

GUÍA DEL USUARIO

**KASPERSKY
INTERNET
SECURITY 2009**

Estimado usuario de Kaspersky Internet Security 2009:

Gracias por elegir nuestro producto. Esperamos que esta documentación le ayude en su trabajo y le aporte respuestas acerca de este programa.

Advertencia. Este documento es propiedad de Kaspersky Lab, y todos los derechos están reservados de conformidad con las leyes de propiedad intelectual de la Federación Rusa y tratados internacionales. Por lo tanto, la reproducción o distribución ilícita de este documento, parcial o total, puede ser objeto de acciones legales ante los tribunales civiles, administrativos o penales, de conformidad con las leyes de la Federación Rusa. Toda reproducción o distribución de estos materiales, inclusive su traducción, requiere autorización escrita de Kaspersky Lab. Este documento y las ilustraciones asociadas sólo se pueden utilizar con fines de información, no comerciales o personales.

Este documento está sujeto a cambios sin previo aviso. La última versión de este documento, está a su disposición en: <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 incluye marcas comerciales registradas o no.

Todas las marcas comerciales mencionadas pertenecen a sus respectivos propietarios.(c) Kaspersky Lab, 1996-2008

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

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

Fecha de revisión: 28.07.2008

INDICE

INTRODUCCIÓN.....	6
Información sobre la aplicación.....	6
Fuentes de información para búsquedas personalizadas.....	6
Contacto con el Departamento de Ventas.....	7
Contacto con el Servicio de Asistencia técnica.....	7
Foro Internet de Kaspersky Lab.....	9
Novedades de Kaspersky Internet Security 2009.....	9
Principios de protección de la aplicación.....	11
Asistentes y herramientas.....	12
Sobre el soporte.....	13
Análisis heurístico.....	14
Requisitos de hardware y software del sistema.....	15
AMENAZAS A LA SEGURIDAD DEL EQUIPO.....	16
Aplicaciones peligrosas.....	16
Programas nocivos.....	17
Virus y gusanos.....	17
Trojanos.....	21
Herramientas nocivas.....	27
Programas potencialmente indeseables.....	30
Programas publicitarios (adware).....	31
Programas pornográficos (pornware).....	31
Otros programas de riesgo.....	32
Métodos de la aplicación para la detección de objetos infectados, sospechosos y potencialmente peligrosos.....	35
Amenazas en Internet.....	36
Correo no solicitado entrante (Spam).....	36
Phishing.....	37
Ataques de hackers.....	38
Publicidad emergente.....	38
INSTALACIÓN DE LA APLICACIÓN EN SU EQUIPO.....	39
Paso 1. Descarga de versiones recientes de la aplicación.....	40

Paso 2. Comprobación de los requisitos del sistema	41
Paso 3. Ventana de bienvenida del Asistente	41
Paso 4. Lectura del Contrato de licencia	41
Paso 5. Selección del tipo de instalación	42
Paso 6. Selección de la carpeta de instalación	42
Paso 7. Selección de los componentes de aplicación para instalar.....	43
Paso 8. Búsqueda de otros programas antivirus	44
Paso 9. Preparación final de la instalación	45
Paso 10. Fin de la instalación	45
INTERFAZ DEL PROGRAMA	46
Icono del área de notificaciones.....	46
Menú contextual.....	47
Ventana principal de la aplicación	49
Notificaciones.....	52
Ventana de configuración de la aplicación.....	52
PRIMEROS PASOS	54
Selección del tipo de red.....	55
Actualización de la aplicación	56
Análisis de seguridad.....	57
Análisis del equipo en busca de virus.....	57
Administración de la licencia	58
Suscripción para la renovación automática de licencias	59
Participación en Kaspersky Security Network	61
Administración de la seguridad	63
Suspensión de la protección	65
VALIDACIÓN DE LOS PARÁMETROS DE LA APLICACIÓN	67
Prueba con el "virus" EICAR y sus modificaciones.....	67
Prueba de protección del tráfico HTTP	71
Prueba de protección del tráfico SMTP	71
Validación de los parámetros del Antivirus de archivos y memoria	72
Validación de los parámetros de la tarea de análisis antivirus	73
Validación de los parámetros del componente Antispam.....	73

DECLARACIÓN DE RECOLECCIÓN DE DATOS DE KASPERSKY SECURITY NETWORK.....	75
KASPERSKY LAB	82
FUNDACIÓN MOZILLA	95
CONTRATO DE LICENCIA.....	96

INTRODUCCIÓN

EN ESTA SECCIÓN:

Información sobre la aplicación	6
Novedades de Kaspersky Internet Security 2009	9
Principios de protección de la aplicación.....	11
Requisitos de hardware y software del sistema.....	15

INFORMACIÓN SOBRE LA APLICACIÓN

Es fácil obtener respuestas a cualquier consulta que Ud. tenga sobre la compra, la instalación o el uso de la aplicación.

Kaspersky Lab dispone de muchas fuentes de información y Ud. puede elegir la que más le convenga, en función de la urgencia o de la importancia de su consulta.

FUENTES DE INFORMACIÓN PARA BÚSQUEDAS PERSONALIZADAS

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

El sistema de ayuda ofrece información sobre la administración de la protección de su equipo: visualización del estado de la protección, análisis de varias áreas del equipo y ejecución de otras tareas.

Para abrir la Ayuda, active el vínculo **Ayuda** de la ventana principal de la aplicación o pulse <F1>.

CONTACTO CON EL DEPARTAMENTO DE VENTAS

Si tiene alguna consulta sobre la elección o compra de la aplicación, o sobre 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 consultas al Departamento de ventas a:
sales@kaspersky.com.

CONTACTO CON EL SERVICIO DE ASISTENCIA TÉCNICA

Si Ud. ya adquirió la aplicación, y desea obtener información sobre ella, contáctese con el servicio de Asistencia técnica por teléfono o por Internet.

Los especialistas del servicio de Asistencia técnica responderán a sus preguntas sobre la instalación y uso de la aplicación; si su equipo está infectado, le ayudarán a eliminar las consecuencias de las acciones de cualquier programa nocivo.

Antes de contactarse con el servicio de Asistencia técnica, infórmese sobre las reglas de consulta (<http://support.kaspersky.com/support/rules>).

Solicitud por correo al servicio de Asistencia técnica (sólo para usuarios registrados)

Ud. puede consultar a los especialistas del servicio de Asistencia técnica mediante el formulario electrónico del Servicio de ayuda (Helpdesk) en la dirección: (<http://support.kaspersky.com/helpdesk.html>).

Puede plantear su consulta en alemán, español, francés, inglés o ruso.

Cuando envíe su consulta, indique el **número de cliente** recibido al registrarse en el sitio Internet del servicio de Asistencia técnica, y su **contraseña**.

Nota

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

Recibirá la respuesta de un especialista del servicio de Asistencia técnica en su **Espacio personal**.

(<https://support.kaspersky.com/en/PersonalCabinet>) así como en la dirección de correo electrónico especificada en su consulta.

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

- **Tipo de consulta.** 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/eliminación de virus". Si no encuentra una categoría apropiada, elija "Pregunta general".
- **Nombre y número de la versión de la aplicación.**
- **Texto de la consulta.** Describa el problema encontrado con el máximo detalle posible.
- **Número y contraseña de cliente.** Escriba el número y contraseña de cliente recibidos al registrarse en el sitio Internet del servicio de Asistencia técnica.
- **Dirección de correo electrónico.** Los especialistas del servicio de Asistencia técnica enviarán la respuesta a su consulta a esta dirección de correo electrónico.

Asistencia técnica por teléfono

Si su problema requiere ayuda urgente, puede llamar al servicio de Asistencia técnica de su ciudad. Por favor, no olvide brindar toda la información necesaria (<http://support.kaspersky.com/support/details>) cuando consulte al servicio de Asistencia técnica ruso (http://support.kaspersky.com/support/support_local) o internacional (<http://support.kaspersky.com/support/international>). Esto permitirá que nuestros especialistas procesen su consulta a la brevedad posible.

FORO INTERNET DE KASPERSKY LAB

Si su consulta no requiere respuesta urgente, puede plantearla a los especialistas de Kaspersky Lab y a otros usuarios de aplicaciones antivirus de Kaspersky Lab en el Foro Internet de Kaspersky Lab <http://forum.kaspersky.com>.

El foro le permite consultar temas publicados anteriormente, aportar con comentarios, plantear temas nuevos y utilizar el motor de búsqueda.

NOVEDADES DE KASPERSKY INTERNET SECURITY 2009

Kaspersky Internet Security 2009 es un enfoque totalmente nuevo de la seguridad de la información. La característica principal de la aplicación son las restricciones de acceso a los recursos del sistema, que contribuye a prevenir acciones indeseables de programas sospechosos y peligrosos. Se mejoró de manera significativa la capacidad de la aplicación para proteger los datos confidenciales del usuario. La aplicación incluye ahora asistentes y herramientas que facilitan de manera notable la ejecución de tareas específicas de protección del equipo.

Presentamos a continuación las nuevas características de Kaspersky Internet Security 2009:

Nuevas características de protección

- Kaspersky Internet Security incluye ahora el componente *Filtrado de actividades* que, junto a la *Defensa proactiva* y al *Firewall*, implementa un nuevo enfoque universal de protección del sistema contra cualquier amenaza, existente o desconocida. Kaspersky Internet Security requiere ahora mucha menos atención del usuario gracias a la utilización de listas de aplicaciones confiables (listas blancas).
- La búsqueda de vulnerabilidades en el sistema operativo y en las aplicaciones, con su consiguiente eliminación, permite mantener un alto nivel de seguridad y evitar la intrusión de programas peligrosos en su sistema.
- Los nuevos *Asistente de análisis de seguridad* y *Asistente de configuración* del navegador facilitan la búsqueda y eliminación de amenazas de seguridad y vulnerabilidades en las aplicaciones instaladas, en el sistema operativo o en el navegador Internet.

- Kaspersky Lab cuenta ahora con una reacción más rápida ante las nuevas amenazas gracias a la tecnología de participación en *Kaspersky Security Network* que recolecta y envía datos sobre cualquier infección del equipo del usuario a los servidores de Kaspersky Lab.
- Las nuevas herramientas *Monitor de red* y *Análisis de paquetes de red* facilitan la recolección y análisis de información sobre las actividades en red de su equipo.
- El nuevo *Asistente para la restauración del sistema* ayuda a corregir los daños causados por ataques nocivos.

Nuevas características de protección de datos confidenciales:

- El nuevo componente *Filtrado de actividades* supervisa de manera eficaz el acceso de las aplicaciones a datos confidenciales, archivos y carpetas del usuario.
- La seguridad de los datos confidenciales introducidos a través del teclado está asegurada por una nueva herramienta: el *Teclado virtual*.
- La estructura de Kaspersky Internet Security incluye el *Asistente para la limpieza de rastros de actividad privada* que elimina del equipo toda la información personal que podría atraer a los intrusos (lista de sitios Internet visitados, archivos abiertos, cookies, etc.).

Nuevas características antispam:

- Se mejoró la efectividad del filtro antispam en el componente Anti-Spam, gracias a las tecnologías de servidor *Recent Terms*.
- Los complementos para Microsoft Office Outlook, Microsoft Outlook Express, The Bat! y Thunderbird simplifican la configuración de los parámetros antispam.
- La renovación del componente *Control parental* restringe de manera eficaz el acceso de menores de edad a recursos Internet indeseables.

Nuevas características de protección para Internet:

- Se mejoró la protección contra intrusos en Internet gracias a bases de datos antiphishing ampliadas.
- Se incluye el análisis del tráfico ICQ y MSN para una mejor seguridad de los mensajeros instantáneos en Internet.
- La seguridad en redes inalámbricas está asegurada gracias al análisis de las conexiones Wi-Fi.

Nuevas características en la interfaz del programa:

- La nueva interfaz del programa es el reflejo de un nuevo enfoque de protección de la información.
- Los cuadros de diálogo, con su gran capacidad de información, ayudan al usuario a tomar decisiones rápidas.
- Se mejoró la funcionalidad de los informes y de la información estadística sobre las actividades de la aplicación. La posibilidad de aplicar filtros para una mayor flexibilidad de trabajo con informes, hace de KIS 2009 un producto irremplazable para los profesionales.

PRINCIPIOS DE PROTECCIÓN DE LA APLICACIÓN

Kaspersky Internet Security garantiza la protección de su equipo contra cualquier amenaza conocida o desconocida, ataques de piratas e intrusos, correo no deseado y otros datos indeseables. 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 la organización.

Kaspersky Internet Security incluye:

- Vigilancia de las actividades de las aplicaciones en el sistema para evitar que ejecuten acciones peligrosas.
- Componentes de protección contra programas nocivos: proporcionan protección en tiempo real de las transferencias y de las rutas de entrada de todos los datos en su equipo.
- Componentes de protección mientras navega en Internet: aseguran la protección de su equipo contra cualquier ataque o intrusión por red conocido hasta ahora.
- Componentes de filtrado de datos indeseables: ahorran tiempo, dinero y reducen el tráfico Internet.
- Tareas de análisis antivirus: utilizadas para buscar virus en archivos, carpetas, unidades o zonas individuales, o para realizar un análisis completo del equipo. Se pueden configurar las tareas de análisis para detectar vulnerabilidades en las aplicaciones instaladas en su equipo.

- Servicio de actualizaciones: indica el estado interno de los módulos de la aplicación y también permite detectar amenazas, intrusiones de piratas y mensajes no deseados.
- Asistentes y herramientas que facilitan la ejecución de tareas durante el funcionamiento de Kaspersky Internet Security.
- Características de Asistencia técnica que proporcionan información 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 debilidades. Además, resulta difícil analizar y procesar la gran cantidad y diversidad de información existente relativa a la seguridad de sistemas.

