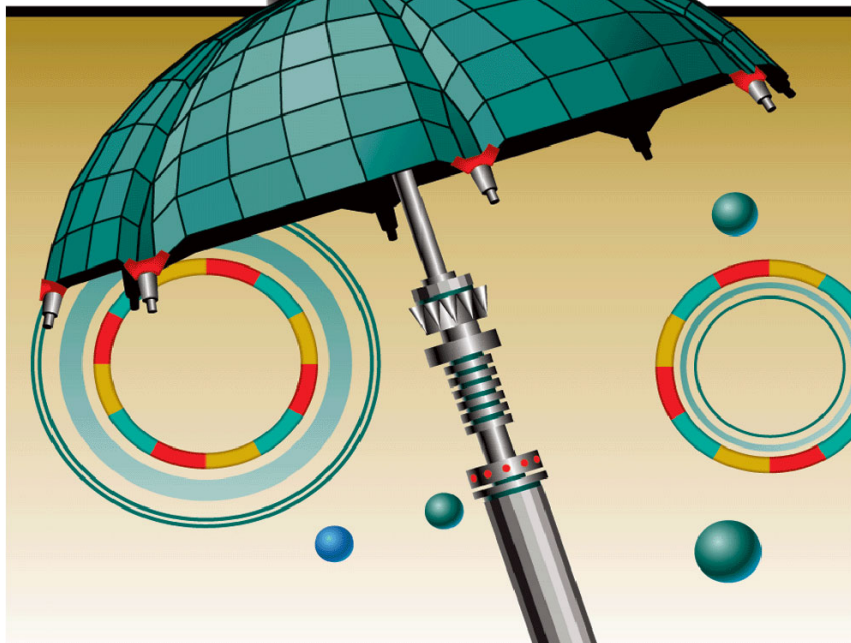


KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



KASPERSKY™



**Kaspersky Anti-Virus® 5.0
for Windows Workstations**

GUÍA DEL USUARIO

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS WORKSTATIONS

Guía del usuario

© Kaspersky Lab
<http://www.kaspersky.com>

Fecha de revisión: Octubre, 2004

Contenido

CAPÍTULO 1. VIRUS INFORMATICOS Y PROGRAMAS MALIGNOS.....	5
CAPÍTULO 2. SI SU EQUIPO ESTÁ INFECTADO... ..	7
2.1. Síntomas de infección.....	7
2.2. Qué hacer ante cualquiera de estos síntomas.....	8
2.3. Si se encontraron virus durante el análisis.....	9
2.4. Si nada lo soluciona... ..	10
2.5. Tras erradicar la infección.....	10
CAPÍTULO 3. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS....	12
3.1. Presentación del producto.....	13
3.2. Servicio para usuarios registrados.....	14
3.3. Convenciones tipográficas.....	14
CAPÍTULO 4. INTERFAZ DEL PROGRAMA.....	16
4.1. Icono de la barra del sistema.....	16
4.2. Menú contextual.....	16
4.3. Ventana principal de la aplicación: estructura general.....	17
4.3.1. <i>Ficha Protección</i>	18
4.3.2. <i>Ficha Soporte</i>	20
4.4. Ventana Analizando.....	21
4.5. Sistema de ayuda.....	22
CAPÍTULO 5. TRABAJAR CON LA APLICACIÓN.....	23
5.1. Actualización de la base antivirus y de los módulos de aplicación.....	23
5.1.1. Elección de la hora de actualización.....	23
5.1.2. Proceso de actualización.....	24
5.2. Cómo impedir una infección vírica.....	25
5.2.1. ¿Cuándo debo analizar mi equipo y objetos individuales?.....	27
5.2.2. Análisis completo.....	28
5.2.3. Análisis a petición de archivos o carpetas seleccionados.....	28
5.2.4. Analizar compilaciones de datos.....	31
5.2.5. Tratamiento diferido de objetos.....	32

5.2.6. Cómo analizar un CD o un disquete	34
5.3. Protección en tiempo real	35
5.4. Funciones avanzadas	36
5.4.1. Zonas de cuarentena y respaldo	36
5.4.1.1. Trabajar con la cuarentena.....	37
5.4.1.2. Trabajar con la zona de respaldo.....	39
5.4.2. Trabajar con informes.....	40
ANEXO A. PREGUNTAS FRECUENTES	44
ANEXO B. CONTACTO CON EL SOPORTE TÉCNICO	49
ANEXO C. GLOSARIO.....	51
ANEXO D. KASPERSKY LAB	57
D.1. Otros productos Kaspersky Lab.....	58
D.2. Cómo encontramos	62
ANEXO E. ÍNDICE.....	64
ANEXO F. CONTRATO DE LICENCIA.....	65

CAPÍTULO 1. VIRUS INFORMATICOS Y PROGRAMAS MALIGNOS

Los riesgos de infección, daños o robo de sus datos por culpa de virus informáticos ha ido creciendo a medida que aumenta el parque de equipos, junto con el número de facilidades para intercambiar datos a través del correo electrónico e Internet.

Le resultará probablemente útil saber más acerca de los diferentes tipos y funcionamiento del software dañino, con el fin de comprender mejor las amenazas que suponen para sus datos.

Es posible definir las siguientes categorías de software en función de sus manifestaciones específicas:

- **Gusanos:** el software dañino de esta categoría se copia a sí mismo en los recursos Internet. Su nombre se inspira de la capacidad de los gusanos para "propagarse" de una equipo a otro a través de redes, mensajes electrónicos y otros canales de intercambio de información. Esta característica permite a los gusanos diseminarse con una extrema rapidez.

Penetran en la memoria del equipo, calculan la dirección de red de otros equipos y transmiten duplicados de sí mismos a dichas direcciones. Además de las direcciones de red, utilizan con frecuencia la información de las libretas de direcciones de los clientes de correo. Los programas de esta categoría pueden llegar a tener archivos de trabajo en discos de sistema, pero también pueden no utilizar ningún recurso del equipo en absoluto (salvo la memoria RAM).

- **Virus:** programas que inyectan su propio código dentro del código de otros programas con el fin de infectarlos y poder tomar su control cuando se ejecutan. Esta definición simplificada no permite identificar el efecto principal de la acción de un virus: la *infección*. Los virus se propagan de forma algo más lenta que los gusanos.
- **Trojanos:** programas que actúan sin la autorización del usuario; dependiendo de ciertas condiciones, puede por ejemplo destruir los datos guardados en discos, provocar el bloqueo (el "cuelgue") del sistema, robar información confidencial, etc. Los programas que pertenecen a esta clase no son virus en el sentido tradicional del término: los trojanos no pueden penetrar en los equipos de forma independiente y son por tanto

transmitidos a través de software intruso, bajo la apariencia de aplicaciones "útiles".

Los daños causados por un troyano pueden multiplicar hasta por diez las pérdidas causadas por un virus, aunque las consecuencias de un ataque pueden ser minimizadas por un sistema de copia de respaldo adecuado.

- **Software bromista:** los programas de esa clase no dañan los equipos directamente, pero van acompañados de efectos visuales o de audio, que los usuarios no pueden desactivar.
- **Programas considerados de alto riesgo:** software legítimo que entraña riesgos por el hecho de usarlo. Por ejemplo, los programas que contienen fallos o errores de seguridad que pueden utilizarse para acceder a su equipo.

Recientemente, los gusanos se han convertido en el tipo más extendido de software dañino para los datos del equipo. Vienen después los virus y troyanos, de acuerdo con su frecuencia de aparición. Algunos programas malignos toman sus características de dos o incluso las tres categorías anteriores.

