. Kaspersky Lab podrá también divulgar datos de identificación personal cuando existan razones para creer que su divulgación es necesaria para identificar, contactar o emprender acciones legales contra alguien que intente violar esta Declaración, alguna cláusula de Acuerdo con nuestra Empresa, las protecciones de seguridad de nuestros usuarios y del público, o los acuerdos de confidencialidad y licencia con aquellas terceras partes que contribuyen al desarrollo, funcionamiento y mantenimiento de Kaspersky Security Network. Para facilitar la anticipación, detección y prevención de riesgos de seguridad en Internet, Kaspersky Lab podrá compartir determinada información con organismos de investigación y otros fabricantes de software de seguridad. Kaspersky Lab también podrá también elaborar estadísticas a partir de la información recolectada, con el fin de seguir la evolución y publicar informes sobre las tendencias en los riesgos de seguridad.

Opciones disponibles a su elección

La participación en Kaspersky Security Network es optativa. Puede activar y desactivar el servicio Kaspersky Security Network en cualquier momento: para ello, abra la entrada Comentarios en la página de configuración de su producto Kaspersky Lab. Observe, sin embargo, que si opta por reservarse la información o los datos solicitados, no podremos asegurarle algunos de los servicios que dependen de la recolección de estos datos.

Al terminar el plazo de funcionamiento de su producto Kaspersky Lab, algunas de las funciones del software Kaspersky Lab podrán seguir funcionando, pero la información no seguirá siendo transmitida automáticamente a Kaspersky Lab.

Nos reservamos también el derecho de enviar a los usuarios mensajes de alerta, poco frecuentes, para informarles de cambios específicos que pueden afectar su capacidad de uso de servicios a los que se han suscrito con anterioridad. Nos reservamos también el derecho de ponernos en contacto con Usted cuando nos obligue a ello un procedimiento legal, o ante la violación de cualquier acuerdo de licencia, garantía o compra aplicable.

Kaspersky Lab se reserva estos derechos porque pensamos que puede ser necesario, en determinados casos, disponer del derecho de entrar en contacto con Usted por motivos legales o razones importantes para Usted. Estos derechos no nos autorizan a ponernos en contacto con Usted con ofertas comerciales de servicios nuevos o existentes, si no ha optado por recibirlas, y en cualquier caso este tipo de comunicaciones es infrecuente.

CONSULTAS Y QUEJAS RELACIONADAS CON LA RECOLECCIÓN DE DATOS

En Kaspersky Lab, admitimos y tratamos las consultas los usuarios acerca de la Recolección de datos con el mayor respeto y la mayor atención. Si piensa que existe cualquier tipo de incumplimiento de esta Declaración en relación con su información o sus datos, o para cualquier otra consulta o duda relacionada, puede escribir o ponerse en contacto con Kaspersky Lab en la dirección electrónica: support@kaspersky.com.

En su mensaje, describa con el mayor detalle posible la naturaleza de su consulta. Su consulta o queja será estudiada con la mayor brevedad.

El envío de información es voluntario. El usuario puede desactivar la opción de recolección de datos en cualquier momento, desde la entrada "**Comentarios**" de la página "**Configuración**" de todos los productos Kaspersky correspondientes.

Copyright © 2008 Kaspersky Lab. Reservados todos los derechos.

KASPERSKY LAB

Fundado en 1997, Kaspersky Lab se ha convertido en un líder reconocido en tecnologías de seguridad de la información. Es fabricante de un amplio conjunto de productos software de seguridad y protección de datos: antivirus, antisпам y sistemas antifracción.

Kaspersky Lab es una organización internacional. Con sede en la Federación Rusa, la organización cuenta con delegaciones en Alemania, países del Benelux, China, Estados Unidos (California), Francia, Polonia, Reino Unido, Rumania y Japón. Un nuevo departamento de la organización, el Centro europeo de investigación antivirus, ha sido recientemente instalado en Francia. La red de colaboradores de Kaspersky Lab incluye más de 500 organizaciones en todo el mundo.