Para facilitar la solución de tareas específicas de seguridad de su equipo, Kaspersky Internet Security incluye un conjunto de asistentes y herramientas:

- Asistente para el análisis de la seguridad: realiza diagnósticos de seguridad del equipo y busca vulnerabilidades en el sistema operativo y en los programas instalados en el equipo.
- Asistente para la configuración del navegador Internet: analiza los parámetros de Microsoft Internet Explorer, en primer lugar, desde una perspectiva de seguridad.
- El Asistente de restauración del sistema elimina los rastros de objetos de programas nocivos en el sistema.
- Asistente para la limpieza de los rastros de actividad: busca rastros de acciones del usuario en el sistema y en los parámetros del sistema operativo, que puedan servir para recuperar información confidencial sobre la actividad del usuario.
- El disco de rescate está diseñado para restaurar el sistema después del ataque de un virus que haya dañado archivos del sistema operativo e impida que éste pueda iniciarse.
- 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.

- El Teclado virtual: permite evitar la intercepción de datos introducidos a través del teclado.

SOBRE EL SOPORTE

La aplicación ofrece un conjunto de características de Asistencia técnica al usuario. Están diseñadas para mantener la protección actualizada, mejorar las prestaciones de la aplicación y ayudarle a utilizarla.

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. Esta base de datos asegura una respuesta más rápida a las amenazas más difundidas y alerta a los usuarios sobre ofensivas virales.

Licencia

Al adquirir la aplicación, Ud. 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 Asistencia técnica durante cierto tiempo. Las condiciones de uso y otros datos necesarios para que el programa sea completamente funcional vienen incluidos en un archivo llave.

El menú **Licencia** le permite consultar información detallada sobre su licencia, renovarla o adquirir una nueva.

Asistencia técnica

Todos los usuarios registrados de Kaspersky Internet Security pueden beneficiarse de nuestro servicio de Asistencia técnica. Para saber dónde exactamente puede obtener Asistencia técnica, utilice la entrada **Asistencia técnica**.

Los vínculos le dan acceso al Foro de usuarios de Kaspersky Lab y le permiten enviar sugerencias o un informe de errores a Asistencia técnica mediante un formulario especial en línea.

También podrá tener acceso al Asistencia técnica en línea, a los servicios de su Espacio personal y, por supuesto, nuestro personal está siempre dispuesto a ayudarle con Kaspersky Internet Security por teléfono.

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; los análisis antivirus también recurren a este método.

Por supuesto, el análisis mediante comparación de firmas, a partir de una base de datos existente que contiene la descripción de las amenazas conocidas y métodos para su reparación, sigue siendo la respuesta definitiva para determinar si un objeto es nocivo y su clasificación como programa peligroso. El método heurístico, a diferencia del método de comparación de firmas, intenta detectar comportamientos típicos (en lugar de firmas de códigos nocivos) que permiten al programa dictaminar sobre la peligrosidad de un archivo con cierto grado de probabilidad.

La ventaja del análisis heurístico es que no hay que actualizar la base de datos para realizar el análisis. Gracias a esto, consigue detectar nuevas amenazas antes de que los analistas antivirus las detecten.

Sin embargo, existen métodos que permiten engañar a los métodos heurísticos. Por ejemplo, una de estas medidas consiste en congelar la actividad de un código nocivo tras detectar un análisis heurístico en curso.

Nota: El uso combinado de varios métodos de análisis garantiza una mayor seguridad.

En caso de amenaza potencial, el analizador heurístico simula la ejecución del objeto dentro del entorno virtual seguro de la aplicación. Si descubre alguna actividad sospechosa durante la ejecución del objeto, la aplicación lo considera como dañino y no le permite ejecutarse en el equipo anfitrión, o presenta un mensaje al usuario solicitando instrucciones adicionales:

- Mover a cuarentena la nueva amenaza para analizarla y procesarla más tarde con bases de datos 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**. Para ello, mueva la barra deslizadora a una de estas posiciones: Superficial, Medio o Detallado. El nivel de detalle asegura el 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 consumo de recursos del sistema y mayor tiempo requerido.

Advertencia!

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

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

REQUISITOS DE HARDWARE Y SOFTWARE DEL SISTEMA

Para asegurar el normal funcionamiento de la aplicación, el equipo debe cumplir las siguientes especificaciones mínimas:

Requisitos generales:

- 75 Mb de espacio libre en disco duro.
- CD-ROM (para instalar la aplicación desde el CD).
- 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), Microsoft Windows XP Professional x64 Edition:

- Procesador Intel Pentium 300 MHz o superior (o su equivalente compatible).
- 256 Mb de memoria RAM libre.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Procesador Intel Pentium 800 MHz 32 bits (x86) / 64 bits (x64) o superior (o su equivalente compatible).
- 512 Mb de memoria RAM libre.

AMENAZAS A LA SEGURIDAD DEL EQUIPO

Las aplicaciones nocivas constituyen una considerable amenaza a la seguridad del equipo. Además, otras amenazas provienen del correo no deseado, mensajes fraudulentos (phishing), intrusiones de piratas, así como programas publicitarios (adware) o pornográficos (pornware). Estas amenazas están asociadas al uso de Internet.

EN ESTA SECCIÓN:

Aplicaciones peligrosas.....	16
Amenazas en Internet.....	36

APLICACIONES PELIGROSAS

La aplicación de Kaspersky Lab puede detectar centenares de miles de programas nocivos residentes en su equipo. Algunos de estos programas constituyen una gran amenaza para su equipo, mientras otros sólo suponen un peligro si se cumplen determinadas condiciones. Después de detectar un programa nocivo, el programa lo clasifica y le atribuye un nivel de peligrosidad (alta o media).

Los analistas antivirus de Kaspersky Lab distinguen dos categorías principales: *programas nocivos* y *programas potencialmente indeseables*.

Programas nocivos (página 17) (Malware): diseñados con el propósito de producir daños al equipo y al usuario, por ejemplo, robo, bloqueo, alteración o eliminación de datos, interrupción en el funcionamiento de los equipos o de la red.

Programas potencialmente indeseables (página 30) (PUP): a diferencia de los programas nocivos, no producen daños, pero pueden ser inoportunos.

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

PROGRAMAS NOCIVOS

Los **programas nocivos (Malware)** están diseñados específicamente para dañar al equipo y al usuario: robar, bloquear, modificar o eliminar información, o alterar el funcionamiento del equipo o de la red.

Los programas nocivos se dividen en tres subcategorías: *virus* y *gusanos*, *troyanos*, y *utilidades nocivas*.

Virus y gusanos (página 17) (*Viruses_and_Worms*): 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 interacción del usuario para poder ejecutarse. Estos programas realizan sus acciones nocivas cuando se los ejecuta.

Troyanos (página 21) (*Trojan_programs*): a diferencia de los gusanos y los virus, no se reproducen. Se infiltran en el equipo, por ejemplo, a través del correo electrónico o de un navegador, cuando el usuario consulta un sitio Internet "infectado". Para ejecutarse y realizar sus acciones nocivas, necesitan la intervención del usuario.

Herramientas nocivas (página 27) (*Malicious_tools*): son herramientas diseñadas especialmente para producir daños. Sin embargo, a diferencia de otros programas nocivos, no ejecutan inmediatamente acciones nocivas y se pueden guardar y ejecutar de forma segura en el equipo del usuario. Estos programas tienen funciones para crear virus, gusanos y troyanos, organizar ataques de red en servidores remotos, piratear equipos o realizar otras acciones nocivas.

VIRUS Y GUSANOS

Subcategoría: Virus y gusanos (*Viruses_and_Worms*)

Nivel de riesgo: alto Máximo.

Los virus y gusanos tradicionales realizan en el equipo acciones sin la autorización del usuario, y pueden crear copias de sí mismos que, a su vez, se reproducen.

Virus tradicionales

Después de infiltrarse en el sistema, un virus tradicional infecta un archivo, se activa en el mismo, realiza su acción nociva y a continuación agrega copias de sí mismo a 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. Sólo pueden penetrar en otros equipos si consiguen agregar una copia de sí mismos a un archivo almacenado 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 es capaz de penetrar en varias zonas del equipo, del sistema operativo o de una aplicación. En función del entorno, pueden haber *virus de archivo*, *virus de arranque*, *virus de secuencia de comandos* y *virus de macro*.

Los virus pueden infectar archivos de diferentes modos. *Los virus de sobreescritura* escriben su propio código reemplazando el código del archivo infectado, tras lo cual destruyen el contenido del archivo. El archivo infectado deja de funcionar y no es posible repararlo. *Los virus parasitarios* modifican los archivos, dejándolos parcial o completamente operacionales. *Los virus compañeros* no alteran los archivos pero crean duplicados de los mismos. Cuando se abre un archivo infectado de esta forma, se ejecuta su copia, es decir el propio virus. Existen también *virus vinculados*, virus (OBJ) que *infectan módulos objeto*, virus que *infectan bibliotecas de compilación (LIB)*, otros que *infectan el texto original de los programas*, etc.

Gusanos

Después de infiltrarse en el sistema, el código de un gusano de red, de forma similar al código de un virus tradicional, se ejecuta y realiza su acción nociva. Los gusanos de red se denominan así por su capacidad para aprovechar los medios de comunicación entre equipos (sin el conocimiento de sus usuarios) para enviar copias de sí mismos a través de varios canales de información.

Es el modo de proliferación lo que permite diferenciar los principales tipos de gusanos. La siguiente continuación describe los tipos de gusanos en función a su modo de proliferación.

Tabla 1. Gusanos según el modo de proliferación

TIPO	NOMBRE	DESCRIPCIÓN
IM-Worm	Gusanos de mensajería instantánea	<p>Se propagan a través de clientes de mensajería instantánea (IM) como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager o Skype.</p> <p>Normalmente, utilizan la lista de contactos para enviar mensajes con un vínculo hacia una copia de su mismo archivo, ubicada en un sitio Internet. Cuando un usuario descarga y abre dicho archivo, el gusano se activa.</p>
Email-Worm	Gusanos de correo	<p>Infectan los equipos a través del correo electrónico.</p> <p>Un mensaje infectado contiene una copia del gusano, o un vínculo a dicho archivo alojado en un sitio Internet infectado o en el sitio del autor. El gusano se ejecuta cuando se abre este tipo de adjuntos: al activar el vínculo, descargar y abrir un archivo, el gusano también se ejecuta y realiza su acción nociva. Tras esto, sigue reproduciéndose mediante copias y buscando nuevas direcciones de correo electrónico para enviarles mensajes infectados.</p>
IRC-Worm	Gusanos de mensajería instantánea	<p>Los gusanos de este tipo penetran en los equipos a través de sistemas IRC (Internet Relay Chat, sistemas que permiten comunicar con otras personas por Internet en tiempo real).</p> <p>Este gusano publica en servicios de chat Internet un archivo con su propia copia o un vínculo a dicho archivo. El gusano se activa cuando un usuario descarga y abre dicho archivo.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Net-Worms	Gusanos de red (residentes en redes)	<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. Dentro de la red local, buscan equipos con programas que presenten vulnerabilidades. Para ello, envían 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, dejará pasar 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 infiltrarse dentro de una red de intercambio de archivos, el gusano se duplica dentro de la carpeta de intercambio normalmente ubicada en el 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>Gusanos más complejos imitan los protocolos de una red de intercambio de archivos específica: Responden positivamente a peticiones de búsqueda y ofrecen la descarga de sus copias.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Gusanos	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 y buscan acceso completo a sus discos. A diferencia de otros gusanos de red, para que se active este gusano, el usuario debe abrir un archivo con su copia. • Gusanos que no utilizan ninguno de los métodos de propagación descritos en esta tabla (por ejemplo, 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 troyanos no crean copias de sí mismos. Se infiltran en el equipo, por ejemplo, a través del correo electrónico, o de un navegador cuando el usuario visita un sitio Internet "infectado". Los troyanos deben ser ejecutados por el usuario antes de realizar sus acciones nocivas.

El comportamiento de los distintos programas troyanos en el equipo infectado puede variar. Las características principales de los troyanos son el bloqueo, modificación y eliminación de datos, y la perturbación del funcionamiento de los equipos en redes informáticas. Además, los troyanos pueden recibir y enviar archivos, ejecutarlos, mostrar mensajes, conectarse a páginas Internet, descargar e instalar programas y reiniciar el equipo infectado.

Los intrusos utilizan a menudo "conjuntos" que incluyen varios programas troyanos.

La siguiente tabla describe los tipos y comportamientos de los troyanos.

Tabla 2. Tipos de troyanos en función a 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 archivo comprimido, el equipo empieza a ralentizarse o se "congela" mientras el 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 paralizarlo.
Backdoor	Troyanos de administración remota (puerta trasera)	Se consideran los más peligrosos de todos los troyanos. Por sus características recuerdan a los programas de administración remota comunes. Estos programas se instalan a sí mismos sin el conocimiento del usuario y facilitan a los intrusos la administración remota del equipo.
Trojans	Troyanos	<p>Los troyanos incluyen los siguientes programas nocivos:</p> <ul style="list-style-type: none"> • Troyanos tradicionales: sólo realizan las funciones principales de los programas troyanos: bloqueo, modificación o eliminación de datos; perturbación del funcionamiento de un equipo o de una red; no tienen funciones adicionales que son características de los otros tipos de troyanos descritos en esta tabla. • Troyanos "polivalentes": disponen de funciones adicionales, características de varios tipos de troyanos.