Internet y el correo electrónico son las vías principales de contagio por virus y software dañino, aunque un disquete o un CD también pueden ser causa de infección. Esta situación queda reflejada por el énfasis puesto en la protección antivirus, que va desde la exploración regular de los equipos en busca de virus, hasta un proceso más complejo de protección en tiempo real contra una infección probable.

CAPÍTULO 2. SI SU EQUIPO ESTÁ INFECTADO...

La infección del equipo por un virus o un troyano no resulta siempre evidente, incluso para un usuario experto, porque estos programas enmascaran su presencia entre otros archivos útiles. Este capítulo describe detalladamente cómo reconocer la infección, restaurar datos después de un ataque de virus, y evitar que programas dañinos penetren en su equipo.

2.1. Síntomas de infección

Un cierto número de síntomas permiten saber que su equipo ha sido infectado. Si observa alguno de los síntomas siguientes, es probable que un virus haya infectado su equipo:

- Mensajes no esperados o imágenes que aparecen repentinamente;
- Sonidos inhabituales, o música reproducida de forma aleatoria;
- La bandeja de su CDROM se abre y cierra misteriosamente;
- Algunas aplicaciones se inician repentinamente en su equipo;
- Si Kaspersky Anti-Hacker está instalado en su equipo, y recibe avisos de que algunas aplicaciones intentan conectarse a Internet sin su permiso.

Además, algunos síntomas típicos indican que la infección se ha producido a través del correo:

- Recibe avisos de que el mensaje recién enviado contenía un virus, o que su destinatario rechazó su mensaje, cuando en realidad, usted no envió este mensaje o está seguro de que dicho mensaje estaba libre de virus.
- Sus contactos reciben mensajes desde su dirección, que nunca les envió.
- Su buzón de correo contiene numerosos mensajes sin dirección de remitente ni cabecera.

Observe que estos problemas no son necesariamente síntomas de actividad vírica. Pueden tener otras causas. Por ejemplo, los mensajes infectados que provienen de su dirección pueden haber sido enviados desde otro equipo.

Si observa alguno de los síntomas siguientes, es probable que un virus haya infectado su equipo:

- Su equipo se bloquea frecuentemente o muestra presenta mensajes de error;
- Su equipo se ralentiza cuando inicia los programas;
- Sus intentos de iniciar el sistema operativo fallan.
- Los archivos y carpetas desaparecen de pronto, o sus contenidos cambian;
- Se producen accesos demasiado frecuentes a su disco duro (la luz inferior de los botones de encendido parpadean).
- Microsoft Internet Explorer "se cuelga" o se comporta de manera errática (por ejemplo, no puede cerrar la ventana de un programa).
- No consigue arrancar su equipo desde el disco duro (aparece un mensaje de error).

Tenga en cuenta que el 90% de estas situaciones corresponden a fallos de hardware o de software. El 10% restante indica sin embargo una infección posible de su equipo. En presencia de cualquiera de los síntomas descritos, le recomendamos ponerse en contacto con su administrador de sistemas y realizar un análisis completo de su equipo.

2.2. Qué hacer ante cualquiera de estos síntomas



Si observa que su equipo se comporta de forma "sospechosa":

1. ¡No se ponga nervioso! Esta regla de oro puede evitarle la pérdida de datos importantes almacenados en su equipo, y un estrés innecesario.
2. Si no consigue arrancar desde el disco duro (su equipo presenta un mensaje de error al iniciar el sistema), intente arrancar el sistema en modo a prueba de fallos o con el disquete de inicio de Windows creado cuando instaló el sistema operativo en su equipo.
3. Antes de tomar cualquier decisión, haga una copia de seguridad de todos los datos imprescindibles en una unidad externa (disquete, CD, tarjeta de memoria, etc.)
4. Instale Kaspersky Anti-Virus si no lo ha hecho todavía.
5. Descargue las últimas actualizaciones de la base antivirus. Si es posible, recupere las actualizaciones desde un equipo no infectado.

Esto es importante, porque si se encuentra conectado a Internet, un virus puede enviar información importante a los causantes de la infección, o intentar enviarse a sí mismo a todas las direcciones de su libreta. Por tanto, si sospecha que su equipo está infectado, debe inmediatamente desconectarlo de Internet. Sin embargo, si no hay otra manera de recuperar las actualizaciones, puede tomarse el riesgo de descargarlas antes de desconectarse.

6. Desconecte su equipo de Internet.
7. Si su equipo está conectado a una red de área local, desconéctelo.
8. Lance un análisis completo (ver sección 5.2.2 pág. 28).
9. Informe a su administrador de sistemas sobre los síntomas sospechosos en el funcionamiento del equipo.

2.3. Si se encontraron virus durante el análisis

Si se encontraron virus durante el análisis, el Kaspersky Anti-Virus los desinfectará automáticamente y recuperará los datos desde la copia de respaldo de su equipo.

Observe que en el 99% de los casos, los equipos domésticos son infectados por gusanos de correo, troyanos o virus (vea Capítulo 1 pág. 5 acerca de programas dañinos). En la mayoría de los casos, todos los datos perdidos pueden ser recuperados con éxito.



Para eliminar los virus y recuperar datos dañados:

1. No interrumpa las operaciones de Kaspersky Anti-Virus. Durante un análisis completo, el programa desinfecta archivos infectados, mueve los archivos sospechosos hacia una carpeta de cuarentena, y elimina los gusanos de correo y los troyanos. Al finalizar el análisis, antes de aplicar la cura, Kaspersky Anti-Virus presenta todos los archivos sospechosos, virus, gusanos de correo y troyanos detectados. También encontrará los nombres de cualquier virus residente en su equipo, dentro del informe (ver la sección 5.4.2 pág. 40).
2. En ciertos casos, necesitará una herramienta especial para recuperar datos dañados. Conéctese a Internet, visite el sitio Web de Kaspersky Lab (www.kaspersky.com) y lea la información acerca del virus, troyano o gusano que infectó su equipo. Descargue, si existe, la herramienta de recuperación de datos específica de un virus. Por

ejemplo, para recuperar datos infectados con el virus **Klez**, descargue y ejecute la aplicación *clrav.com*.

3. Lea atentamente cualquier información aplicable a su caso en el sitio Web. Deberá probablemente tomar medidas adicionales.
4. Unos virus (por ejemplo, **Nimda**, **Klez**, o **Badtrans**) que han penetrado en su equipo aprovechando las vulnerabilidades de Microsoft Outlook Express, pueden reactivarse incluso después de que Kaspersky Anti-Virus limpie el sistema, por ejemplo, cuando vuelva a leer mensajes previamente infectados. Por lo tanto, compruebe que tiene activado el modo de protección que analiza las bases de correos (para más información, póngase en contacto con su administrador de sistemas) e instale las últimas revisiones de seguridad para garantizar un funcionamiento seguro Microsoft Outlook en adelante.

Desgraciadamente, algunos virus no pueden ser eliminados completamente de los objetos infectados. Algunos de ellos destruyen los datos de su sistema durante la infección.

2.4. Si nada lo soluciona...

Si se repiten los síntomas descritos anteriormente incluso después de analizar su equipo y comprobar todo el hardware y discos duros instalados con las herramientas de Windows, envíe un mensaje con una descripción completa de su problema al servicio de soporte de Kaspersky Lab.

Si está seguro que determinados archivos son troyanos o han sido infectados, envíe estos archivos a Kaspersky Lab para que sean analizados por nuestros expertos.



Para más detalles acerca de cómo enviar mensajes Kaspersky Lab, vea Anexo B pág. 49.

2.5. Tras erradicar la infección

Tras librarse de la infección, analice todos los discos y disquetes que pueden haber sido infectados por un virus.