Actualmente, Kaspersky Lab emplea más de 450 especialistas altamente cualificados, con 10 titulares de MBA y 16 titulares de Doctorado. Numerosos expertos antivirus de Kaspersky Lab son miembros de la CARO (Computer Antivirus Internet Researchers Organization).

Nuestros más preciados valores empresariales son los conocimientos y la experiencia acumulados por nuestros especialistas durante cuarenta años de lucha incesante contra los virus informáticos. Mediante un análisis en profundidad del comportamiento de los virus informáticos, nuestros especialistas son capaces de anticipar las tendencias del código malintencionado y proporcionar a tiempo a nuestros usuarios la protección contra nuevos tipos de ataques. La resistencia a ataques futuros es la directiva básica de todos los productos Kaspersky Lab. Constantemente, nuestros productos superan los de muchos otros proveedores a la hora de asegurar una cobertura antivirus.

Años de duro trabajo nos han convertido en uno de los fabricantes líder de software de seguridad. Kaspersky Lab fue una de las primeras empresas de este tipo en desarrollar los estándares contemporáneos para la defensa antivirus. Nuestro producto estrella, Kaspersky Anti-Virus, ofrece protección integral para todos los niveles jerárquicos de una red: estaciones de trabajo, servidores de archivos, sistemas de correo, cortafuegos y pasarelas Internet, así como equipos portátiles. Sus herramientas de administración adaptadas y sencillas ofrecen el máximo grado de automatización para la protección antivirus de los equipos y redes empresariales. Numerosos fabricantes conocidos utilizan el núcleo de Kaspersky Anti-Virus: Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israel), Sybaris (EEUU), G Data (Alemania), Deerfield (EEUU), Alt-N (EEUU), Microworld (India) y BorderWare (Canadá).

Los clientes de Kaspersky Lab se benefician de una amplia oferta de servicios avanzados que les garantiza un funcionamiento estable de nuestros productos y una compatibilidad total con sus necesidades específicas de negocio. Diseñamos, instalamos y mantenemos avanzados productos antivirus corporativos. La base antivirus de Kaspersky Lab se actualiza cada hora.

Nuestra organización ofrece a sus usuarios un servicio de asistencia técnica de 24 horas, disponible en numerosos idiomas.

Para cualquier pregunta, póngase en contacto con nuestros distribuidores o con Kaspersky Lab directamente. Consultas de detalle se facilitan por teléfono o correo electrónico. Recibirá respuestas completas y detalladas a cualquier consulta.

Dirección:	Russia, 123060, Moscow, 1-st Volokolamsky Proezd, 10, Building 1
Teléfono, Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Servicio de urgencia 24/7:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Servicio a usuarios empresariales:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (de 10 a 7 de la tarde) http://support.kaspersky.com/helpdesk.html
Servicio a usuarios corporativos:	La información de contacto se facilita después de adquirir un producto software para empresa, en función del modelo de asistencia elegido.
Foro Web de Kaspersky Lab:	http://forum.kaspersky.com
Laboratorio antivirus:	newvirus@kaspersky.com (sólo para envío de nuevos virus en archivos comprimidos)
Equipo de documentación:	docfeedback@kaspersky.com (sólo para comentarios sobre la documentación y el sistema de ayuda)
Departamento comercial:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Información general:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.com http://www.viruslist.com

CRYPTOEX LLC

Para la creación y comprobación de firmas digitales, Kaspersky Internet Security utiliza la biblioteca Crypto C de software de seguridad para datos, desarrollada por Crypto Ex LLC.

Crypto Ex posee una licencia de la Agencia Federal Estadounidense para el servicio de Comunicaciones e Información del Gobierno (un departamento del FSB - Servicio Federal de Seguridad) para desarrollar, fabricar y distribuir software para cifrado de datos que no constituyan secretos de Estado.

La biblioteca Crypto C está diseñada para proteger información confidencial de clase K1 y goza del certificado de conformidad de la FSB N° SF/114-0901 del 1 de julio 2006.