TIPO	NOMBRE	DESCRIPCIÓN
Trojans-Ransoms	Troyanos chantajistas	"Secuestran" la propia información del usuario, modificando, bloqueando o perturbando el funcionamiento del equipo, de forma que el usuario es incapaz de utilizar sus datos. A continuación, el pirata pide un rescate al usuario a cambio de proporcionarle un programa que restablecerá el funcionamiento del equipo.
Trojans-Clickers	Troyanos generadores de clics	<p>Acceden a páginas Internet desde el equipo del usuario: Envían instrucciones al programa navegador o sustituyen direcciones Internet almacenadas en los archivos del sistema.</p> <p>Gracias a estos programas, los intrusos organizan ataques por red y aumentan el tráfico hacia esos sitios para mejorar la cantidad de apariciones de banners publicitarios.</p>
Trojans-Downloaders	Troyanos descargadores	Acceden a la página Internet del intruso, descargan e instalan otros programas nocivos en el equipo del usuario; guardan el nombre del archivo del programa nocivo que descargan, o lo obtienen de la página Internet consultada.

TIPO	NOMBRE	DESCRIPCIÓN
Trojan-Droppers	Troyanos dropper	<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 (Droppers) para:</p> <ul style="list-style-type: none"> • Instalar programas nocivos sin la participación del usuario: estos “droppers” no muestran ningún mensaje propio o falso, por ejemplo para informar acerca de un error de archivo o de una versión incorrecta del sistema operativo. • Evitar la detección de otros programas nocivos conocidos: ningún programa antivirus puede detectar un programa nocivo alojado en un “dropper”.
Trojans-Notifiers	Troyanos notificadores	<p>Notifican al pirata que el equipo infectado está conectado, y luego le transfieren información sobre el equipo: Direcciones IP, el número de un puerto abierto, o una dirección de correo electrónico. Se comunican con el intruso por correo electrónico, mediante FTP, conectándose a su página Internet, o mediante otros métodos.</p> <p>Este tipo de troyanos se utiliza a menudo en conjuntos compuestos por varios troyanos. Informan al pirata sobre la instalación exitosa de otros troyanos en el equipo del usuario.</p>
Trojans-Proxies	Troyanos proxy	<p>Permiten al intruso acceder, de forma anónima, a páginas Internet desde el equipo del usuario y sirven a menudo para enviar correo no deseado.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Trojans-PSWs	Ladrones de contraseñas	<p>Trojans ladrones de contraseñas (PSW, Password Stealing Ware); roban cuentas de usuarios, por ejemplo, información sobre registro de programas. Buscan datos confidenciales en los archivos del sistema y en el Registro y los envían al pirata por correo electrónico, mediante FTP, conectándose a su página Internet, o mediante otros métodos.</p> <p>Algunos de estos trojans pertenecen a los tipos especiales descritos en esta tabla. Se trata de trojans que roban información de cuentas bancarias (Trojans-Bankers), trojans que roban datos personales de usuarios de clientes de mensajería instantánea (Trojans-IMs) y trojans que roban datos de usuarios de juegos en línea (Trojans-GameThieves).</p>
Trojans-Spies	Trojans espía	<p>Se usan para espiar al usuario: recopilan información sobre sus acciones en el equipo, por ejemplo, interceptando datos introducidos mediante el teclado, capturando imágenes de la pantalla y generando listas de aplicaciones activas. Después de recuperar esta información, la transmiten al intruso por correo electrónico, mediante FTP, conectándose a su página Internet, o mediante otros métodos.</p>
Trojans-DDoS	Trojans DDoS	<p>Envían numerosas peticiones al servidor remoto desde el equipo del usuario. El servidor agota sus recursos para procesar las peticiones hasta que deja de funcionar (Denial-of-Service (DoS)). Estos programas sirven a menudo para infectar múltiples equipos desde los que atacan al servidor.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Trojans-IMs	Ladrones de datos en mensajerías instantáneas	Estos programas roban números y contraseñas a los usuarios de programas de mensajería instantánea (programas de chat), como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager o Skype. A continuación, transmiten la información al intruso por correo electrónico, mediante FTP, conectándose a su página Internet, o mediante otros métodos.
Rootkits	Rootkits	Estos programas ocultan otros programas nocivos y su actividad, facilitando así su existencia y propagación dentro del sistema; ocultan archivos o procesos en la memoria de un equipo infectado, registran claves ejecutadas por los programas nocivos, ocultan el intercambio de datos entre las aplicaciones instaladas en el equipo del usuario y otros equipos de la red.
Trojans-SMS	Trojanos de mensajes SMS	Infectan teléfonos móviles desde los que envían mensajes SMS a números de pago que se facturan al usuario.
Trojans-GameThieves	Ladrones de datos en juegos de red.	Estos programas roban los datos de cuentas de usuarios de juegos en línea; a continuación, transmiten esta información al pirata por correo electrónico, mediante FTP, conectándose a su página Internet, o mediante otros métodos.
Trojans-Bankers	Ladrones de cuentas bancarias	Estos programas roban datos de cuentas bancarias o de dinero electrónico; después, transmiten estos datos al intruso por correo electrónico, mediante FTP, conectándose a la página Web del intruso o con otros métodos.

TIPO	NOMBRE	DESCRIPCIÓN
Trojans-Mailfinders	Buscadores de direcciones electrónicas	Estos programas recuperan direcciones de correo electrónico en el equipo y las transmiten al pirata por correo electrónico, mediante FTP, conectándose a su página Internet, o mediante otros métodos. El pirata utiliza las direcciones recopiladas para enviarles correo no deseado.

HERRAMIENTAS NOCIVAS

Subcategoría: Herramientas nocivas (Malicious_tools) **Nivel de riesgo:** alto medio

Son herramientas diseñadas especialmente para producir daños. Sin embargo, a diferencia de otros programas nocivos, no ejecutan inmediatamente acciones nocivas y se pueden guardar y ejecutar de forma segura en el equipo del usuario. Estos programas cuentan con funciones para crear virus, gusanos y troyanos, organizar ataques de red en servidores remotos, piratear equipos o realizar otras acciones nocivas.

Son varios tipos de herramientas nocivas con diferentes funciones. La tabla a continuación describe sus diferentes tipos.

Tabla 3. Herramientas nocivas por su función

TIPO	NOMBRE	DESCRIPCIÓN
Constructor	Constructores	Los constructores sirven para generar virus, gusanos y troyanos nuevos. Algunos constructores poseen una interfaz estándar con ventanas que permite seleccionar el tipo de programa nocivo a crear, el método utilizado para evitar la depuración así como otras propiedades.
	Ataques de red DoS	Envían numerosas peticiones al servidor remoto desde el equipo del usuario. El servidor agota sus recursos para procesar las peticiones hasta que deja de funcionar (Denial-of-Service (DoS)).

TIPO	NOMBRE	DESCRIPCIÓN
Exploit	Exploit/Hazaña	<p>Se denomina "exploit" a un conjunto de datos o código de programa que usa vulnerabilidades de un programa para ejecutar acciones nocivas en un equipo. Por ejemplo, un exploit puede escribir o leer archivos, o abrir páginas Internet "infectadas".</p> <p>Los diferentes exploits aprovechan las vulnerabilidades de diferentes aplicaciones o servicios de red. Un exploit se transmite por la red a múltiples equipos como un paquete de red para encontrar equipos con servicios de red vulnerables. Una hazaña incluida en un archivo DOC aprovecha las vulnerabilidades de los procesadores de texto. Puede ejecutar operaciones programadas por el intruso cuando el usuario abre un archivo infectado. Un exploit contenido en un mensaje de correo busca vulnerabilidades dentro de los programas de correo; es capaz de ejecutar su acción nociva tan pronto como el usuario abre el mensaje infectado dentro del programa.</p> <p>Los exploits sirven para propagar 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 nocivos 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. Estos canales incluyen, por ejemplo, programas IRC ("chat").</p> <p>Sin embargo, este tipo de programa nocivo no incluye programas que saturen el tráfico de correo, los canales de mensajería instantánea o envíen SMS. La tabla a continuación clasifica estos programas por tipos separados (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 (por ejemplo, agregando sin permiso usuarios de sistema, borrando los informes de sistema para ocultar cualquier rastro de su presencia en el equipo). Incluyen algunos "sniffers" (analizadores de red) que ejecutan funciones nocivas, como interceptar contraseñas, por ejemplo. Los sniffers son programas que permiten analizar el tráfico de red.</p>
not-virus:Hoax	Bromistas	<p>Asustan al usuario con mensajes falsos sobre virus: Pueden "detectar" un virus en un archivo limpio o mostrar un mensaje sobre un formateado del disco que nunca se realizará.</p>
Spoofers	Spoofers	<p>Envían mensajes y peticiones de red con una dirección de remite falsa. Los intrusos los utilizan, por ejemplo, para aparentar ser otro remitente.</p>
VirTools	Herramientas que modifican programas nocivos	<p>Permiten modificar otros programas nocivos para ocultarlos de las aplicaciones antivirus.</p>

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

PROGRAMAS POTENCIALMENTE INDESEABLES

Programas potencialmente indeseables: a diferencia de los programas nocivos, no están diseñados sólo para producir daños. Sin embargo, pueden servir para violar la seguridad del equipo.

Los programas potencialmente indeseables incluyen *programas publicitarios (adware)*, *captadores pornográficos (pornware)* y *otros programas potencialmente indeseables*.

Los programas publicitarios (Adware) (página 31) presentan información publicitaria al usuario.

Los programas pornográficos (página 31): (Pornware) presentan información pornográfica al usuario.

Otros programas de riesgo (página 32): más a menudo de lo deseable, muchos usuarios informáticos utilizan estos programas. Sin embargo, si un pirata consigue introducirse o instalar dichos programas en el equipo del usuario, podrá explotar algunas de sus características para violar su seguridad.

Los programas potencialmente indeseables se instalan mediante uno de los siguientes métodos:

- El mismo usuario los instala, individualmente o junto con otro programa (por ejemplo, los desarrolladores de programas incluyen programas publicitarios dentro sus programas freeware o shareware).
- También los instalan los piratas que, por ejemplo, los incluyen en paquetes de otros programas nocivos, aprovechan "vulnerabilidades" del navegador Internet o utilizan cargadores o lanzaderas de troyanos, cuando el usuario visita un sitio Internet "infectado".

PROGRAMAS PUBLICITARIOS (ADWARE)

Subcategoría: programas publicitarios (adware)

Nivel de riesgo: alto medio

Los programas publicitarios (Adware) tienen como fin mostrar publicidad al usuario. Muestran pancartas (banners) publicitarias en la interfaz de otros programas, y remiten las consultas de búsqueda hacia sitios Internet de publicidad. Algunos programas publicitarios recopilan y redirigen a sus autores datos de marketing acerca del usuario, por ejemplo, qué sitios visita, qué búsquedas hace (a diferencia de los troyanos espía, estos programas transfieren la información con la autorización del usuario).

PROGRAMAS PORNOGRÁFICOS (PORNWARE)

Subcategoría: Programas pornográficos (pornware)

Nivel de riesgo: alto medio

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

Los piratas también pueden instalar estos programas en el equipo del usuario para mostrar publicidad de sitios y servicios comerciales pornográficos sin autorización del usuario. Para instalarlos, aprovechan vulnerabilidades del sistema operativo o del navegador Internet o utilizan cargadores o lanzaderas de troyanos.

Existen tres tipos de programas pornográficos, en función de sus características. La tabla a continuación describe estos tipos.

Tabla 4. Tipos de programas pornográficos, según características

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

OTROS PROGRAMAS DE RIESGO

Subcategoría: Otros programas de riesgo

Nivel de riesgo: alto medio

Muchos usuarios utilizan la mayoría de estos programas. Incluyen los clientes IRC, marcadores telefónicos, programas de descarga de archivos, monitores de actividad del sistema informático, herramientas para trabajar con contraseñas, servidores Internet FTP, HTTP o Telnet.

Sin embargo, si un pirata consigue introducirse o instalar dichos programas en el equipo del usuario, podrá explotar algunas de sus características para violar la seguridad.

A otros programas de riesgo se los clasifica por sus características. La tabla a continuación describe sus diferentes tipos.

Tabla 5. Otros tipos de programas de riesgo según sus características

TIPO	NOMBRE	DESCRIPCIÓN
Client-P2P	Programas clientes de chat Internet	Los usuarios los instalan para comunicarse por IRC. Los piratas los utilizan para propagar programas nocivos.
Dialers	Programas de marcación automática	Establecen conexiones telefónicas "ocultas" por módem.
Downloaders	Descargadores	Descargan en secreto archivos desde sitios Internet.
Monitors	Monitores	Permiten supervisar la actividad de los equipos donde se encuentran instalados (rendimiento de las aplicaciones, cómo intercambiar datos con aplicaciones de otros equipos, etc.)
PSWTools	Herramientas de recuperación de contraseñas	Sirven para mostrar y recuperar contraseñas olvidadas. Los piratas buscan exactamente lo mismo cuando los instalan en los equipos de los usuarios.
RemoteAdmin	Programas de administración remota	<p>Los administradores de sistema los utilizan a menudo; dan acceso a la interfaz del equipo remoto con el fin de supervisarla y controlarla. Los piratas buscan exactamente lo mismo cuando los instalan en los equipos, para vigilarlos y controlarlos.</p> <p>Son diferentes de los troyanos de administración remota, o puertas traseras (Backdoors). Los troyanos poseen funciones que les permiten infiltrarse e instalarse en el sistema de forma independiente, mientras que los programas de riesgo no disponen de estas características.</p>

TIPO	NOMBRE	DESCRIPCIÓN
Server-FTP	Servidores FTP	Realizan las funciones de un servidor FTP. Los piratas se instalan en los equipos de los usuarios para tener acceso remoto a través del protocolo FTP.
Server-Proxy	Servidores proxy	Realizan las funciones de un servidor proxy. Los piratas los instalan en los equipos de los usuarios para enviar correo no deseado sin el conocimiento del usuario.
Server-Telnet	Servidores Telnet	Realizan las funciones de un servidor Telnet. Los piratas los instalan en los equipos de los usuarios para tener acceso remoto a través del protocolo Telnet.
Server-Web	Servidores Internet	Realizan las funciones de un servidor Internet. Los piratas los instalan en los equipos de los usuarios para tener acceso remoto a través del protocolo HTTP.
RiskTool	Herramientas locales del equipo	Proporcionan características avanzadas que operan tan sólo en el equipo del usuario (ocultan archivos o ventanas de aplicaciones activas, cierran procesos activos).
NetTool	Herramientas de red	Proporcionan al usuario del equipo donde están instaladas características avanzadas que le permiten administrar otros equipos de la red (reiniciarlos, encontrar puertos abiertos, ejecutar programas instalados en estos equipos).
Client-P2P	Clientes P2P	Son utilizados en redes punto a punto (P2P). Los piratas pueden utilizarlos para propagar programas nocivos.