Asegúrese de que su equipo tiene instalada la última versión de Kaspersky Anti-Virus Personal y la última actualización de la base antivirus, y aplique la configuración recomendada por los expertos de Kaspersky Lab (para más información acerca de la configuración de Kaspersky Anti-Virus, póngase en contacto con su administrador de sistemas).

Lea con atención la sección **Cómo impedir una infección vírica** (ver sección 5.2 pág. 25) y preste atención a las reglas básicas de seguridad que le ayudarán a evitar infecciones víricas en el futuro.

CAPÍTULO 3. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (al que nos referimos también en esta guía de usuario como Kaspersky Anti-Virus) ha sido diseñado para proteger estaciones de trabajo contra virus y software dañino.

Las siguientes características han sido implementadas por la aplicación:

- *Protección en tiempo real del sistema de archivos contra código dañino en el modo supervisión:* interceptación y análisis de los accesos al sistema de archivos y a los directorios de red; desinfección o eliminación de objetos infectados y aislamiento de objetos sospechosos para su análisis posterior.
- *Análisis y neutralización del código dañino a petición del usuario o del administrador:* búsqueda y análisis de objetos infectados o sospechosos dentro de coberturas definidas; eliminación o aislamiento de objetos infectados o sospechosos para su análisis posterior.
- *Análisis del correo en modo supervisión:* análisis de las peticiones de envío o de recepción de correo electrónico. El antivirus evita que el código dañino presente en el correo pueda llegar hasta el buzón del usuario, o que puedan enviarse objetos sospechosos o infectados a otras direcciones. El antivirus analiza todos los mensajes entrantes y salientes de Microsoft Outlook; también explora los mensajes entrantes y salientes de cualquier cliente de correo que utilice los protocolos SMTP y POP3.
- *Protección constante de las aplicaciones ofimáticas que utilizan macros VBA:* análisis de comandos de macro antes de su ejecución, y bloqueo de comandos potencialmente peligrosos en el momento de su ejecución.
- *Protección permanente contra la ejecución de las secuencias de comandos VBScript y Javascript peligrosas:* análisis de los comandos antes de su ejecución por el intérprete de secuencias de comandos del S.O.; bloqueo de la ejecución de secuencias peligrosas.
- *Cuarentena de objetos sospechosos:* almacenamiento de objetos sospechosos en un directorio de cuarentena; con la posibilidad de desviarlos hacia Kaspersky Lab para su investigación posterior; restauración de objetos desde la cuarentena a petición del administrador o del usuario.

- *Creación de copias de respaldo de objetos infectados antes de su desinfección o eliminación* esto permite la restauración a petición de objetos si éstos contienen datos valiosos.
- *Actualizaciones de la base antivirus y de los módulos de aplicación* incluidas en el paquete de la aplicación, desde servidores de actualización de Kaspersky Lab; creación de copias de respaldo para todos los archivos que van a ser actualizados, lo que permite anular la última actualización; inclusión de las actualizaciones recibidas en un directorio especial, antes de su distribución posterior.



Tenga presente que nuevos virus aparecen cada día en todo el mundo. Le recomendamos por tanto actualizar la base antivirus todas las horas.

3.1. Presentación del producto

Puede adquirir el software en nuestros distribuidores (en caja), o en cualquiera de nuestras tiendas Web (por ejemplo, www.kaspersky.com, en la sección **E-Store**).

Si adquiere la caja del producto, el contenido incluye:

- Un sobre sellado con un CD de instalación con los archivos de programa;
- Un manual del usuario;
- Una llave de licencia incluida en el paquete de distribución o guardada en un disquete flexible;
- El contrato de licencia.



Lea detenidamente el Contrato de licencia antes de abrir el envoltorio del CD.

Si adquiere nuestro producto en una tienda en línea o lo descarga desde el sitio de Kaspersky Lab, su copia también incluye este manual. La llave de licencia viene incluida en el archivo de instalación, o será enviada por correo electrónico a recepción del pago.

El Contrato de licencia es un contrato legal entre Usted y Kaspersky Lab que describe los términos y condiciones de uso del software que acaba de comprar.



Lea con atención el Contrato de licencia

Si no está de acuerdo con los términos y condiciones del Contrato de licencia, puede devolver la caja que contiene Kaspersky Anti-Virus al distribuidor donde lo

compró; el dinero abonado le será devuelto siempre que el sobre con el CD de instalación siga cerrado.

La apertura del sobre sellado del CD o la instalación del producto en un equipo significa su aceptación de todos los términos y condiciones del contrato de licencia.

3.2. Servicio para usuarios registrados

Kaspersky proporciona a sus usuarios registrados un amplio abanico de servicios para utilizar de forma eficiente Kaspersky Anti-Virus.

Quando adquiere una suscripción, se convierte en usuario registrado, con la posibilidad de beneficiarse de los servicios siguientes, durante el tiempo de validez de su suscripción:

- actualizaciones del software;
- consultas relativas a la instalación, configuración y uso de este software, a través del teléfono o por correo electrónico;
- información acerca de la disponibilidad de nuevos productos software de Kaspersky Lab y de la aparición de nuevos virus en todo el mundo (para suscriptores de la lista de correo de noticias de Kaspersky Lab).







No se facilitan consultas para problemas relacionados con el funcionamiento o el uso del propio sistema operativo o de otras tecnologías.

3.3. Convenciones tipográficas

El texto de este documento utiliza diferentes estilos, en función del tipo de contenido. La tabla a continuación enumera las convenciones tipográficas adoptadas para el texto.

Estilo	Descripción
Negrita	Títulos y opciones de menús, títulos de ventana, partes de cuadros de diálogo, etc.



Estilo	Descripción
 <p>Nota.</p>	<p>Información o notas adicionales</p>
 <p>¡Advertencia!</p>	<p>Información que requiere especial atención</p>
 <p>Para completar la acción,</p> <ol style="list-style-type: none"> 1. Paso 1. 2. ... 	<p>Descripción de las etapas que debe realizar el usuario, con sus posibles acciones</p>
 <p>Tarea, ejemplo</p>	<p>Descripción de un problema, ejemplo de uso de alguna función del software</p>




CAPÍTULO 4. INTERFAZ DEL PROGRAMA

Kaspersky Anti-Virus posee una interfaz sencilla y fácil de usar. Este capítulo describe con detalle sus principales elementos: el icono de la barra del sistema, el menú contextual, la ventana principal de la aplicación y algunas de las ventanas de servicio.

4.1. Icono de la barra del sistema

Después de iniciar el programa, su icono aparece en la barra del sistema. La imagen del icono depende del estado de protección antivirus, y señala si la protección en tiempo real está habilitada o si el análisis a petición ha sido iniciado.


Si la protección en tiempo real está habilitada, el icono aparece activado (rojo) , si está deshabilitada: el icono aparece desactivado (gris) .

El icono parpadeará en la barra del sistema  durante el transcurso de un análisis completo del sistema, archivo individual o disco, o cuando se produce el análisis en tiempo real de algún objeto. El análisis de los correos entrantes se indica por el icono , y el icono  aparece si se producen errores durante la ejecución de cualquier tarea de protección en tiempo real.

Si se produce un evento de cierta importancia en términos de protección antivirus, aparece durante un momento por encima del icono un cuadro con un mensaje informativo y la recomendación de los expertos de Kaspersky Lab (esta característica no está disponible en Windows98/NT).

4.2. Menú contextual

Si hace clic con el botón derecho del ratón encima del icono en la barra del sistema, aparece un menú (ver Figura 1) con las opciones siguientes:

- **Abrir Kaspersky Anti-Virus:** abre la ficha **Protección** de la ventana principal de la aplicación. Puede obtener el mismo resultado con un doble-clic en el icono de la aplicación  en la barra del sistema.