La biblioteca es capaz de cifrar y descifrar paquetes de tamaño fijo o flujos de datos mediante las tecnologías siguientes:

- algoritmo de cifrado (GOST 28147-89);
- algoritmos para la generación y comprobación de firmas digitales (GOST R 34.10-94 y GOST 34.10-2001);
- funciones hash (GOST 34.11-94);
- generación de claves mediante un programa transmisor de números pseudoaleatorios,
- un sistema generador de claves y vectores de simulación (GOST 28147-89).

Los módulos de la biblioteca están implementados en lenguaje ANSI C estándar y su código puede integrarse en aplicaciones de forma estática o cargarse de forma dinámica. Pueden ejecutarse en plataformas x86, x86-64, Ultra SPARC II y otras plataformas compatibles.

Es posible migrar los módulos de la biblioteca a los siguientes entornos operativos: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris para Ultra SPARC II).

Para obtener más información, visite el sitio Web corporativo de CryptoEx LLC en la dirección <http://www.cryptoex.ru> póngase en contacto con dicha organización por correo electrónico en la dirección info@cryptoex.ru

MOZILLA FOUNDATION

La biblioteca **Gecko SDK ver. 1.8** ha servido para el desarrollo de los componente de esta aplicación.

La utilización de este software está sujeta a los términos y condiciones de la licencia MPL 1.1 de Public Mozilla Foundation <http://www.mozilla.org/MPL>.

Para obtener más detalles acerca de la biblioteca Gecko SDK consulte: http://developer.mozilla.org/en/docs/Gecko_SDK.

© Mozilla Foundation

Sitio Web de Mozilla Foundation: <http://www.mozilla.org>.

CONTRATO DE LICENCIA

Contrato estándar de licencia de usuario final

NOTA PARA TODOS LOS USUARIOS: LEA ATENTAMENTE EL SIGUIENTE CONTRATO DE LICENCIA ("CONTRATO") PARA KASPERSKY INTERNET SECURITY ("SOFTWARE") FABRICADO POR KASPERSKY LAB ("KASPERSKY LAB").

SI HA ADQUIRIDO ESTE SOFTWARE POR INTERNET HACIENDO CLIC SOBRE EL BOTÓN ACEPTAR, USTED ("PARTICULAR O ENTIDAD") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. SI NO ACEPTA TODOS LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO, HAGA CLIC EN EL BOTÓN QUE INDICA QUE NO LOS ACEPTA Y NO INSTALE EL SOFTWARE.

SI HA COMPRADO ESTE SOFTWARE EN UN MEDIO FÍSICO, Y HA ROTO EL ESTUCHE DEL CD, USTED ("PARTICULAR O ENTIDAD") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. SI NO ACEPTA TODOS LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO NO ABRA EL ESTUCHE DEL CD NI DESCARGUE, INSTALE O UTILICE ESTE SOFTWARE.

DE ACUERDO CON LA LEGISLACION VIGENTE APLICABLE AL SOFTWARE KASPERSKY DESTINADO A CONSUMIDORES PARTICULARES Y ADQUIRIDO EN LINEA EN EL SITIO INTERNET DE KASPERSKY LAB O SUS DISTRIBUIDORES, LOS COMPRADORES DISPONDRAN DE CATORCE (14) DÍAS HÁBILES A CONTAR DE LA ENTREGA DEL PRODUCTO PARA DEVOLVERLO AL ESTABLECIMIENTO VENDEDOR, CAMBIARLO O RECUPERAR EL DINERO, SIEMPRE QUE EL SOFTWARE NO HAYA SIDO ABIERTO.

EL SOFTWARE KASPERSKY DIRIGIDO A CONSUMIDORES PARTICULARES QUE NO HA SIDO ADQUIRIDO POR INTERNET NO PODRÁ SER DEVUELTO NI CAMBIADO, SALVO CLAUSULAS CONTRARIAS DEL DISTRIBUIDOR QUE VENDIÓ EL PRODUCTO. EN ESTE CASO, KASPERSKY LAB NO SE HARÁ RESPONSABLE DE LAS CONDICIONES DE DICHO DISTRIBUIDOR.