TIPO	NOMBRE	DESCRIPCIÓN
Client-SMTP	Cientes SMTP	Envían correo de forma oculta. Los piratas los instalan en los equipos de los usuarios para enviar correo no deseado sin el conocimiento del usuario.
WebToolbar	Barras de herramientas Internet	Agregan sus propias barras de herramientas a las de otras aplicaciones.
FraudTool	Programas fraudulentos	Se presentan como si fuesen programas auténticos. Por ejemplo, existen programas antivirus fraudulentos que muestran mensajes acerca de la detección de programas nocivos, pero no encuentran ni neutralizan nada.

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

La aplicación de Kaspersky Lab detecta programas nocivos en los objetos mediante dos métodos: *reactivo* (mediante bases de datos) y *proactivo* (mediante análisis heurístico).

Las bases de datos son archivos con registros utilizados para identificar centenares de miles de amenazas conocidas en objetos. Los registros contienen información acerca de secciones de control en el código de los programas nocivos, y de los algoritmos utilizados para desinfectar los objetos que contienen estos programas. Los analistas antivirus de Kaspersky Lab detectan a diario centenares de programas nocivos, crean registros que los identifican y los incluyen en actualizaciones a la base de datos.

Si la aplicación de Kaspersky Lab detecta en un objeto segmentos de código que coinciden exactamente con el identikit de un programa nocivo existente en la base de datos, dictaminará que se trata de un objeto *infectado*. Si sólo

coincide en parte (de acuerdo con ciertas condiciones), lo clasificará como objeto *sospechoso*.

Con el método proactivo, la aplicación consigue detectar los programas nocivos más recientes, cuya información todavía no aparece en la base de datos.

La aplicación Kaspersky Lab es capaz de detectar objetos que contienen nuevos programas nocivos basándose en el análisis de su comportamiento. No sería cierto decir que el código de este objeto coincide en parte o en totalidad con el de un programa nocivo conocido, pero sí decir que contiene algunas secuencias de comandos que son características de programas nocivos, como la apertura o escritura de un archivo, o la interceptación de interrupciones. La aplicación determina, por ejemplo, que un archivo puede estar infectado por un *virus de arranque* desconocido.

Los objetos detectados por el método proactivo son clasificados como potencialmente peligrosos.

AMENAZAS EN 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 (ver sección " Correo entrante no solicitado o spam " en la página 36);
- Fraudes (phishing) (página 37);
- Ataques de hackers (página 38);
- Banners publicitarios (página 38).

CORREO NO SOLICITADO ENTRANTE (SPAM)

La aplicación Kaspersky Lab protege a los usuarios contra el correo no solicitado. Se considera spam a los mensajes entrantes no solicitados, a menudo de carácter publicitario. El correo no solicitado supone una carga adicional de los canales y servidores de correo del proveedor. El destinatario paga por el tráfico no deseado generado y los mensajes legítimos se reciben con mayor demora. Por esta razón, el correo no solicitado se considera ilegal en muchos países.

La aplicación Kaspersky Lab analiza los mensajes entrantes de Microsoft Office Outlook, Microsoft Outlook Express y The Bat! y, si detecta que alguno es un mensaje no deseado, aplica las acciones seleccionadas, por ejemplo, moverlo hacia una carpeta especial o eliminarlo.

La aplicación Kaspersky Lab detecta el correo no deseado con un elevado grado de precisión. Aplica varias tecnologías de filtrado antispam: detecta el correo no solicitado en función de la dirección del remitente así como de las palabras y frases presentes en el campo del 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 de datos antispam contienen listas “blancas” y “negras” de direcciones de remitentes, listas de palabras y frases relacionadas con publicidad, medicinas y salud, juegos de azar, etc.

PHISHING

El *phishing* 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.

El phishing está a menudo asociado con la banca en Internet. Los intrusos crean una réplica exacta del sitio web de un determinado banco y envían mensajes a sus clientes en nombre del banco. Les informan que debido a ciertos cambios o fallos en el sistema informático bancario, se han perdido las cuentas de los usuarios por lo que éstos deben confirmar o modificar sus datos en el sitio Internet del banco. El usuario activa el vínculo al sitio Internet creado por los piratas e introduce sus datos personales.

Las bases de datos del componente antiphishing contienen la lista de direcciones URL de sitios Internet conocidos como origen de los fraudes.

La aplicación Kaspersky Lab analiza los mensajes entrantes de Microsoft Office Outlook y Microsoft Outlook Express y si encuentra un vínculo a una dirección URL registrada en la base de datos, lo clasifica como no deseado. Si el usuario abre el mensaje e intenta seguir el vínculo, la aplicación bloquea el acceso al sitio Internet.

ATAQUES DE HACKERS

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

Los ataques de red son acciones intrusivas (por ejemplo, análisis de puertos, intentos de robo de contraseñas) o programas nocivos que ejecutan instrucciones en nombre del usuario y transmiten la información a su autor, o realizan otras funciones vinculadas con ataques por red. Entre ellos, se cuentan algunos troyanos, ataques DoS (denegación de servicio), scripts nocivos y algunos tipos de gusanos de red.

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

La aplicación Kaspersky Lab bloquea los ataques de red sin interrumpir las conexiones de red. Utiliza bases de datos especiales del componente Firewall. Estas bases de datos contienen registros que identifican características de los paquetes de datos IP de varios programas intrusivos. La aplicación antivirus analiza las conexiones de red y las bloquea si encuentra en ellas paquetes IP que considere peligrosos.

PUBLICIDAD EMERGENTE

Los banners o avisos publicitarios con vínculos al sitio Internet del anunciante se presentan, la mayoría de las veces, como imágenes. La aparición de pancartas en el sitio Internet no supone ninguna amenaza para la seguridad del equipo, pero se considera una interferencia del funcionamiento normal del equipo. La intermitencia de las publicidades en la pantalla irrita y reduce el rendimiento laboral. El usuario se distrae con información irrelevante. Además, los vínculos de los avisos aumentan el tráfico Internet.

Muchas organizaciones prohíben la presentación de avisos publicitarios en sus interfaces, como parte de sus directivas de seguridad informática.

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

INSTALACIÓN DE LA APLICACIÓN EN SU EQUIPO

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

Advertencia!

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

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

Nota:

La instalación con el archivo de distribución descargado por Internet es idéntica a la instalación desde el CD.

Tras esto, el Asistente de instalación busca el paquete de instalación de la aplicación (con extensión *.msi) y, si lo encuentra, busca una versión nueva en los servidores de Internet de Kaspersky Lab. Si no encuentra el paquete de instalación, le ofrece descargarlo. Después de descargar el archivo, comienza la instalación de la aplicación. Si cancela la descarga, el proceso de instalación de la aplicación se reanudará en modo normal.

El programa de instalación está diseñado como un Asistente. Cada ventana contiene un conjunto de botones para controlar el proceso de instalación. A continuación brindamos 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.....	40
Paso 2. Comprobación de los requisitos del sistema.....	41
Paso 3. Ventana de bienvenida del Asistente	41
Paso 4. Lectura del Contrato de licencia.....	41
Paso 5. Selección del tipo de instalación	42
Paso 6. Selección de la carpeta de instalación.....	42
Paso 7. Selección de los componentes de aplicación para instalar	43
Paso 8. Búsqueda de otros programas antivirus	44
Paso 9. Preparación final de la instalación.....	45
Paso 10. Fin de la instalación.....	45

PASO 1. DESCARGA DE VERSIONES RECIENTES DE LA APLICACIÓN

Antes de instalar la aplicación en su equipo, el Asistente consulta los servidores de actualización de Kaspersky Lab para determinar si existe una nueva versión de la aplicación.

Si no detecta la presencia de una versión nueva en los servidores de actualización de Kaspersky Lab, el Asistente de instalación continuará la instalación en curso.

Si encuentra una versión más reciente de la aplicación en los servidores, el Asistente le ofrecerá descargarla. Si cancela la descarga, el Asistente de instalación se reanudará para instalar la versión en curso. Si decide instalar una versión más reciente, los archivos de instalación se descargarán a su equipo y el Asistente de instalación empezará 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 de la aplicación.

PASO 2. COMPROBACIÓN DE LOS REQUISITOS DEL SISTEMA

Antes de instalar la aplicación en su equipo, el Asistente comprueba la conformidad del sistema operativo y de la instalación de sus actualizaciones (Service Pack) con los requisitos de instalación de la aplicación (sección "Requerimientos de hardware y software" en la página 15). También comprueba que los programas requeridos estén instalados en su equipo y que Ud. disponga de los permisos suficientes para instalar la aplicación.

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

PASO 3. VENTANA DE BIENVENIDA DEL ASISTENTE

Si su sistema cumple con todos los requisitos (sección "Requerimientos de hardware y software" en la página 15), y 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 reanudará para instalar la versión actual de la aplicación. El primer cuadro de diálogo del Asistente, con información sobre el inicio de la instalación, aparecerá en la pantalla.

Para continuar con la instalación, pulse el botón **Siguiente**. Para cancelar la instalación, pulse el botón **Cancelar**.

PASO 4. LECTURA DEL CONTRATO DE LICENCIA

El cuadro de diálogo siguiente incluye un *Contrato de licencia* entre Ud. 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 pulse el botón **Siguiente**. La instalación continuará.

Para cancelar la instalación, pulse el botón **Cancelar**.

PASO 5. SELECCIÓN DEL TIPO DE INSTALACIÓN

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

- **Instalación rápida.** Si selecciona esta opción, se instalará la aplicación completa en su equipo, con los parámetros de protección recomendados por los expertos de Kaspersky Lab. Después de completar la instalación, se abrirá el Asistente de instalación de la aplicación.
- **Instalación personalizada.** En este caso, podrá seleccionar los componentes de la aplicación que desea instalar en su equipo, especificar la carpeta de destino de la instalación (sección "Paso 6. Selección de la carpeta de instalación" en la página 42), activar y configurar la aplicación con un Asistente especial.

Si selecciona la primera opción, el Asistente de instalación de la aplicación pasará directamente al Paso 8 (ver sección "Paso 8. Búsqueda de otras aplicaciones antivirus" en la página 44). En el 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 42).

En este paso, puede identificar una carpeta en su equipo en la que se instalará la aplicación. La ruta predeterminada es:

- <Drive> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009 : para sistemas de 32 bits.
- <Drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009 : para sistemas de 64 bits.

Para especificar una carpeta diferente pulse el botón **Examinar** y selecciónela 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, pulse el botón **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 42).

En caso de optar por la instalación personalizada, deberá seleccionar los componentes de la aplicación que desea instalar en su equipo. De manera predeterminada, se seleccionará todos los componentes de la aplicación para su instalación: protección, análisis y actualización.

Para decidir qué componentes no desea instalar, consulte una breve descripción de cada uno. Seleccione el componente en la lista y lea la descripción asociada en el campo inferior. La información contiene una descripción breve del componente y los requisitos de espacio libre en disco para su instalación.

Para cancelar la instalación de cualquier componente, abra el menú contextual pulsando 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 pulsando 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, pulse el botón **Siguiente**. Para regresar a la lista predeterminada de componentes para instalar, pulse el botón **Borrar**.

PASO 8. BÚSQUEDA DE OTROS PROGRAMAS ANTIVIRUS

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

Si los detecta en su equipo, la lista de estos programas aparecerá en la 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.

Si la lista de programas antivirus detectados contiene Kaspersky Lab 7.0, guarde el archivo llave de esta aplicación antes de eliminarla. Podrá utilizar esta llave para la versión nueva de la aplicación. También le recomendamos guardar los objetos almacenados en cuarentena y en la zona de respaldo; estos objetos son automáticamente desplazados a la cuarentena de la nueva versión donde podrá administrarlos después de la instalación.

Si elimina automáticamente la versión 7.0, se guardará la información de activación para utilizarla durante la instalación de la versión 2009.

Advertencia!

La aplicación acepta los archivos llave de las versiones 6.0 y 7.0. Las llaves utilizadas para aplicaciones de la versión 5.0 no son compatibles.

Para continuar con la instalación, pulse el botón **Siguiente**.

PASO 9. PREPARACIÓN FINAL DE LA INSTALACIÓN

En este paso, puede proceder a la preparación final 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 42) recomendamos no desactivar la casilla **Activar la Autoprotección antes de instalar** durante la instalación inicial. De esta manera, si la opción de protección del módulo está activada y ocurre un error durante la instalación, se asegura una correcta reversión del procedimiento de instalación. Cuando vuelva a intentar la instalación, recomendamos desactivar esta casilla.