- **Analizar Mi PC:** ejecuta un análisis completo del equipo de acuerdo con el nivel de protección definido.
- **Actualizar las bases antivirus:** ejecuta la descarga de actualizaciones de la base antivirus.
- **Tareas en ejecución:** esta opción aparece en el menú contextual cuando el programa antivirus inicia cualquier tarea planificada. La selección de esta opción abre un submenú con la lista de todas las tareas planificadas en ejecución en ese instante. Seleccione una tarea dentro de la lista (ver Figura 4) para mostrar información sobre su operación.
- **Acerca de la aplicación:** abre una ventana de ayuda con información acerca de Kaspersky Anti-Virus for Windows Workstations.
- **Cambiar a modo usuario/ Cambiar a modo administrador** (sólo para MS Windows 98/ME): permite cambiar entre una interfaz de usuario y otra ampliada para el administrador, respectivamente. Al elegir **Cambiar a modo administrador**, se abre un cuadro de diálogo solicitando la contraseña del administrador de seguridad antivirus.

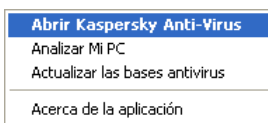


Figura 1. Menú contextual

4.3. Ventana principal de la aplicación: estructura general

La ventana principal de Kaspersky Anti-Virus está diseñada para integrar todas las características del producto, y asegurar la protección antivirus completa de su equipo. También puede:

- iniciar las tareas de protección antivirus;
- descargar actualizaciones de la base antivirus;
- trabajar con objetos en cuarentena o copiados hacia la zona de respaldo;
- trabajar con informes, etc.

Toda la configuración antivirus, la información necesaria y las tareas se agrupan en las fichas siguientes de la ventana principal:

- **Protección:** estado y tareas de protección antivirus. Es la ficha principal cuando trabaja con la aplicación.

- **Soporte:** información indispensable en caso de problema, o necesaria para obtener ayuda de Kaspersky Lab.

Cada ficha cuenta dos paneles:

- **La lista de tareas** es el panel izquierdo con las tareas que realmente aseguran la protección antivirus. La lista de tareas depende de la finalidad de la ficha. La ficha **Protección**, por ejemplo, contiene todas las tareas capaces de analizar su equipo en busca de virus.
- **El estado de protección antivirus** queda reflejado en el panel derecho de la ficha, con información sobre el estado actual de la protección antivirus del equipo (protección en tiempo real, análisis completos del sistema, y base antivirus). La ficha **Protección**, por ejemplo, indica el estado de la protección antivirus.

Existen tres niveles de protección antivirus. Están señalados por los iconos siguientes:



Nivel crítico de protección antivirus. Este estado significa que la protección en tiempo real está desactivada, que algunas tareas (análisis, actualización) no han sido ejecutadas desde hace tiempo, o que la configuración actual no ofrece una protección antivirus adecuada para el equipo; también informa al usuario de los errores aparecidos al ejecutar una tarea del antivirus.



El nivel de protección antivirus es diferente del recomendado. Este estado se posiciona cuando la configuración personalizada no corresponde con la configuración recomendada por Kaspersky Lab. También indica la necesidad de realizar una determinada tarea de protección antivirus.



Nivel recomendado de protección antivirus. Este nivel corresponde a un estado de plena conformidad con la configuración de protección y seguridad antivirus recomendada por los expertos de Kaspersky Lab.

Cada uno de los estados anteriores está acompañado de comentarios y recomendaciones. Así, por ejemplo, cuando el nivel de protección antivirus es diferente del recomendado, la aplicación le ofrece regresar a la configuración recomendada, porque ésta ofrece el nivel óptimo de protección antivirus.

4.3.1. Ficha Protección

La ficha **Protección** (ver Figura 2) está diseñada para ejecutar tareas como el análisis completo, así como el análisis de discos, carpetas o archivos individualmente. También puede iniciar aquí la descarga de actualizaciones de

la base antivirus. Puede iniciar las tareas con un clic en los hipervínculos correspondientes del panel izquierdo de la ficha.

El panel izquierdo de la ficha también incluye vínculos a las zonas de cuarentena y respaldo, y para los informes del programa:

- [Cuarentena](#): abre la zona de almacenamiento de objetos sospechosos.
- [Copia de respaldo](#): abre la zona de respaldo de objetos infectados.
- [Informes](#): abre los registros de informes.

En la parte derecha de la ficha, encontrará el *estado actual de la protección en tiempo real*, del *análisis completo del sistema*, y de la *base antivirus*. Las *recomendaciones de Kaspersky Anti-Virus* son indispensables enA los niveles crítico y medio de protección antivirus.



Figura 2. Ficha Protección

El panel derecho de la ficha, junto a los indicadores de estado de la protección antivirus, muestra información general acerca del número total de objetos analizados y de virus detectados desde la instalación de Kaspersky Anti-Virus.

El panel derecho de la ficha, junto a los indicadores de estado de la protección antivirus, muestra información acerca del número de objetos analizados y de virus detectados desde el inicio de Kaspersky Anti-Virus.

La información es reemplazada por un vínculo [Se han detectado virus...](#) si una tarea de análisis planificado descubre objetos infectados o sospechosos. Haga clic en el vínculo para ver la lista de tareas asignadas a los objetos para su tratamiento.

4.3.2. *Ficha Soporte*

Desde la ficha **Soporte** (ver Figura 3), puede obtener información del Servicio de asistencia técnica, al que es posible acudir en caso de problemas relacionados con el funcionamiento del antivirus o con situaciones que no puede controlar. Contiene información acerca del programa, la llave de licencia y el sistema operativo instalados en su equipo. Toda esta información se encuentra en el panel derecho de esta ficha.

El panel izquierdo contiene los vínculos siguientes:

- [Escribir al servicio de soporte](#): enviar una pregunta relacionada con el funcionamiento del antivirus al Servicio técnico.
- [Enviar archivo para análisis](#): envía un objeto sospechoso por correo electrónico a Kaspersky Lab para su análisis.

El panel izquierdo de todas las fichas de la ventana principal de Kaspersky Anti-Virus contiene vínculos a información de ayuda:

- [Ayuda](#): ayuda general acerca del software.
- [Cómo...](#): sistema de ayuda para optimizar las tareas y solución a los problemas que puedan surgir.
- [Enciclopedia de virus](#): vínculo al sitio Web www.viruslist.com, que contiene una descripción detallada de todos el software dañino existente hasta el momento.
- [Sitio Web de Kaspersky Lab](#): vínculo al sitio Web de Kaspersky Lab.



Figura 3. Soporte

4.4. Ventana Analizando

Cuando se inicia un análisis del equipo o de objetos individuales (discos, archivos o carpetas), dicho proceso aparece en pantalla (ver Figura 4).

La ventana de análisis consta de dos partes:

- La parte superior presenta el progreso del análisis, la hora de inicio, la hora de finalización prevista y el nombre del archivo analizado en ese momento.
- La parte inferior consta de tres fichas: una ficha **Estadísticas** con los resultados del análisis, una ficha **Informe** con un informe de los eventos que se produjeron durante el análisis, y una ficha **Configuración** con una lista de parámetros aplicados sobre el análisis anterior o el actual.

El vínculo [Ver cuarentena](#) conduce al usuario a la ventana Cuarentena (ver sección 5.4.1.1 pág. 37). Si la aplicación detecta objetos infectados o sospechosos durante el análisis y se activó el tratamiento diferido, incluirá entonces el vínculo [Virus detectados](#): haga clic en él para abrir una ventana de

administración de los objetos infectados que serán procesados más tarde (ver sección 5.2.5 pág. 32).