EL DERECHO A DEVOLUCIÓN Y REINTEGRO SÓLO SE EXTIENDE AL COMPRADOR ORIGINAL.

De aquí en adelante en todas las referencias al "Software" se considerará que éste incluye el código de activación de software proporcionado por Kaspersky Lab como parte de Kaspersky Internet Security.

1. *Contrato de licencia.* Si los gastos de licencia han sido pagados, y de acuerdo con los términos y condiciones de este Contrato, Kaspersky Lab le concede por el presente Contrato un derecho de uso no exclusivo y no transferible de una copia de la versión especificada del Software y de la documentación que lo acompaña ("Documentación") únicamente para sus propios fines de negocio. Puede instalar una sola copia del Software en un sólo equipo.

1.1 *Uso*. Si el Software fue adquirido en un soporte físico, tiene el derecho de utilizar el Software para la protección de tantos equipos como se mencione en el paquete. Si el Software fue adquirido por Internet, tiene el derecho de utilizar el Software para la protección de tantos equipos como ordenó al adquirir el Software.

1.1.1 El Software está "en uso" en un equipo cuando está cargado en la memoria temporal (es decir, memoria de acceso-aleatorio o RAM) o instalado en la memoria permanente (es decir, el disco duro, un CDROM u otro dispositivo de almacenamiento) del equipo. Esta licencia sólo le autoriza a reproducir las copias adicionales del Software que sean necesarias para su uso legítimo, y sólo para producir copias de seguridad, a condición de que todas las copias contengan toda la información de propiedad del Software. Deberá mantener un registro con el número y ubicación de todas las copias del Software y Documentación y tomará las precauciones razonables para impedir que el Software sea copiado o utilizado sin autorización.

1.1.2 El software protege el equipo contra virus y ataques de red cuyas firmas aparezcan en la base de la aplicación y de ataques de red disponible en los servidores de actualización de Kaspersky Lab.

1.1.3 En caso de que venda el equipo donde tiene instalado el software, tomará medidas previas para asegurarse de que todas las copias del Software han sido borradas.

1.1.4 No deberá descompilar, hacer ingeniería inversa, descodificar o restituir de ningún modo parte de este Software a una forma humanamente legible, ni facilitar a terceras partes que lo hagan. La información de interfaz necesaria para asegurar la interoperabilidad del Software con programas independientes será suministrada por Kaspersky Lab a petición, previo pago de los costes y gastos razonables ocasionados por el suministro de esta información. En caso de que Kaspersky Lab le informe de que no tiene intención de poner a su disposición esta información por cualquier, incluidos (sin limitación) razones de costos, estará autorizado a dar los pasos necesarios para lograr la interoperabilidad a condición de que usted sólo utilice ingeniería inversa o descompilación dentro de los límites permitidos por la ley.

1.1.5 No le está permitido a Usted, ni a terceras partes, corregir errores ni, en general, modificar, adaptar, traducir ni crear productos derivados de este Software, ni permitir a un tercero hacer copias de él (salvo que lo autorice expresamente este contrato).

1.1.6 No debe arrendar o prestar el Software a ninguna otra persona, ni transferir o sublicenciar sus derechos de licencia a ninguna otra persona.

1.1.7 No le está permitido facilitar a terceros el código de activación o el archivo llave de licencia, ni facilitar a terceros el acceso al código de activación o a la llave de licencia. El código de activación y la llave de licencia son datos confidenciales.

1.1.8 Kaspersky Lab podrá pedirle al Usuario que instale la última versión del Software (última versión y último paquete de mantenimiento).

1.1.9 No podrá utilizar este Software en herramientas automáticas, semiautomáticas o manuales diseñadas para crear firmas de identificación de virus, rutinas de detección de virus, ni cualquier otra información o código para la detección de código o de datos malintencionados.