Nota:

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

Para continuar con la instalación, pulse el botón **Siguiente**. Tras esto, se iniciará 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 la aplicación incluye componentes para interceptar el tráfico de red. La mayoría de las conexiones terminadas serán restauradas automáticamente tras un breve tiempo.

PASO 10. FIN DE LA INSTALACIÓN

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

Si es necesario reiniciar el equipo para completar correctamente la instalación, aparecerá un aviso correspondiente en pantalla. Después de reiniciar, el Asistente de instalación se reanudará automáticamente.

Si no es necesario reiniciar el sistema para completar la instalación, pulse el botón **Siguiente** para iniciar el *Asistente de configuración* de la aplicación.

INTERFAZ DEL PROGRAMA

La aplicación posee una interfaz sencilla y fácil de usar. Este capítulo describe en detalle sus características básicas.

Además de la interfaz principal del programa, existen complementos para Microsoft Office Outlook (análisis antivirus y antispam), Microsoft Outlook Express (Windows Mail), The Bat! (análisis antivirus y antispam), Microsoft Internet Explorer y Microsoft Windows Explorer. Los complementos amplían las características de las aplicaciones indicadas y permiten administrar y configurar los componentes Antivirus de correo y chat y Antispam desde su interfaz.



EN ESTA SECCIÓN:

Icono del área de notificaciones	46
Menú contextual	47
Ventana principal de la aplicación	49
Notificaciones	52
Ventana de configuración de la aplicación	52

ICONO DEL ÁREA DE NOTIFICACIONES

Tras instalar la aplicación, el icono de la aplicación aparecerá en el área de notificaciones de la barra de tareas de Microsoft Windows.

Este icono es un indicador del funcionamiento de la aplicación. Refleja el estado de protección y muestra un número de funciones básicas realizadas por el programa.

Si el icono está activo  (color), la protección está completamente activa o algunos de sus componentes 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:



– Correo en curso de análisis.



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



– Debe reiniciar el equipo para aplicar las actualizaciones.




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

El icono también permite acceder a las funciones en la interfaz de la aplicación: el menú contextual (ver sección "Menú contextual" en la página 47) y la ventana principal de la aplicación (ver sección "Ventana principal de la aplicación" en la página 49).

Para abrir el menú contextual, pulse el botón derecho en el icono de la aplicación.

Para abrir la ventana principal de la aplicación, pulse dos veces el icono de la aplicación. La ventana principal del programa 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 . Pulse dos veces el icono para mostrar las noticias en la ventana de respuesta.

MENÚ CONTEXTUAL

Puede ejecutar tareas de protección básica desde el menú contextual.

El menú de la aplicación contiene los elementos siguientes:

- **Actualización:** ejecuta la actualización de las bases de datos y de los módulos de la aplicación, y los instala en su equipo.
- **Análisis completo del equipo:** ejecuta un análisis completo del equipo en busca de objetos peligrosos. Se analizan los archivos en 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 e iniciar un análisis antivirus.

- **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 del programa" en la página 49).
- **Configuración:** examinar y configurar los componentes de la aplicación.
- **Activar:** activa el programa. Para beneficiarse de la condición de usuario registrado, debe activar su aplicación. Esta opción de menú sólo está disponible si el programa no está activado.
- **Acerca de:** abre una ventana con información acerca de la aplicación.
- **Suspender la protección / Reanudar la protección:** desactiva temporalmente o activa los componentes de protección en tiempo real. Esta opción del menú no afecta a las actualizaciones del producto 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, vuelva a seleccionar este ítem desde el menú contextual.
- **Salir:** cierra la aplicación (al seleccionar esta opción, la aplicación se descarga de la RAM del equipo).



Figura 1: Menú contextual

Cuando 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 el estado de la tarea en curso.

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 posibles de protección y 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 advierten sobre la presencia de amenazas a la seguridad de la configuración o del funcionamiento de la aplicación. Además de los programas nocivos, también se consideran amenazas las bases de datos obsoletas de la aplicación, los componentes de protección desactivados, la selección de parámetros mínimos, etc.

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

- La parte izquierda de la ventana - panel de navegación - sirve para acceder rápidamente a cualquier función de la aplicación, ejecución de tarea de análisis antivirus, tarea de actualización, etc.

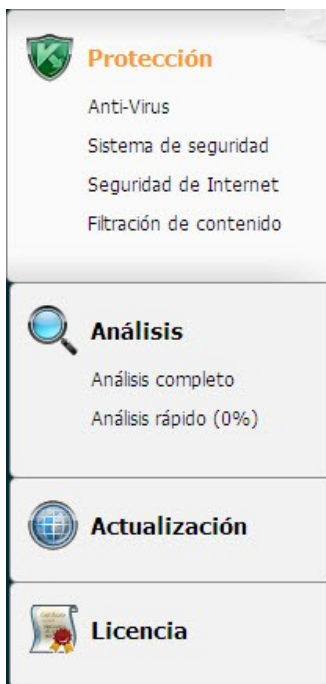


Figura 3: Parte izquierda de la ventana principal

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



Figura 4: Parte informativa de la ventana principal

También puede utilizar los botones:

- **Configuración:** para acceder a la configuración de la aplicación.
- **Ayuda:** para abrir el sistema de ayuda de la aplicación.
- **Detectados:** para abrir la lista de objetos dañinos detectados como resultado de la actividad de cualquier componente o tarea de análisis antivirus, y visualizar estadísticas detalladas de la actividad de la aplicación.
- **Informes:** para abrir la lista de eventos ocurridos durante el funcionamiento de la aplicación.
- **Asistencia técnica:** abre la ventana con información acerca del sistema y vínculos hacia recursos de información de Kaspersky Lab (sitio del Servicio de Asistencia técnica, foro).

Nota:

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

NOTIFICACIONES

Si se produce algún evento durante el funcionamiento de la aplicación, aparecerán 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 cuanto a 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 de una actividad peligrosa en su sistema. Conviene decidir de inmediato cómo debe reaccionar el programa. 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. Instruya al programa en función del peligro relacionado con este evento. Este tipo de notificación aparece en amarillo.
- **Nota:** Esta notificación le informa sobre eventos no críticos. Este tipo, por ejemplo, incluye notificaciones relativas al funcionamiento del componente **Filtración de Contenidos**. Las notificaciones informativas son de color 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 49) o el menú contextual (sección "Menú contextual" en la página 47) de la aplicación. Para abrir esta ventana, active 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 tiene de dos partes:

- La parte izquierda de la ventana da acceso a los componentes de la aplicación, tareas de análisis antivirus, tareas de actualización, etc.;
- La parte derecha de la ventana contiene la lista de parámetros del componente, tarea, etc. seleccionado 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. Esto hace posible que un usuario con cualquier nivel de conocimientos informáticos pueda proteger su equipo correctamente después de su instalación, sin perder horas en configurarlo.

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 el programa. 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 con programas nocivos antes de instalar la aplicación. Para detectar programas nocivos, ejecute un análisis del equipo (sección "Escaneo Anti-Virus del equipo" en la página 57).

Como consecuencia de una actuación nociva o de fallos en el sistema, la configuración de su equipo puede resultar dañada. Ejecute el Asistente de análisis de seguridad para encontrar vulnerabilidades en las aplicaciones instaladas o anomalías en la configuración del sistema.

Es posible que en ese momento, las bases de datos de la aplicación incluidas en el paquete de bases de datos estén desactualizadas. Inicie la actualización de la aplicación (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 autoaprendizaje 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 anteriores, la aplicación estará lista para funcionar. Para evaluar el nivel de protección de su equipo, utilice el Asistente de administración de seguridad (sección "Administración de la seguridad Management" en la página 63).

EN ESTA SECCIÓN:

Selección del tipo de red	55
Actualización de la aplicación.....	56
Análisis de seguridad.....	56
Análisis del equipo en busca de virus	57
Administración de la licencia	58
Suscripción para la renovación automática de licencias	59
Participación en Kaspersky Security Network	61
Administración de la seguridad.....	63
Suspensión de la protección	65

SELECCIÓN DEL TIPO DE RED

Después de instalar la aplicación, el componente Firewall analizará las conexiones de red activas en su equipo. A cada conexión de red se le atribuye un estado que determina qué actividades de red están 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: estado para conexiones de red en las que no se autoriza el acceso al equipo desde el exterior. Para estas redes, el acceso a carpetas públicas e impresoras también está autorizado. Este es el estado recomendado para redes Internet.
- Red local: estado para conexiones de red en las que se autoriza el acceso a carpetas públicas e impresoras de red. Le recomendamos atribuir este estado a las redes locales protegidas, por ejemplo, una red corporativa.

- Red de confianza: estado para conexiones de red en las que cualquier actividad está autorizada. La atribución de este estado sólo está recomendada para zonas absolutamente seguras.

Para cada estado de red, Kaspersky Internet Security incluye el 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, en el momento de instalar la aplicación, es posible que las bases de datos hayan quedado obsoletas, ya que Kaspersky Lab actualiza éstas y los módulos de aplicación con regularidad.

Es posible seleccionar el modo de ejecución de la actualización con el Asistente de configuración de la aplicación. De forma predeterminada, Kaspersky Internet Security busca automáticamente las actualizaciones en los servidores de Kaspersky Lab. Si el servidor contiene actualizaciones recientes, Kaspersky Internet Security 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 manualmente,
 1. Abra la ventana principal de aplicación.
 2. Seleccione la entrada **Actualizar** en la parte izquierda de la ventana.
 3. Pulse el botón **Iniciar la actualización**.

ANÁLISIS DE SEGURIDAD

Como consecuencia de actividades no deseadas en su equipo causadas por fallas en el sistema o por la actuación de programas nocivos, la configuración de su sistema operativo puede resultar dañada. Adicionalmente, las aplicaciones instaladas en su equipo pueden presentar vulnerabilidades que los intrusos pueden aprovechar para causar daños a su equipo.

Para detectar y eliminar estos problemas de seguridad, los expertos de Kaspersky Lab recomiendan ejecutar el Asistente para el análisis de seguridad después de instalar la aplicación. El Asistente de análisis de seguridad 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 DEL EQUIPO EN BUSCA DE VIRUS

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

Una vez instalada en el equipo, la aplicación ejecuta automáticamente la tarea **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 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. Pulse **Iniciar análisis** para iniciar el análisis. Si necesita detener la ejecución de la tarea, pulse **Detener análisis** durante el funcionamiento de la tarea.

ADMINISTRACIÓN DE LA LICENCIA

La aplicación necesita una llave de licencia para funcionar. Al adquirir el programa se le hará entrega dicha llave. Esta llave le otorga a Ud. el derecho de usar el programa desde el momento en que lo adquiere e instala la llave.

Sin una llave de licencia, y a menos que se trate de una versión de prueba, la aplicación se ejecutará en el modo que sólo permite una sola actualización. La aplicación no podrá descargar ninguna otra actualización posterior.

Si se activó una versión de prueba, la aplicación dejará de funcionar cuando expire el periodo de prueba.

Al expirar la llave de licencia, el programa seguirá funcionando con la excepción de que ya no podrá actualizar las bases de datos. Al igual que antes, Ud. podrá realizar análisis antivirus de su equipo y también podrá seguir usando los componentes de protección, pero sólo con las bases de datos disponibles en el momento de expirar la licencia. No podemos garantizarle que estará protegido contra virus que surjan después de la expiración de la licencia.

Para proteger su equipo contra infecciones causadas por nuevos virus, le recomendamos renovar su llave de licencia. La aplicación le avisará con una antelación de dos semanas antes de la expiración de la llave. Por algún tiempo un mensaje en este sentido aparecerá cada vez que se inicie la aplicación.

La información sobre la actual llave aparece en la sección Licencia en la ventana principal de la aplicación: identificación y tipo (comercial, suscripción comercial, prueba, prueba beta) de la aplicación, número de equipos en los que puede instalarse esta llave, fecha de expiración y número de días restantes de vigencia de la licencia. No se mostrará información sobre la expiración de la llave si se encuentra instalada una licencia comercial con suscripción (ver sección "Suscripción para la renovación automática de licencias", en la página 2).

Para acceder al contrato de licencia de la aplicación, pulse el botón **Ver Contrato de licencia para el usuario final**. Para eliminar una llave de la lista, pulse el botón **Eliminar**.

Para adquirir o renovar una licencia:

1. Para adquirir una nueva llave, pulse el botón **Adquirir licencia** (si la aplicación todavía no se ha activado) o **Renovar licencia**. La ventana que se abrirá contiene toda la información para adquirir una llave a través de la tienda en línea de Kaspersky Lab o de sus partners. Si Ud. Elige realizar la compra por Internet, se le enviará un archivo llave o un código de activación a la dirección de correo electrónico que Ud. especificó en el formulario tras realizar el pago.
2. Para instalar la llave, pulse el botón **Instalar llave** que se encuentra en la sección Licencia en la ventana principal de la aplicación o use el comando **Activación** ubicado en el menú principal de la aplicación. Se activará el Asistente de activación.

Nota

Kaspersky Lab ofrece de manera regular ofertas especiales de precios para la ampliación de licencias para nuestros productos. Conozca estas ofertas en el sitio web de Kaspersky Lab en el área **Productos → Ventas y ofertas especiales**.

SUSCRIPCIÓN PARA LA RENOVACIÓN AUTOMÁTICA DE LICENCIAS

Si cuenta con la suscripción para la renovación automática de licencias, la aplicación se contactará automáticamente con el servidor de activación en determinados intervalos de tiempo para mantener la vigencia de su licencia durante todo el periodo de suscripción.