Figura 4. Ventana Analizando

4.5. Sistema de ayuda

Una información de referencia completa del programa está disponible desde la ficha **Soporte** de la ventana principal de la aplicación: siga simplemente el vínculo [Ayuda](#) en el panel izquierdo de la ficha.

Cuando necesite saber cómo realizar una determinada tarea, siga el vínculo [Cómo...](#) en la ventana principal de Kaspersky Anti-Virus for Windows Workstations. El vínculo [Cómo...](#) contiene una descripción detallada de las tareas clave para la protección antivirus realizadas por Kaspersky Anti-Virus for Windows Workstations, así como una lista de preguntas frecuentes.

Si tiene alguna duda sobre un cuadro de diálogo en particular, presione la tecla **<F1>** o haga clic en [Ayuda](#) en el ángulo inferior izquierdo del cuadro de diálogo.

CAPÍTULO 5. TRABAJAR CON LA APLICACIÓN

5.1. Actualización de la base antivirus y de los módulos de aplicación

El funcionamiento eficiente de Kaspersky Anti-Virus depende de que su información sea reciente para proteger su equipo contra las últimas amenazas descubiertas. Kaspersky Lab pone esta información a disposición de sus usuarios mediante actualizaciones regulares de su base antivirus.



La descarga de actualizaciones de la base antivirus garantiza una protección antivirus continuada de su equipo. Centenares de nuevos virus aparecen a diario, y los expertos de Kaspersky Anti-Virus actualizan todos los días la base antivirus con información de última hora sobre nuevas amenazas. Le recomendamos actualizar su base antivirus cada hora.

Para descargar las actualizaciones, Kaspersky Anti-Virus Personal se conecta por Internet a uno de los servidores de actualizaciones de Kaspersky Lab, o a un servidor de actualizaciones local.

Las actualizaciones pueden ser descargadas automáticamente mediante un calendario recomendado, establecido al instalar la aplicación, o un calendario personalizado por el administrador. La aplicación descarga y actualiza la base antivirus mientras se encuentra conectado a Internet. Kaspersky Anti-Virus copia las actualizaciones desde servidores de actualizaciones remotos, e instala los archivos necesarios en su equipo.

5.1.1. Elección de la hora de actualización

La aplicación le informa de la necesidad de actualizar la base antivirus. También puede tomar personalmente la decisión de actualizar tras examinar los indicadores en el panel derecho de la ficha **Protección** (ver Figura 2).

El estado de las actualizaciones está señalado por los iconos siguientes:



– No es necesario actualizar la base antivirus o el proceso de actualización esté en curso.



– Una actualización de la base antivirus es necesaria. Si las actualizaciones no están disponibles porque la licencia ha caducado, el programa aporta información relativa a su ampliación.



– Se requiere una actualización urgente; la base antivirus está caducada o ausente.

5.1.2. Proceso de actualización



Para ejecutar el proceso de actualización manualmente,

utilice el vínculo [Actualizar ahora](#) en el panel izquierdo de la ficha **Protección**

o:

el vínculo [actualizar la base antivirus](#) de información acerca del estado de la base antivirus en el panel derecho de la ficha **Protección**;

o:

seleccione el comando **Actualizar las bases antivirus** en el menú contextual que se abre con un clic del botón derecho en el icono del programa en la barra del sistema.

Haga clic en un vínculo para abrir una ventana (ver Figura 5) con información sobre el avance de la actualización de la base antivirus y de los módulos de aplicación.

El proceso de descarga de actualizaciones puede dividirse en las etapas siguientes:

1. El programa recibe una lista con información sobre el tamaño de las actualizaciones desde el servidor de actualizaciones de Kaspersky Lab.
2. A continuación el programa compara su base antivirus con los datos recuperados del servidor. Si ya tiene instaladas las últimas bases antivirus en su equipo, un mensaje emergente le confirmará que su base antivirus está actualizada.
3. El campo **Tamaño** del cuadro de diálogo **Actualización** (ver Figura 5) indica el tamaño total de las actualizaciones descargadas. Si no son necesarias las actualizaciones, el proceso de actualización termina. En

otro caso, la aplicación comienza a copiar archivos desde los servidores de actualizaciones de Kaspersky Lab en Internet. El progreso de la descarga aparece reflejado por el indicador. El campo **Total descargado** muestra el tamaño (en Kb) de las actualizaciones ya descargadas. Tras completar el proceso de descarga, las actualizaciones de la base de datos son instaladas automáticamente en su equipo.

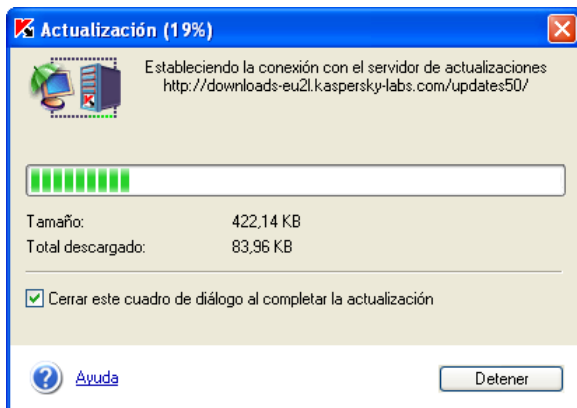


Figura 5. Actualización de la base antivirus y de los componentes de aplicación

5.2. Cómo impedir una infección vírica

Ni la más prudente y segura de las actuaciones le garantiza un 100% de protección contra los virus de ordenador y los troyanos, pero puede reducir considerablemente el riesgo de infecciones por ataques de virus y de este modo controlar las pérdidas causados por una posible infección.

Uno de los métodos principales de la lucha contra virus, al igual que en medicina, es tomar medidas de prevención. La protección del equipo se basa en algunas reglas, cuyo cumplimiento reduce considerablemente la probabilidad de infección por los virus y la pérdida de cualquier información.

Las reglas clave de seguridad para ayudar a prevenir los riesgos de virus en su equipo son enumeradas a continuación.

Regla 1: *Inspeccione periódicamente su ordenador en con programas antivirus y perímetros de protección Web (cortafuegos). Para ello:*

- Instale Kaspersky Anti-Virus.

- Para mantener su protección actualizada, actualice su antivirus todos los días. En periodos de epidemias víricas, puede recuperar actualizaciones varias veces al día, ya que en estos periodos la base antivirus de los servidores de Kaspersky Lab se actualizan constantemente.
- Le recomendamos también instalar Kaspersky Anti-Hacker para una protección completa de su equipo, mientras navega por Internet.

Regla 2: *Tenga cuidado cuando introduzca cualquier dato nuevo en su equipo:*

- Analice siempre todos los discos extraíbles (disquetes, CDROM, tarjetas de memoria, etc.) antes de utilizarlos.
- Tenga precaución con los mensajes electrónicos. No abra nunca un adjunto de correo, incluso si proviene de alguien conocido, a menos que tenga la seguridad de que se trata del adjunto solicitado o esperado. En particular, no confíe en mensajes enviados por fabricantes antivirus "de imitación".
- Tenga precaución cuando descarga en Internet. No descargue nunca software sin certificado de seguridad.
- Si descarga un archivo ejecutable de Internet o de la red local, analícelo con Kaspersky Anti-Virus.
- Seleccione los sitios Web que visita. Algunos sitios Web contienen secuencias de comandos peligrosas o gusanos de Internet.

Regla 3: *Preste atención a la información de Kaspersky Lab.*

Los expertos de Kaspersky Lab advierten del comienzo de una nueva epidemia mucho antes de que alcance su visan mayor virulencia. Si se protege a tiempo con actualizaciones recientes, esto le ayudará a evitar la infección con cualquier virus nuevo.