1.1.10 Kaspersky Lab, con su consentimiento explícito confirmado en la correspondiente Declaración, tiene el derecho de recolectar información sobre amenazas y vulnerabilidades potenciales en su equipo. La información recopilada, en formato genérico, se utiliza únicamente para mejorar los productos Kaspersky Lab.

2. Support¹.

(i) Kaspersky Lab le proporcionará servicios de soporte ("Servicios de soporte") para el periodo definido a continuación, especificado en el Archivo llave de licencia (periodo de servicio) y en la ventana "Servicio", a partir de la fecha de activación, en los siguientes supuestos:

- (a) Pago de la cuota vigente de soporte, y:
- (b) Cumplimentación satisfactoria del Formulario de suscripción a los Servicios de Soporte que acompaña este Contrato o disponible en el sitio Internet de Kaspersky Lab, lo que requiere introducir el código de activación también proporcionado por Kaspersky Lab junto con este Contrato. Si usted ha satisfecho esta condición o no para el suministro de Servicios de soporte estará a la discreción absoluta de los servicios de soporte.

El servicio de soporte estará disponible después de la activación del Software. El Servicio de soporte técnico de Kaspersky Lab está también habilitado para solicitarle a Usted datos de registro adicionales con el fin identificarle como usuario con derecho a asistencia.

Hasta la activación del Software, o la obtención del identificador de Usuario final (Id. de cliente), el soporte técnico tan sólo facilita ayuda para la activación del software y el registro del Usuario final.

(ii) Los Servicios de soporte terminarán si no los renueva anualmente pagando la cuota de Soporte anual y volviendo a rellenar el formulario de suscripción a los Servicios de soporte.

¹ El uso de la versión de demostración del Software no le da acceso al Soporte técnico descrito en la cláusula 2 de este CLUF, ni le autoriza a vender a terceros la copia en su posesión.

Le está permitido utilizar el Software con fines de demostración durante el periodo especificado en el archivo llave de licencia, a contar del momento de la activación (puede consultar dicho periodo en la ventana Servicio de la interfaz del programa).

- (iii) "Servicio de soporte" significa:
 - (a) Actualizaciones regulares de la base antivirus;
 - (b) Actualizaciones de la base contra ataques de red;
 - (c) Actualizaciones de la base antisпам;
 - (d) Actualizaciones gratuitas del software, incluidas actualizaciones de la versión de antivirus;
 - (e) Soporte técnico por Internet y línea telefónica directa facilitados por el proveedor o distribuidor;
 - (f) Detección de virus y actualizaciones para su desinfección en un plazo de 24 horas.
- (iv) El Servicio de soporte se proporciona sólo cuando la última versión del software (incluyendo los paquetes de mantenimiento), disponible en el sitio Internet oficial de Kaspersky Lab (www.kaspersky.com), esté instalada en su equipo.

3. *Derechos de propiedad.* El Software está protegido por las leyes de derechos de autor. Kaspersky Lab y sus proveedores se reservan y retienen todos los derechos, titularidad e intereses de y sobre el Software, incluyendo todos los derechos de autor, patentes, marcas registradas y otros derechos de propiedad intelectual. Su posesión, instalación o uso del Software no le transfiere ningún título de propiedad intelectual sobre el Software: usted no adquiere ningún otro derecho sobre el Software salvo especificado en este Contrato.

4. *Confidencialidad.* Usted acepta que el Software y la Documentación, incluidos el diseño y estructura de los programas individuales, constituyen información confidencial y propietaria de Kaspersky Lab. No debe desvelar, proporcionar u ofrecer la información confidencial en cualquiera de sus formas a terceras partes sin autorización escrita de Kaspersky Lab. Deberá tomar las medidas de seguridad necesarias para proteger esta información confidencial y, sin que esto suponga una restricción a lo anterior, proteger lo mejor posible el código de activación.