Si la actual licencia ya expiró, Kaspersky Anti-Virus verificará, en segundo plano, la disponibilidad de una llave actualizada en el servidor, y si encuentra dicha llave, la aplicación la descargará e instalará en el anterior modo de reemplazo de llaves. De esta manera, la licencia se renovará sin que Ud. tenga que intervenir. Si además expiró el periodo de tiempo durante el cual la licencia se renueva, se la puede renovar de forma manual. Durante el lapso de tiempo en que se permite la renovación se mantendrá la funcionalidad de la aplicación. Tras el vencimiento de este plazo, y si no se renovó la licencia, la aplicación ya

no instalará las actualizaciones de las bases de datos. Para rechazar la suscripción de la renovación automática de licencias, póngase en contacto con nuestra tienda en línea de la que adquirió la aplicación.

Advertencia!

Si para el momento de su activación la aplicación ya está activada mediante una licencia comercial, esta licencia se reemplazará con una llave de suscripción. Si Ud. desea volver a utilizar la licencia comercial, debe eliminar la llave de suscripción y volver a activar la aplicación con el código de activación que se le hizo llegar al obtener la llave comercial.

La condición de suscripción se caracteriza por los siguientes estados:

1. *Dañado.* Su petición para activar la suscripción aún no se procesó (se necesita de un tiempo para procesar una petición en el servidor). Kaspersky Anti-Virus opera en un modo de completa funcionalidad. Si después de cierto tiempo la petición de suscripción aún no se procesó, se le notificará al respecto. En este caso, las bases de datos de la aplicación ya no podrán actualizarse.
2. *Activación.* La suscripción para la renovación automática de licencias se activó por un periodo de tiempo ilimitado (no se especifica una fecha) o por un determinado periodo de tiempo (se especifica la fecha de expiración de la suscripción).
3. *Renovada.* La suscripción se renovó de manera automática o manual por un periodo de tiempo, ilimitado (no se especifica una fecha) por un determinado periodo de tiempo (se especifica la fecha de expiración de la suscripción).
4. *Error.* Hubo un error en la renovación de la suscripción.
5. *Expiró.* El periodo de suscripción llegó a su vencimiento. Ud. puede usar otro código de activación o renovar su suscripción contactándose con nuestra tienda en línea de la que adquirió la aplicación.
6. *Cancelación de la suscripción.* Ud. canceló la suscripción para la renovación automática de licencias.
7. *Actualización requerida.* Por alguna razón no se recibió a tiempo la llave para renovar la suscripción. Active el **Estado de renovación de la suscripción** para renovar la suscripción.

Si expiró el periodo de vigencia de la suscripción, así como el periodo adicional durante el cual se permite renovar la licencia (estado de suscripción – *Expiró*), la aplicación le notificará al respecto y cesarán sus intentos de obtener una llave actualizada del servidor. La funcionalidad de la aplicación se mantendrá, a excepción de la actualización de las bases de datos de la aplicación.

Si por alguna razón no se renovó la licencia (estado de suscripción – *Es necesario actualizar*) a tiempo (por ejemplo, el equipo estaba apagado durante todo el tiempo en que la renovación de la licencia estaba disponible), Ud. puede renovar su estado de forma manual, pulsando el botón **Estado de renovación de la suscripción**. Kaspersky Anti-Virus no actualizará las bases de datos de la aplicación hasta que se renueve la suscripción.

Mientras la suscripción se encuentra vigente, no es posible instalar llaves de otro tipo ni usar otros códigos de activación para renovar la licencia. Sólo se podrá utilizar otro código de activación cuando concluya el periodo de vigencia de la suscripción (estado de suscripción – *Expiró*).

Advertencia!

Al utilizar su suscripción para la renovación automática de licencias, si vuelve a instalar la aplicación en su equipo, necesitará activar el producto manualmente de nuevo usando el código de activación que se le entregó al momento de adquirir la aplicación.

PARTICIPACIÓN EN KASPERSKY SECURITY NETWORK

Todos los días, aparece un gran número de nuevas amenazas en todo el mundo. Para facilitar la recolección de datos estadísticos sobre los tipos y orígenes de nuevas amenazas y desarrollar métodos para su eliminación, Kaspersky Lab le ofrece su servicio Kaspersky Security Network.

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

- Un identificador único que la aplicación le asigna a su equipo. Se trata de un identificador de la configuración del hardware de su equipo y no contiene ninguna otra información.

- Información sobre amenazas detectadas por los componentes de la aplicación. La organización y el contenido de la información dependen del tipo de la amenaza detectada.
- Información del sistema: versión del sistema operativo, Service Pack instalados, servicios y controladores descargables, versiones de clientes de correo y navegadores, extensiones del navegador, número de aplicaciones Kaspersky Lab instaladas.

Kaspersky Security Network también recopila datos estadísticos ampliados con información sobre:

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

La información estadística se envía al finalizar la aplicación actualizada.

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 datos estadísticos:
 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 servicio Kaspersky Security Network. Active la casilla **Acepto enviar estadísticas avanzadas dentro del marco de Kaspersky Security Network** para confirmar que acepta enviar 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. Si aparece 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 que se han producido, su descripción y sus posibles soluciones en la ficha **Estado** (ver figura siguiente) que se abre desde el vínculo **Reparar ahora** (ver figura anterior).

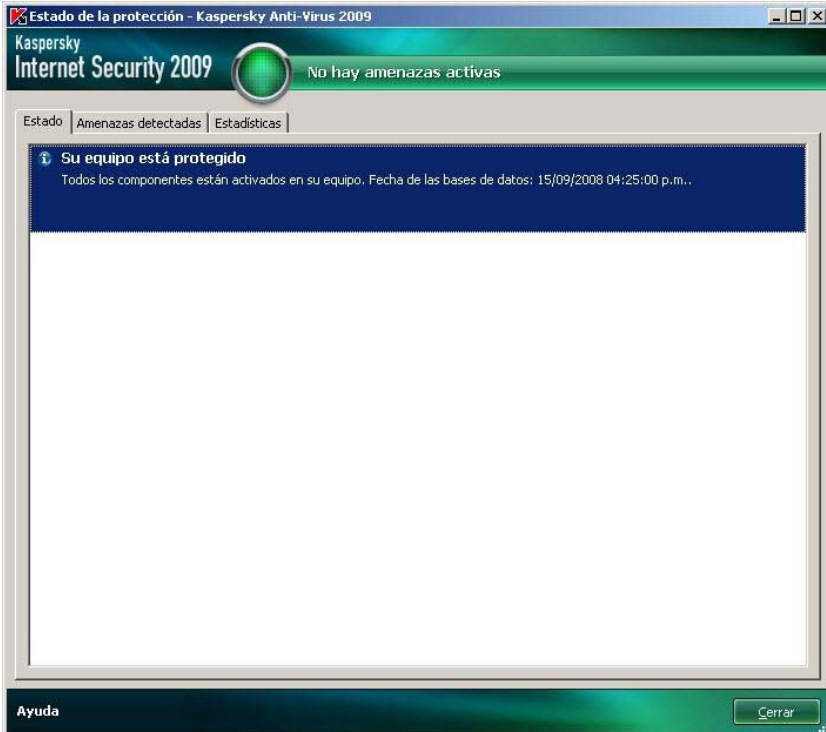


Figura 6: Solución de problemas de seguridad

Puede ver la lista de problemas existentes. Los problemas se encuentran organizados en base a la urgencia de su resolución: Primero, los problemas más críticos, es decir, los problemas con el icono de estado en rojo; después, lo menos importantes, con el icono de estado en amarillo; por último, los mensajes informativos. Se proporciona una descripción detallada de cada problema y las siguientes acciones están disponibles:

- **Eliminar inmediatamente.** Con los botones correspondientes, puede solucionar la amenaza, aplicando la acción recomendada.
- **Posponer la eliminación.** Si, por cualquier motivo, no fuera posible eliminar inmediatamente el problema, puede postergar la acción para más tarde. Para ello pulse el botón **Ocultar mensaje**.

Nótese que esta opción no está disponible para problemas graves. Estos problemas incluyen, por ejemplo, objetos nocivos que no fueron desinfectados, bloqueo de alguno o de varios componentes o daños en archivos del programa.

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:
 4. Seleccione la entrada **Suspender la protección** en el **menú contextual** de la aplicación (sección "Menú contextual" en la página 47).
 5. En la ventana abierta **Suspender la protección**, indique después de cuánto tiempo desea volver a activar 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 que tenga activado el inicio de la aplicación junto con el equipo).
 - **Manualmente**: la protección sólo se activará si Ud. interviene. 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 notificación" en la página 46) en la barra de sistema.

- Color rojo del icono indicador de estado y del panel de la ventana principal de la aplicación.

Si existían conexiones de red cuando se suspendió la protección, aparecerá una notificación informando sobre 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	67
Prueba de protección del tráfico HTTP	71
Prueba de protección del tráfico SMTP	71
Validación de los parámetros del Antivirus de archivos y memoria.....	72
Validación de los parámetros de la tarea de análisis antivirus.....	73
Validación de los parámetros del componente Antispam	73

PRUEBA CON EL "VIRUS" EICAR Y SUS MODIFICACIONES

Este "virus" fue especialmente diseñado por el  European Institute for Computer Antivirus Research con el fin de realizar pruebas con productos antivirus.

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

Advertencia!

¡Nunca utilice un virus real para hacer pruebas de funcionamiento de su antivirus!

Puede descargar este virus de prueba del sitio Internet oficial de la organización EICAR: 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 las variantes del "virus" de prueba estándar para comprobar el buen funcionamiento de la aplicación. Para cambiar el contenido del "virus" estándar, agregue alguno de los prefijos siguientes (ver cuadro a continuación). Para crear variantes 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 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 contiene los prefijos que deben insertarse delante de la cadena del "virus" de prueba estándar. La segunda columna enumera los posibles valores de estado que el antivirus le atribuye al objeto, de acuerdo con los resultados del análisis. La tercera columna informa acerca del procesamiento aplicado a objetos con el estado especificado por la aplicación. Observe que las acciones aplicadas a los objetos dependerán de los parámetros de la aplicación.

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

Tabla 6. Modificaciones del "virus" de prueba

Prefijo	Estado del objeto	Información del 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 cuando se intenta desinfectar el objeto; se aplicará la acción asociada para objetos que no se pueden neutralizar.
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 el código de un virus desconocido. No se puede neutralizar.	El analizador heurístico de códigos detecta el objeto como sospechoso. En el momento de la detección, las bases de datos de firmas de amenazas del antivirus no contienen ningún tratamiento para este objeto. Aparecerá una notificación cuando se detecte este tipo de objetos.
SUSP-	Sospechoso. Objeto sospechoso que contiene el código modificado de un virus conocido. No se puede neutralizar.	La aplicación detectó una correspondencia parcial de una sección del código del objeto, con la sección de un virus conocido. En el momento de la detección, las bases de datos de firmas de amenazas del antivirus no contienen ningún tratamiento para este objeto. Aparecerá una notificación cuando se detecte este tipo de objetos.

Prefijo	Estado del objeto	Información del procesamiento del objeto
ERRO-	Error de análisis:	<p>Ocurrió un error durante el análisis de un objeto. La aplicación no pudo acceder al objeto: El programa no tiene acceso al objeto, porque la integridad del objeto está dañada (por ejemplo, no se encuentra el final de un archivo multivolumen) o porque no es posible conectarse 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.</p>
CURE-	<p>Infectado. Objeto infectado que contiene el código de un virus conocido. Se puede desinfectar.</p>	<p>El objeto contiene un virus que es posible neutralizar. La aplicación neutralizará el objeto; el contenido del cuerpo del "virus" se reemplazará por la palabra CURE. Aparecerá una notificación cuando se detecte este tipo de objetos.</p>
DELE-	<p>Infectado. Objeto infectado que contiene el código de un virus conocido. No se puede neutralizar.</p>	<p>La aplicación identifica el objeto como un virus que no se puede desinfectar.</p> <p>Ocurre un error cuando se intenta desinfectar el objeto; se aplicará la acción asociada para objetos que no se pueden neutralizar.</p> <p>Aparecerá una notificación cuando se detecte este tipo de objetos.</p>

PRUEBA DE PROTECCIÓN DEL TRÁFICO HTTP

- ▶ Para comprobar la detección de virus en el flujo de datos transmitido a través del protocolo HTTP, haga lo siguiente:

Puede descargar este virus de prueba del sitio Internet oficial de la organización EICAR: http://www.eicar.org/anti_virus_test_file.htm.

Cuando 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 termina y el navegador muestra un mensaje informándole que este objeto está infectado con el virus EICAR-Test-File.

PRUEBA DE PROTECCIÓN DEL TRÁFICO SMTP

Para detectar virus dentro de los flujos de datos recibidos a través del protocolo SMTP, puede 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 salientes, incluyendo el cuerpo de los mensajes y los adjuntos. Para probar la detección de virus en el cuerpo del mensaje, copie el texto de un "virus" de prueba estándar o modificado dentro del cuerpo del mensaje.

- ▶ *Para ello:*

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 se analizará si se 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 y lo identifica como infectado. El envío del mensaje con un objeto infectado se bloqueará.

VALIDACIÓN DE LOS PARÁMETROS DEL ANTIVIRUS DE ARCHIVOS Y MEMORIA

- ▶ Para comprobar que la configuración del componente Antivirus de archivos y memoria es correcta, haga lo siguiente:
 1. Cree una carpeta en un disco, copie en ella el virus de prueba descargado desde el sitio Internet oficial del organismo (http://www.eicar.org/anti_virus_test_file.htm) así como las modificaciones del virus de prueba que haya creado.
 2. Autorice 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 su versión modificada.