Regla 4: *Desconfíe de los rumores de virus: mensajes ficticios que quieren avisarle contra amenazas de virus reales.*

Regla 5: *Actualice regularmente su sistema operativo con la herramienta de actualización de Windows.*

Regla 6: *Compre sus nuevos programas a vendedores autorizados.*

Regla 7: *Ponga restricciones al número de personas que tienen acceso a su equipo.*

5.2.1. ¿Cuándo debo analizar mi equipo y objetos individuales?

Kaspersky Anti-Virus puede realizar un análisis antivirus del equipo completo, o de objetos particulares: discos duros o extraíbles, carpetas, archivos o mensajes de correo electrónico.

Observe que la obtención de resultados positivos mientras analiza determinado objetos a petición no le garantiza que su equipo esté libre de virus. Por ello, Kaspersky Anti-Virus siempre está atento a si su equipo completo ha sido analizado.

Durante un análisis completo, el programa analiza una cantidad mayor de objetos que con la protección en tiempo real. Por ello, se recomienda analizar su equipo al menos una vez a la semana, como medida de precaución. El programa le avisará cuando llegue el momento de realizar un análisis completo. Si la ventana principal de la aplicación está cerrada, un mensaje recomendándole iniciar un análisis completo se mostrará encima del icono de Kaspersky Anti-Virus en la barra del sistema.

Para leer información más completa, abra la ventana principal de la aplicación y lea el estado de análisis completo en el panel derecho de la ventana principal, en la ficha **Protección** (Figura 2). Son posible los siguientes indicadores del análisis completo:



– Le recomendamos fuertemente realizar un análisis completo inmediatamente.



– Le recomendamos realizar un análisis completo con la configuración recomendada.



– Un análisis completo ha sido realizado recientemente, o está en curso.

Si es necesario, puede ejecutar un análisis completo directamente en la zona de estado del análisis completo estado con un clic en [realizar un análisis completo](#).

5.2.2. Análisis completo



Para iniciar un análisis antivirus a petición de su equipo:

haga clic en [Analizar Mi PC](#) en el panel izquierdo de la ficha **Protección** (Figura 2). La misma acción puede ser ejecutada con un clic en [realizar un análisis completo](#) el panel derecho de la ficha **Protección**. Dispone también de la opción **Analizar Mi PC** en el menú emergente, que se abre con un clic del botón derecho en el icono del programa en la barra del sistema.

Tras hacer clic en el vínculo, se abrirá el cuadro de diálogo **Analizando** (ver Figura 4), que muestra el porcentaje de objetos analizados, la duración desde el inicio del análisis, el tiempo estimado y real hasta el final del análisis, y el nombre del objeto analizado.

Es posible ver un informe sobre el rendimiento del programa (ver sección 5.4.2 pág. 40, acerca de los informes).

5.2.3. Análisis a petición de archivos o carpetas seleccionados

En algunos casos, interesa analizar determinados objetos en lugar del equipo completo. Estos objetos pueden ser, por ejemplo, un disco duro con programas y juegos, bases de datos de los mensajes de correo que se ha traído de la oficina, un adjunto recibido en un mensaje electrónico, etc. Puede seleccionar estos objetos con las opciones de Kaspersky Anti-Virus o con las herramientas estándar de Windows (por ejemplo, el **Explorador, Mi PC**, etc.).



Para definir qué objetos analizar con las aplicaciones estándar de Windows,

seleccione el objeto y haga clic con el botón derecho del ratón. Se abre el menú contextual de Windows. En este menú, seleccione el comando **Buscar virus** (ver Figura 6).

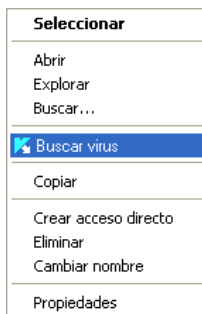


Figura 6. Análisis de un objeto desde el menú contextual de Windows



Recuerde que para seleccionar un objeto para su análisis desde el menú contextual de Windows, antes debe instalar Kaspersky Anti-Virus



Para ejecutar el análisis antivirus a la demanda de un objeto o de unidades extraíbles, seleccione los elementos siguientes en el panel izquierdo de la ficha **Protección**:

- [Analizar unidades extraíbles](#) inicia el análisis de unidades extraíbles;
- [Analizar objeto\(s\)](#): seleccione desde aquí un objeto (archivo, carpeta o disco) y ejecute el análisis. Se abre una nueva ventana con el título **Seleccionar objetos para su análisis** (ver Figura 7) que contiene una lista de objetos disponibles para análisis, con botones para agregar elementos e iniciar el análisis.

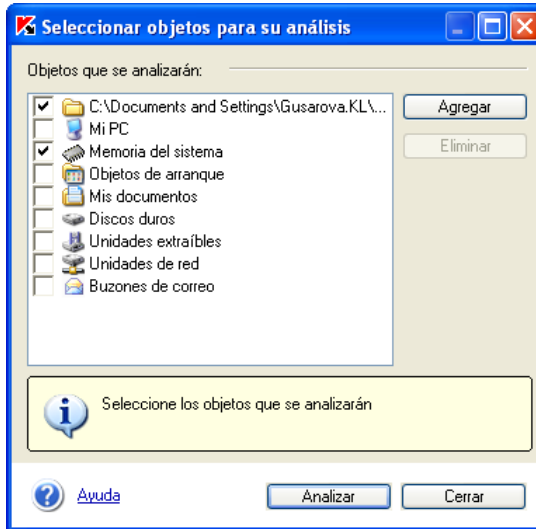


Figura 7. Selección de objetos analizados

Para agregar un nuevo objeto a la lista, haga clic en **Agregar** y abra el archivo o la carpeta deseada. Todos los objetos incluidos en la lista estarán disponibles para futuros análisis.

Para retirar un objeto de la lista, active la casilla correspondiente y haga clic en **Eliminar**. Observe sin embargo que sólo puede quitar de la lista los objetos que incluye, no los objetos iniciales.



Para analizar objetos en la lista:

1. Active las casillas correspondientes.
2. Haga clic en **Analizar**.

Sin tener en cuenta cómo inició el análisis (desde Kaspersky Anti-Virus o desde el menú contextual de Windows), se abre la ventana **Analizando** (ver Figura 4). El cuadro de diálogo muestra el porcentaje de objetos analizados, la duración desde el inicio del análisis, el tiempo estimado y real hasta el final del análisis, y el nombre del objeto analizado.

Es posible ver un informe sobre el rendimiento del programa (ver sección 5.4.2 pág. 40).

5.2.4. Analizar compilaciones de datos

Kaspersky Anti-Virus analiza compilaciones de datos en el modo a petición en los niveles de **Máxima protección** y **Recomendado**, siempre que no se establezcan exclusiones (para más información, consulte su administrador de seguridad).



Observe que Kaspersky Anti-Virus no desinfecta compilaciones anidadas, con niveles múltiples. Cuando detecta objetos de este tipo, muestra una ventana con la acción recomendada **Ignorar**.

Si una compilación está protegida con contraseña, el programa la solicitará antes de proseguir el análisis de los objetos contenidos (ver Figura 8).