5. *Garantía limitada.*

- (i) Kaspersky Lab le garantiza que durante seis (6) meses desde la primera descarga o instalación del Software adquirido en un soporte físico, su funcionamiento responderá esencialmente a lo descrito por la Documentación, si se ejecuta de forma apropiada y de la manera especificada en la Documentación.
- (ii) Al seleccionar este software, usted acepta toda la responsabilidad derivada de la satisfacción de sus necesidades. Kaspersky Lab no garantiza que el Software y/o la Documentación son adecuados para sus necesidades, funcionarán de forma ininterrumpida ni que estén libres de errores.

- (iii) Kaspersky Lab no garantiza que este Software identifique todos los virus ni todos los correos indeseados, ni que el Software no detecte erróneamente en ocasiones un virus en un archivo no infectado por ese virus.
- (iv) Su único recurso y la entera responsabilidad de Kaspersky Lab por la ruptura de la garantía mencionada en el párrafo (i) será, según la decisión de Kaspersky Lab, la reparación, el reemplazo o el reembolso del Software si ha informado de esto a Kaspersky Lab o sus proveedores durante el período de la garantía. Debe proporcionar toda la información que pueda ser necesaria para ayudar al Proveedor a determinar el elemento defectuoso.
- (v) La garantía mencionada en el párrafo (i) no se aplicará si usted (a) realiza o causa cualquier modificación a este Software sin autorización de Kaspersky Lab, (b) utiliza el Software de una manera no prevista o (c) no permitida por este Contrato.
- (vi) Las garantías y condiciones especificadas en este Contrato sustituyen todas las otras condiciones, garantías u otros términos acerca de las prestaciones o prestación prevista, ausencia o tardanza en las prestaciones del Software o la Documentación que puedan tener efecto entre Kaspersky Lab y usted, excepto en los casos especificados en este párrafo (vi), o estuvieren implícitas o incorporadas a este Contrato o cualquier contrato colateral, por normativa legal, derecho común o cualquier otra razón, que quedan todas excluidas (incluidas, sin limitación alguna, condiciones implícitas, garantías u otros criterios cualitativos relativos a la satisfacción, conveniencia o competencia y cuidado necesarios).

6. Limitación de responsabilidad.

- (i) Nada en este Contrato excluirá o limitará la responsabilidad de Kaspersky Lab por (a) acto delictuoso de engaño, (b) muerte o daños personales debidos al incumplimiento de obligaciones relativas a la salud o por violación negligente de este Contrato o (c) cualquier responsabilidad que no quede excluida por ley.
- (ii) De acuerdo con el párrafo (i) anterior, el Proveedor no será responsable (por contrato, daño, restitución o cualquier otra forma) por las siguientes pérdidas o daños (si tales pérdidas o daños estaban previstas, eran previsibles, o conocidas de cualquier otra forma):
 - (a) Pérdida de ingresos;
 - (b) Pérdida de beneficios reales o anticipados (incluyendo la pérdida de beneficios en contratos);
 - (c) Pérdida del uso de dinero;
 - (d) Pérdida de ahorros anticipados;
 - (e) Pérdida de negocios;

- (f) Pérdida de oportunidad;
 - (g) Pérdida de buena fe;
 - (h) Pérdida de reputación;
 - (i) Pérdida, daños o corrupción de datos, o:
 - (j) Cualquier otra pérdida o daño incidental o consecuente causado de cualquier forma (incluyendo, para eliminar cualquier duda, pérdida o daño del tipo especificado en los párrafos (ii), (a) - (ii), (i).
- (iii) De acuerdo con el párrafo (i), la responsabilidad de Kaspersky Lab (por contrato, daño, restitución o cualquier otra forma) que sea resultado de o esté relacionada con la entrega del Software, estará en cualquier circunstancia limitada a una cantidad no mayor que la pagada por el Software.

7. Este contrato contiene el pleno conocimiento de las partes en cuanto a su contenido y reemplaza todos y cualquier declaración, acuerdo o compromiso entre Usted y Kaspersky Lab, tanto oral o como por escrito o formulado en negociaciones con nosotros o nuestros representantes anteriores a este Acuerdo así como los contratos entre partes relativa a las cuestiones antedichas, que cesan a partir del momento en que este Contrato entre en vigor.