El componente Antivirus de archivos y memoria interceptará la llamada, analizará el archivo y aplicará la acción especificada en la configuración. 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 sea correcta, haga lo siguiente:
 1. Cree una carpeta en un disco, copie en ella el virus de prueba descargado desde el sitio Internet oficial del organismo (http://www.eicar.org/anti_virus_test_file.htm) así como las modificaciones del virus de prueba que haya creado.
 2. Cree una nueva tarea de análisis antivirus e incluya la carpeta que contiene el conjunto de "virus" de prueba dentro de la cobertura.
 3. Autorice el registro de todos los eventos para que archivo de informe muestre información acerca de los objetos dañados o no analizados por causa de errores.
 4. Ejecute la tarea de análisis antivirus.

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

Puede examinar los resultados completos de la tarea en el informe correspondiente.

VALIDACIÓN DE LOS PARÁMETROS DEL COMPONENTE ANTISPAM

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.
```

Después de recibir este mensaje en el equipo, la aplicación lo analiza, le atribuye el estado de correo no deseado 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 NUESTRAS APLICACIONES. AL SEGUIR UTILIZANDO LAS APLICACIONES 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 cualquier momento, previa publicación de las modificaciones en esta misma página. Compruebe la fecha de revisión a continuación para determinar si este acuerdo se modificó desde la última vez que lo leyó. La utilización continuada de cualquiera de los Servicios de Kaspersky Lab después de la publicación de las modificaciones a la Declaración de recolección de datos significa su aceptación de estas modificaciones.

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

Acerca de Kaspersky Lab

Kaspersky Lab tiene el sólido compromiso de ofrecer servicios de calidad a todos sus clientes y en particular, en lo relacionado con sus preocupaciones sobre 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 preparamos esta declaración 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 los principales procesos y áreas, 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 mensaje 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, y 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, relacionados con los 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 nocivos.** 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, Ud. 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 se pueden utilizar 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 se mencionara 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 al

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 los 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. La 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, servicios, extensiones para Internet Explorer, extensiones de impresión, extensiones para 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 el número de versión del producto de Kaspersky Lab que normalmente no permite la identificación personal;

- Identificador exclusivo generado por el producto de Kaspersky Lab para identificar equipos individuales sin identificar al usuario y que no contiene ningún dato de carácter personal;
- Información sobre el estado de la protección antivirus de su equipo, así como datos sobre cualquier archivo o actividad sospechosa de ser un programa nocivo (nombre del virus, 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 nociva). Observe que los datos recolectados antes enumerados no contienen ninguna información que permita la identificación personal.

Datos ampliados

- Información de aplicaciones firmadas que el usuario descarga (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 sólo personal autorizado tienen acceso a los datos recolectados. Kaspersky Lab toma todas las medidas necesarias para asegurar un tratamiento seguro de su información, de acuerdo con esta Declaración. Por desgracia, 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 de

que esta información, en caso de ser transferida, reciba 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 en el 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 será 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 promocionales 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 nocivos, sitios Internet 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.

Divulgación 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 obligatorio. 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 Compañía, las protecciones de seguridad de nuestros usuarios y del público, o los acuerdos de confidencialidad y licencia con aquellas terceras partes que contribuyan 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 soluciones de seguridad. Kaspersky Lab también podrá 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 de la aplicación de 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 los servicios a los que se suscribieron 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 Ud. por motivos legales o razones importantes para Ud. Estos derechos no nos autorizan a ponernos en contacto con Ud. con ofertas comerciales de servicios nuevos o existentes, si no optó por recibirlos, y en cualquier caso este tipo de comunicaciones es poco frecuente.

CONSULTAS Y QUEJAS RELACIONADAS CON LA RECOLECCIÓN DE DATOS

En Kaspersky Lab, admitimos y tratamos las consultas de los usuarios acerca de la Recolección de datos con el mayor respeto y la mayor atención. Si Ud. considera 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. support@kaspersky.com.

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

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

Copyright (c) 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. Fabrica un amplio conjunto de soluciones de seguridad y protección de datos: antivirus, antispam y sistemas antifraude.

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

Actualmente, Kaspersky Lab emplea más de 450 especialistas altamente cualificados, de los cuales 10 poseen una Maestría, y 16 un Doctorado. Los expertos Senior de Kaspersky Lab son miembros de la CARO (Computer Antivirus Internet Researchers Organization).

Nuestros más preciados valores empresariales son el conocimiento y la experiencia acumulados por nuestros especialistas durante estos catorce años de lucha incesante contra los virus informáticos. Mediante un análisis en profundidad del comportamiento de los virus informáticos, los especialistas de nuestra compañía son capaces de anticipar las tendencias del código nocivo y proporcionar así a nuestros usuarios una protección rápida contra nuevos tipos de ataques. La resistencia a ataques futuros es la directiva básica de todos los productos Kaspersky Lab. Constantemente, nuestros productos superan a los de otras marcas a la hora de asegurar una cobertura antivirus.

Años de duro trabajo nos convirtieron en uno de los desarrolladores líderes de soluciones de seguridad. Kaspersky Lab fue una de las primeras empresas de este tipo en desarrollar los mejores estándares 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 adaptadas y de sencilla administración ofrecen el máximo grado de automatización de la protección antivirus de los equipos y redes empresariales. Numerosos fabricantes conocidos utilizan el núcleo de Kaspersky Anti-Virus. En la lista de estas organizaciones encontramos a Nokia ICG (EE.UU.), F-Secure (Finlandia), Aladdin (Israel), Sybari (EE.UU.), G Data (Alemania), Deerfield (EE.UU.), Alt-N (EE.UU.), Microworld (India) y BorderWare (Canadá).

Los clientes de Kaspersky Lab se benefician de una amplia oferta de servicios adicionales que garantizan no sólo un funcionamiento estable de nuestros productos sino también la compatibilidad con cualquier necesidad específica 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.

EN ESTA SECCIÓN:

Otros productos de Kaspersky Lab

..... 83

Cómo encontrarnos 93

OTROS PRODUCTOS DE KASPERSKY LAB

Kaspersky Lab News Agent

El Agente de noticias (News Agent) sirve para comunicar rápidamente noticias de Kaspersky Lab, notificaciones acerca del "clima viral" y los últimos eventos. La aplicación consulta la lista de canales de noticias y la información que contienen en el servidor de noticias de Kaspersky Lab a intervalos especificados.

Adicionalmente, el Agente de noticias permite:

- visualizar el "clima viral" en la barra del sistema;
- suscribirse o cancelar la suscripción a los canales de noticias de Kaspersky Lab;
- recibir las noticias de cada canal suscrito a intervalos seleccionados; asimismo, está prevista la posibilidad de recibir notificaciones acerca de nuevas noticias aún sin leer;
- leer las noticias de los canales de suscripción;

- mostrar la lista y el estado de los canales;
- abrir páginas en el navegador con el detalle de la noticia.

El Agente de noticias es una aplicación que se ejecuta con Microsoft Windows, y puede usarse de forma independiente o integrada en soluciones ofrecidas por Kaspersky Lab.

Kaspersky® Online Scanner

Este programa es un servicio gratuito para visitantes del sitio Internet de nuestra compañía, y ofrece un eficiente análisis antivirus en línea de su equipo. Kaspersky OnLine Scanner se ejecuta en el navegador. De este modo, los usuarios pueden recibir rápidamente una respuesta a sus preguntas acerca de una infección causada por un código nocivo. Durante el análisis, el usuario puede:

- Excluir del análisis los archivos comprimidos y las bases de datos de correo.
- Seleccionar bases de datos estándar o ampliadas para realizar el análisis.
- Guardar un informe con los resultados del análisis en formato txt o html.

Kaspersky® OnLine Scanner Pro

Este programa es un servicio a suscriptores disponible para visitantes del sitio Internet de nuestra compañía, que ofrece un análisis antivirus eficiente de su equipo y la desinfección de archivos peligrosos, en línea. Kaspersky OnLine Scanner Pro se ejecuta directamente en el navegador. Durante el análisis, el usuario puede:

- Excluir del análisis los archivos comprimidos y las bases de datos de correo .
- Seleccionar bases de datos estándar o ampliadas para realizar el análisis.
- Desinfectar los objetos infectados detectados.
- Guardar un informe con los resultados del análisis en formato txt o html.

Kaspersky Anti-Virus ® Mobile

Kaspersky Anti-Virus Mobile ofrece protección antivirus para terminales móviles bajo sistemas operativos Symbian y Microsoft Windows Mobile. La aplicación realiza un análisis antivirus avanzado que incluye:

- Análisis a petición de la memoria interna del dispositivo móvil, de las tarjetas de memoria, de carpetas individuales o de archivos específicos. Cuando detecta un objeto infectado, lo mueve a cuarentena o lo elimina.
- Protección en tiempo real: analiza todos objetos entrantes o modificados así como los archivos abiertos;
- Protección contra SMS y MMS no deseados.

Kaspersky Anti-Virus para servidores de archivos

Este producto ofrece una protección segura de los sistemas de archivos de servidores con Microsoft Windows, Novell NetWare y Linux contra todo tipo de programas nocivos. En la composición de este producto entran siguientes las aplicaciones de Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Ventajas y prestaciones operativas:

- *Protección en tiempo real de los sistemas de archivos de servidores.* Análisis de todos los archivos del servidor al abrirse o guardarse en el servidor.
- *Prevención de epidemias virales.*
- *Análisis a petición* del sistema de archivos completo o de archivos y carpetas individuales.
- *Uso de tecnologías de optimización* cuando se analizan objetos en el sistema de archivos del servidor.
- *Restauración del sistema después de su infección.*

- Escalabilidad del programa dentro de los límites de disponibilidad de los recursos del sistema.
- *Control del equilibrio de carga del sistema.*
- *Creación de una lista de procesos de confianza*, cuyas actividades en el servidor no supervisa este producto.
- Administración remota del producto, incluyendo su instalación, configuración y administración centralizadas.
- *Conservación de copias de respaldo de objetos infectados y eliminados* en caso de ser necesaria su restauración.
- *Aislamiento de objetos sospechosos* en una zona especial.
- *Notificación sobre eventos* ocurridos durante el funcionamiento del producto, enviados al administrador del sistema.
- *Generación de informes detallados.*
- *Actualización automática* de las bases de datos del programa.

Kaspersky Open Space Security

Kaspersky Open Space Security es un paquete informático con un novedoso enfoque de la seguridad de las redes corporativas actuales, de cualquier tamaño, que ofrece protección centralizada de la información y Asistencia técnica para oficinas remotas y usuarios móviles.

Este producto incluye cuatro programas:

- Kaspersky Open Space Security.
- Kaspersky Business Space Security.
- Kaspersky Enterprise Space Security.
- Kaspersky Total Space Security.

Encontrará a continuación la descripción detallada de cada producto.

Kaspersky Work Space Security es un producto diseñado para ofrecer protección centralizada a estaciones de trabajo en redes corporativas contra todo tipo de amenazas actuales en Internet: virus, programas espía, intrusiones de piratas y correo no deseado

Ventajas y prestaciones operativas:

- Protección integral contra virus, ataques de piratas y correo no deseado.
- Defensa proactiva contra nuevos programas nocivos aún no registrados en las bases de datos.
- Cortafuegos personal con sistema para la detección de intrusiones y la prevención de ataques de red.
- Reversión de los cambios nocivos introducidos en el sistema.
- Protección contra fraudes (phishing) y correo no deseado.
- Reasignación dinámica de recursos durante el análisis completo del sistema.
- Administración remota del producto, incluyendo su instalación, configuración y administración centralizadas.
- Compatibilidad con Cisco(r) NAC (Network Admission Control);
- Análisis del correo y tráfico Internet en tiempo real.
- Bloqueo de ventanas emergentes y banners publicitarios en Internet.
- Funcionamiento seguro en cualquier tipo de red, incluso inalámbrica (WiFi).
- Herramientas de creación de discos de rescate que permiten la restauración del sistema después de un ataque viral.
- Sistema avanzado de informes acerca del estado de la protección.
- Actualizaciones automáticas de las bases de datos.
- Total compatibilidad con sistemas operativos de 64 bits.
- Optimización de las aplicaciones para portátiles (Tecnología Intel® Centrino® Duo para equipos portátiles).
- Posibilidades de desinfección remota (Tecnología de administración remota Intel® Active Management, componente Intel® vPro™).

Kaspersky Business Space Security garantiza una protección óptima de su información contra las modernas amenazas en Internet. Kaspersky Business Space Security protege las estaciones de trabajo y los servidores de archivos contra cualquier tipo de virus, troyanos y gusanos, evita

epidemias virales y asegura la información mientras los usuarios se benefician de un acceso instantáneo a los recursos de la red.

Ventajas y prestaciones operativas:

- Administración remota del producto, incluyendo su instalación, configuración y administración centralizadas.
- Compatibilidad con Cisco® NAC (Network Admission Control).
- Protección de estaciones de trabajo y servidores de archivos contra cualquier tipo de amenaza en Internet.
- Tecnología iSwift para evitar análisis repetitivos dentro de la red.
- Distribución de carga entre los procesadores del servidor.