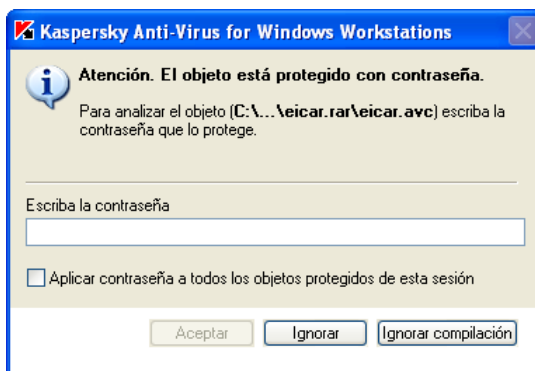


Figura 8. Escritura de contraseña para analizar un archivo protegido

En el campo **Contraseña**, escriba la contraseña de los objetos contenidos y haga clic en **Aceptar**. Tras indicar la contraseña, el programa analizará la compilación y todos los objetos que contiene.

Si encuentra otra compilación protegida, Kaspersky Anti-Virus utiliza automáticamente la contraseña de la primera compilación, para analizar los objetos de la siguiente. Sólo deberá indicar otra contraseña si la primera no es válida.

Si desconoce la contraseña, el programa no podrá analizar la compilación ni los objetos contenidos que la requieran. Le recomendamos que haga clic en **Ignorar** y continúe con el análisis.

Haga clic en el vínculo **Ignorar compilación** para ignorar todos los objetos protegidos por contraseña dentro de una compilación que se encuentren durante el análisis en curso. De este modo, todos los demás objetos dentro de la

compilación que no estén cifrados podrán ser analizados y procesados de acuerdo con la configuración prevista para el análisis antivirus.




Aplicar contraseña a todos los objetos protegidos de esta sesión la acción seleccionada se aplicará a todos los objetos protegidos con contraseña dentro de la compilación encontrada durante la ejecución del análisis actual. Por ejemplo, si activó esta casilla y selecciona **Ignorar**, **Ignorar compilación**, entonces los restantes objetos protegidos con contraseña no serán analizados. O bien, si escribe la contraseña y hace clic en **Aceptar**, el programa antivirus intentará aplicar la misma contraseña a todos los restantes objetos que estén cifrados, sin mostrar ningún cuadro de diálogo.

5.2.5. Tratamiento diferido de objetos

La necesidad de administrar objetos infectados se produce cuando el administrador selecciona la variante *Preguntar al usuario después de terminar el análisis* como acción aplicada por el antivirus a cualquier objeto infectado o sospechoso posteriormente detectado durante el análisis.

Después de terminar el análisis, el antivirus abre la ventana **Control de objetos infectados** (ver Figura 10), donde puede seleccionar las acciones aplicadas a dichos objetos. También tiene acceso a la ventana de control diferido de objetos directamente desde la ventana de progreso del análisis (ver Figura 4) con el vínculo [Virus detectados](#).

Cuando las tareas planificadas de análisis antivirus en segundo plano encuentran objetos infectados o sospechosos, una lista de estas tareas se muestra en la ventana (ver Figura 9) y se abre cuando hace clic en  [Se han detectado virus...](#) en el panel derecho de la ficha **Protección**. Para revisar y controlar objetos de forma diferida, active la tarea correspondiente dentro de la lista y haga clic en **Objetos...**

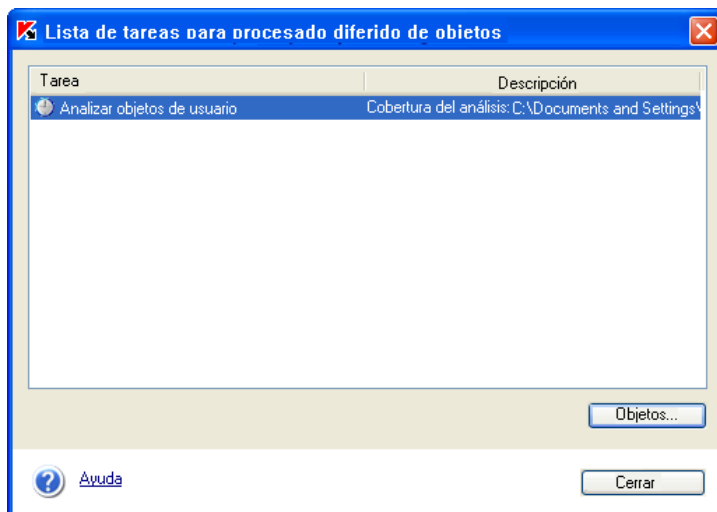


Figura 9. Lista de tareas para procesamiento diferido de objetos

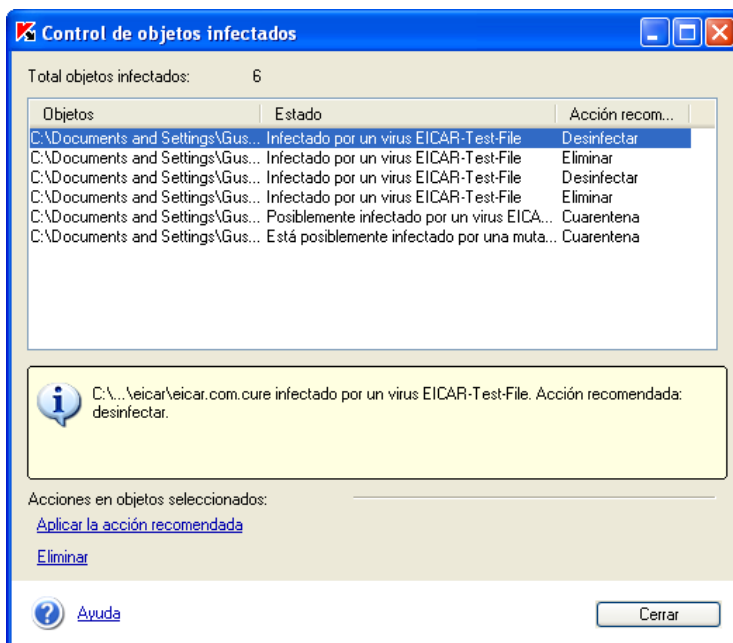


Figura 10. Control de objetos infectados y sospechosos



Observe que **NO SE REALIZA** el análisis y la desinfección de objetos protegidos con contraseña en modo diferido.

En este cuadro de diálogo, puede ver una lista de los objetos infectados y sospechosos encontrados durante el análisis (ver Figura 10). La columna **Objetos** contiene la ruta y el nombre de cada objeto, la columna **Estado**, su estado, y la columna **Acción recomendada**, indica la acción recomendada por Kaspersky Lab para el objeto.

Para seleccionar un objeto y realizar alguna acción con él, debe activar la casilla asociada. Puede seleccionar varios objetos en la lista al mismo tiempo. Es posible seleccionar todos los objetos de la lista, para ello, active la casilla en el encabezado de la lista.

Elija una de las opciones siguientes:

- [Aplicar la acción recomendada](#): realiza la acción recomendada por Kaspersky Lab. La acción recomendada en el caso de objetos infectados, es **Desinfectar**, o **Eliminar**, y para objetos sospechosos, es **Cuarentena**.
- [Eliminar](#): Elimina un archivo.

Después de aplicar una acción, el programa abre un cuadro de diálogo para mostrar su progreso. Siempre puede detener la acción con **Detener**.

Los objetos procesados serán retirados de la lista. Una vez procesados todos los objetos de la lista, haga clic en **Cerrar**.

5.2.6. Cómo analizar un CD o un disquete

Su equipo puede ser fácilmente infectado por virus residente en disquetes, CD o cualquier otro soporte extraíble. Si utiliza un disquete (o un CD autoarrancable) infectado por un virus de arranque, y reinicia su equipo con el disco en la unidad, esto puede tener graves consecuencias para su sistema.

Le recomendamos analizar todos los soportes antes de utilizarlos.

Puede analizar soportes extraíbles tanto desde la ventana principal de Kaspersky Anti-Virus como desde el menú contextual de Windows, abierto en el **Explorador de Windows**, en el **Escritorio**, etc.