- Aislamiento de objetos sospechosos en una zona especial;
- Reversión de los cambios nocivos introducidos en el sistema.
- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;
- Defensa proactiva de las estaciones de trabajo contra nuevos programas nocivos aún no registrados en las bases de datos.
- Análisis del correo y tráfico Internet en tiempo real.
- Cortafuegos personal con sistema para la detección de intrusiones y la prevención de ataques de red.
- Funcionamiento seguro en redes inalámbricas WiFi.
- Tecnología de autoprotección del propio antivirus contra programas nocivos.
- Aislamiento de objetos sospechosos en una zona especial.
- Actualizaciones automáticas de las bases de datos.

Kaspersky Enterprise Space Security

Este paquete informático incluye componentes para la protección de estaciones de trabajo y servidores de archivos contra cualquier tipo de amenaza moderna en Internet, elimina los virus de los flujos de correo, garantiza la seguridad de los datos y un acceso instantáneo a los recursos de la red.

Ventajas y prestaciones operativas:

- Protección de estaciones de trabajo y servidores de archivos contra cualquier tipo de virus, troyanos y gusanos.
- Protección de servidores de correo Sendmail, Qmail, Postfix y Exim.
- Análisis de todos los mensajes en el servidor Microsoft Exchange incluyendo las disco duros compartidos.
- Procesamiento de mensajes, bases de datos y otros objetos de servidores Lotus Domino.
- Protección contra fraudes (phishing) y correo no deseado.
- Prevención contra envíos masivos de correo y epidemias virales.
- Escalabilidad del paquete dentro de los límites de disponibilidad de los recursos del sistema;
- Administración remota del producto, incluyendo su instalación, configuración y administración centralizadas.
- Compatibilidad con Cisco® NAC (Network Admission Control).
- Defensa proactiva de las estaciones de trabajo contra nuevos programas nocivos aún no registrados en las bases de datos.
- Cortafuegos personal con un sistema para la detección de intrusiones y la prevención de ataques de red.
- Funcionamiento seguro en redes inalámbricas WiFi.
- Análisis del tráfico Internet en tiempo real.
- Reversión de los cambios nocivos introducidos en el sistema.
- Reasignación dinámica de recursos durante el análisis completo del sistema.
- Aislamiento de objetos sospechosos en una zona especial.
- Sistema avanzado de informes de estado del sistema de protección.
- Actualizaciones automáticas de las bases de datos.

Kaspersky Total Space Security

Esta solución supervisa todos los flujos de datos entrantes y salientes (correo, tráfico Internet y todas las comunicaciones por red). El producto cuenta con componentes que protegen estaciones de trabajo y los dispositivos móviles, garantizan un acceso instantáneo y seguro de los usuarios a los recursos de información corporativos y a Internet, y garantizan comunicaciones seguras de correo electrónico.

Ventajas y prestaciones operativas:

- Protección integral contra virus, ataques de piratas y correo no deseado en todos los niveles de la red corporativa, desde las estaciones de trabajo hasta las pasarelas.
- Defensa proactiva de las estaciones de trabajo contra nuevos programas nocivos aún no registrados en las bases de datos.
- Protección de servidores de correo y servidores compartidos.
- Análisis en tiempo real del tráfico Internet LAN (HTTP / FTP) entrante en la red local.
- Escalabilidad del paquete dentro de los límites de disponibilidad de los recursos del sistema.
- Acceso denegado a estaciones de trabajo infectadas.
- Prevención de epidemias virales.
- Informes centralizados sobre el estado de protección.
- Administración remota del producto, incluyendo su instalación, configuración y administración centralizadas.
- Compatibilidad con Cisco® NAC (Network Admission Control).
- Compatibilidad con el hardware de los servidores proxy.
- Filtrado del tráfico Internet de acuerdo con la lista de servidores de confianza, tipos de objetos y grupos de usuarios.
- Tecnología iSwift para evitar análisis repetitivos dentro de la red.
- Reasignación dinámica de recursos durante el análisis completo del sistema.
- Cortafuegos personal con un sistema para la detección de intrusiones y la prevención de ataques de red.

- Funcionamiento seguro en cualquier tipo de red, incluso inalámbrica (WiFi).
- Protección contra fraudes (phishing) y correo no deseado.
- Posibilidades de desinfección remota (Tecnología Intel® Active Management, componente Intel® vPro™).
- Reversión de los cambios nocivos introducidos en el sistema.
- Tecnología de autoprotección del propio antivirus contra programas nocivos.
- Total compatibilidad con sistemas operativos de 64 bits.
- Actualizaciones automáticas de las bases de datos.

Kaspersky Security for Mail Servers

Paquete informático para la protección de servidores de correo y servidores compartidos contra programas nocivos y correo no deseado. Este producto incluye aplicaciones para la protección de todos los servidores de correo conocidos: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix y Exim, y permite la implementación de una pasarela de correo dedicada. Esta solución incluye:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus® for Linux Mail Server

Este programa dispone de las características siguientes:

- *Protección confiable contra programas nocivos y potencialmente peligrosos.*
- *Filtrado del correo no deseado.*
- *Análisis de los mensajes entrantes y salientes y de sus adjuntos.*
- *Análisis antivirus de todos los mensajes del servidor Microsoft Exchange incluyendo disco duros compartidos.*
- *Análisis de mensajes, bases de datos y otros objetos de servidores Lotus Domino.*

- *Filtrado de mensajes* en función del tipo de adjunto.
- *Aislamiento de objetos sospechosos* en una zona especial.
- *Cómodo sistema de administración* del producto.
- *Prevención de epidemias virales*.
- *Supervisión del estado del sistema de protección* mediante notificaciones.
- Sistema de informes sobre el funcionamiento de la aplicación.
- Escalabilidad del programa dentro de los límites de disponibilidad de los recursos del sistema.
- *Actualizaciones automáticas de las bases de datos*.

Kaspersky Security for Gateways

Este producto garantiza un acceso seguro a Internet para todos los empleados de la organización, al eliminar automáticamente los programas nocivos y de riesgo dentro del flujo de datos recibidos por la red, a través de los protocolos HTTP/FTP. Esta solución incluye:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Este programa dispone de las características siguientes:

- *Protección confiable contra programas nocivos y potencialmente peligrosos*.
- *Análisis del tráfico Internet* (HTTP/FTP) en tiempo real.
- *Filtrado del tráfico Internet* de acuerdo con la lista de servidores de confianza, tipos de objetos y grupos de usuarios.
- *Aislamiento de objetos sospechosos* en una zona especial.
- *Cómodo sistema de control*.
- *Sistema de informes sobre el funcionamiento de la aplicación*.
- *Compatibilidad con el hardware de los servidores proxy*;

- Escalabilidad del programa dentro de los límites de disponibilidad de los recursos del sistema.
- *Actualizaciones automáticas de las bases de datos.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam es el primer paquete ruso utilizado para asegurar la protección de pequeñas y medianas empresas contra el correo no deseado. Este producto combina tecnologías revolucionarias de análisis lingüístico, todos los métodos modernos de filtrado del correo (incluyendo listas negras de DNS y análisis formal de los mensajes), y un conjunto exclusivo de servicios que permiten al usuario detectar y eliminar el 95% del tráfico no deseado.

Kaspersky Anti-Spam es un conjunto de filtros que actúa a la "entrada" de la red corporativa, analizando el flujo entrante en busca de mensajes no deseados. Es compatible con cualquier sistema de mensajería existente en las instalaciones del cliente, y puede instalarse en un servidor de correo existente o dedicado.

El programa consigue su alto grado de efectividad gracias a una actualización diaria automática del contenido de las bases de datos de filtrado, a partir de muestras facilitadas por los especialistas del laboratorio lingüístico. Las actualizaciones se publican cada 20 minutos.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® analiza a gran velocidad el tráfico de servidores donde se ejecutan los productos Clearswift MIMESweeper for SMTP, Clearswift MIMESweeper for Exchange o Clearswift MIMESweeper for Web.

La aplicación se presenta como un complemento o plug-in (módulo de ampliación) y realiza en tiempo real el análisis antivirus y el procesamiento del correo entrante y saliente.

CÓMO ENCONTRARNOS

Para cualquier pregunta, póngase en contacto con nuestros distribuidores o con Kaspersky Lab directamente. Se atienden consultas detalladas por teléfono o correo electrónico. Su consulta recibirá respuestas completas y detalladas.

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.m. a 7 p.m.) http://support.kaspersky.com/helpdesk.html
Servicio a usuarios corporativos:	La información de contacto se facilita después de adquirir un producto corporativo, en función del modelo de Asistencia técnica.
Foro Internet 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

FUNDACIÓN MOZILLA

La biblioteca **Gecko SDK ver. 1.8** se usó para el desarrollo de la versión 1.8 del componente de la aplicación.

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

Para mayores detalles sobre la biblioteca Gecko, visite: [http://developer.mozilla.org/en/docs/Gecko SDK](http://developer.mozilla.org/en/docs/Gecko_SDK).

© Mozilla Foundation

<http://www.mozilla.org>.

CONTRATO DE LICENCIA

Contrato estándar de licencia de usuario final

Aviso a todos los usuarios: LEA ATENTAMENTE EL SIGUIENTE CONTRATO DE LICENCIA LEGAL ("CONTRATO"), PARA KASPERSKY INTERNET SECURITY ("SOFTWARE") FABRICADO POR KASPERSKY LAB ("KASPERSKY LAB").

SI ADQUIRIÓ ESTE SOFTWARE POR INTERNET PULSANDO EL BOTÓN ACEPTAR, UD. ("PARTICULAR O ENTIDAD") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. SI NO ACEPTA TODAS LAS CONDICIONES DE ESTE CONTRATO, PULSE EL BOTÓN QUE INDICA QUE NO LOS ACEPTA Y NO INSTALE EL SOFTWARE.

SI COMPRÓ ESTE SOFTWARE EN UN MEDIO FÍSICO, Y ROMPIÓ EL ESTUCHE DEL CD, UD. ("PARTICULAR O ENTIDAD") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. SI NO ACEPTA TODAS LAS CONDICIONES DE ESTE CONTRATO NO ABRA EL ESTUCHE DEL CD NI DESCARGUE, INSTALE O UTILICE ESTE SOFTWARE.

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

EL SOFTWARE KASPERSKY DIRIGIDO A CONSUMIDORES PARTICULARES QUE NO SE HAYA ADQUIRIDO POR INTERNET NO PODRÁ SER DEVUELTO NI CAMBIADO, SALVO CLÁUSULAS 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 ésta incluye el código de activación de software proporcionado por Kaspersky Lab como parte de Kaspersky Internet Security 2009.

1. *Contrato de licencia.* Si se pagaron los gastos de licencia, y de acuerdo a las 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 documentación que la acompaña ("Documentación") únicamente para sus propios fines de negocio. Puede instalar una sola copia del Software en un solo equipo.

1.1 *Uso.* El Software está licenciado como un solo producto; no puede usarse en más de un equipo o por más de un usuario a la vez, excepto en los casos especificados en esta Sección.

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 CD ROM 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 debidas precauciones 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 bases de datos 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 se hayan borrado todas las copias del Software.

1.1.4 No deberá descompilar, realizar 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 razón, incluidos (sin limitación) razones de costos, Ud. estará autorizado a dar los pasos necesarios para lograr la interoperabilidad a condición de que sólo utilice ingeniería inversa o descompilación dentro de los límites permitidos por la ley.

1.1.5 No le está permitido ni a Ud. 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 facilitarles 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 Ud. 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 nocivos.

1.1.10 Le está permitido informar a Kaspersky Lab sobre las amenazas y vulnerabilidades potenciales de su equipo: para más detalles vea las especificaciones de la Declaración de recolección de datos. La información recopilada, en formato genérico, se utiliza únicamente para mejorar los productos Kaspersky Lab.

1.1.11 Para los fines descritos en la cláusula 1.1.10, el Software recopilará automáticamente información sobre sumas de control de archivos ejecutados en el equipo y las enviará a Kaspersky Lab.

Soporte¹.

- (i) Kaspersky Lab le proporcionará servicios de soporte ("Servicio de soporte") para el periodo definido a continuación, especificados en el Archivo llave de licencia e indicados en la ventana "Servicio", a partir de su fecha de activación en los siguientes supuestos:
 - (a) Pago de la cuota vigente de soporte, y;
 - (b) Llenado satisfactorio del Formulario de suscripción a los Servicios de soporte que acompaña a este Contrato o disponible en el sitio Internet de Kaspersky Lab, lo que requiere introducir el código de

¹ Al utilizar Software de demostración, Ud. no está autorizado ni para recurrir al Soporte técnico especificado en la cláusula 2 de este EULA, ni para vender la copia en su poder a otras partes.

Ud. está autorizado a usar el Software de demostración durante el periodo especificado en el archivo llave de licencia a partir de su activación (puede Ud. ver este periodo en la ventana "Servicio" del GUI del Software).

activación también proporcionado por Kaspersky Lab junto con este Contrato. Si usted satisface o no esta condición para el suministro de Servicios de soporte, está a la discreción absoluta de los Servicios de soporte.

El Servicio de soporte estará disponible después de la activación del Software. El Servicio de Asistencia técnica de Kaspersky Lab está también habilitado para solicitarle a Ud. 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 Asistencia técnica 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 llenar el formulario de suscripción a los Servicios de soporte.
- (iii) "Servicio de soporte" significa:
 - (a) Actualizaciones regulares de la base de datos antivirus;
 - (b) Actualizaciones de la base de datos de ataques de red;
 - (c) Actualizaciones de la base de datos antispam;
 - (d) Actualizaciones gratuitas del software, incluidas actualizaciones de la versión de antivirus;
 - (e) Asistencia técnica 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.* Ud. 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, de ninguna forma, la información confidencial 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 sean adecuados para sus necesidades, ni que 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, reparación, reemplazo o 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 (i) no se aplicará si Ud. (a) realiza o causa cualquier modificación a este Software sin autorización de Kaspersky Lab, (b) utiliza el Software de una manera no aplicable (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 Ud., 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 (incluyendo, sin limitación alguna, a condiciones implícitas, garantías u otros términos

relativos a niveles razonables de calidad, conveniencia, capacidad y cuidados 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 Ud. 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.