Para analizar un soporte extraíble desde el menú contextual de Windows:

Seleccione el soporte (puede seleccionar el CDROM y las disqueteras al mismo tiempo) y haga clic con el botón derecho del ratón. Se abre el

menú contextual de Windows. En este menú, elija **Buscar virus** (ver Figura 6).



Para buscar virus en un CDROM o disquete a partir de la ventana principal de Kaspersky Anti-Virus:

1. Introduzca el disco en el lector de CDROM o el disquete en la disquetera. Nota: el programa puede analizar un CD y un disquete al mismo tiempo.
2. Haga clic en [Analizar unidades extraíbles](#) en el panel izquierdo de la ficha **Protección** (Figura 2).

Tras iniciar el análisis de los objetos seleccionados, el cuadro de diálogo **Analizando** muestra el porcentaje de la progresión (ver Figura 4).



Tome nota de las siguientes características del programa:

- Si olvida introducir el CD o el disquete que desea analizar en la unidad, o si el CDROM o la disquetera están desconectados, el soporte no será analizado y no mostrará ningún mensaje.
- Si introduce el disquete dentro de la disquetera después de iniciar el análisis, el programa no lo analizará. Lo mismo ocurre en el caso de unidades de CDROM y otros soportes extraíbles.
- Si retira un disquete de la unidad o desconecta la disquetera durante el análisis, el programa devuelve un error pero no proporciona información adicional. Tras esto, el programa analizará la unidad extraíble siguiente, si existe alguna en su equipo.

5.3. Protección en tiempo real

La protección en tiempo real es un modo de funcionamiento del programa antivirus en el cual ésta queda residente en la memoria RAM del equipo, supervisa todas las llamadas a los objetos del sistema de archivos, todas las acciones de secuencias de comandos VBScript y JavaScript potencialmente peligrosas, así como los comandos de macro utilizados en aplicaciones ofimáticas.

Antes de permitir el acceso a un objeto, la aplicación analiza la presencia de virus y, si detecta un virus en el objeto, la aplicación lo desinfecta, lo elimina o bloquea el acceso al éste, de acuerdo con la configuración definida. De este modo, la aplicación es capaz de detectar y eliminar el código dañino antes de que se produzca la infección del sistema.

De forma predeterminada, la protección en tiempo real sigue activa desde el momento en que se carga el sistema operativo hasta que termina de trabajar con su equipo.

La información sobre el estado actual de protección en tiempo real se muestra en el panel derecho de la ficha **Protección** (Figura 2) en la ventana principal de Kaspersky Anti-Virus.

El estado de la protección en tiempo real está señalado por los iconos siguientes:





– La protección en tiempo real está activa. El nivel de protección de su equipo es el recomendado.



– La protección en tiempo real está desactivada. La configuración de la protección en tiempo real es diferente de la recomendada.



– La protección en tiempo real está desactivada o no funciona.

El cambio del icono de actividad  (rojo) al icono de inactividad  (gris) confirma que la protección en tiempo real está activada.

5.4. Funciones avanzadas

Kaspersky Anti-Virus dispone de numerosas opciones adicionales de uso del producto, incluyendo:

- Desplazamiento de objetos sospechosos hacia la cuarentena.
- Operaciones con copias de objetos eliminados o modificados por el programa antivirus, y colocadas en la zona de respaldo.
- Ver el informe de actividad de la aplicación.

5.4.1. Zonas de cuarentena y respaldo

Kaspersky Anti-Virus permite aislar objetos sospechosos en una zona de cuarentena, o conservar copias de objetos infectados en una zona de respaldo, antes de curarlos o eliminarlos.

Cuando detecta un objeto sospechoso, la aplicación lo aísla en un directorio de cuarentena, donde es posible volver a analizar el objeto, eliminarlo, restaurarlo o enviarlo a Kaspersky Lab para su análisis.

La aplicación crea una copia de respaldo cuando detecta un objeto, antes del primer intento de desinfección o de eliminación; la copia se conserva en el directorio de respaldo, desde el cual es posible restaurar más tarde el objeto, si éste contiene datos importantes.

5.4.1.1. Trabajar con la cuarentena

De forma predeterminada, Kaspersky Anti-Virus mueve todos los objetos sospechosos detectados durante un análisis completo del equipo o en modo de protección en tiempo, y los coloca en cuarentena, donde puede seguir trabajando con ellos (análisis, restauración, eliminación, etc.).

Kaspersky Anti-Virus vuelve a analizar la cuarentena después de cada actualización de su base antivirus. Si necesita analizar objetos en cuarentena manualmente, le recomendamos actualizar la base antivirus antes de hacerlo. La base actualizada puede venir con información incluida acerca de los virus sospechosos de sus archivos, de forma que éste puede quedar desinfectado.

De este modo, el trabajo con archivos sospechosos se realiza desde la ventana de **Cuarentena** (ver Figura 11), que puede abrir con un clic en el vínculo [Cuarentena](#) de la ficha **Protección** (ver Figura 2) de la ventana principal de la aplicación o en el vínculo [Ver cuarentena](#) de la ventana de análisis terminado (ver Figura 4).

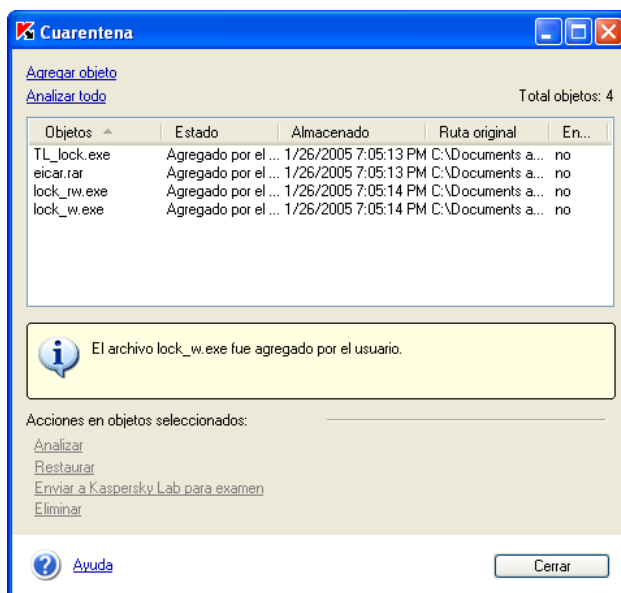


Figura 11. Ventana de cuarentena

Este cuadro de diálogo permite las siguientes operaciones en la cuarentena:

- Mover a cuarentena un archivo que sospecha contiene un virus, aunque no haya sido detectado por el programa antivirus. Para ello, haga clic en el vínculo [Agregar objeto](#) y seleccione el archivo sospechoso en la ventana estándar de selección. Será transferido desde la lista hasta su ubicación original.
- Analizar y desinfectar todos los archivos sospechosos, o los archivos seleccionados en una lista, a partir de la base antivirus actual. Para ello haga clic en los vínculos [Analizar todo](#) o [Analizar](#) (tras seleccionar los archivos que desea analizar). El análisis y desinfección de un objeto en cuarentena puede modificar su indicador a *infectado* o *desinfectado*.

El estado *infectado* significa que el objeto ha sido identificado, pero falló la desinfección. Recomendamos eliminar los objetos con este indicador.

Todos los objetos con el estado de *falsa alarma* pueden ser restaurados sin problema, al resultar equivocada la evaluación anterior (*posiblemente infectado*) de Kaspersky Anti-Virus.



De forma predeterminada, los archivos del directorio de cuarentena son analizados automáticamente después de cada actualización de la base antivirus.

- Restaura los archivos en sus mismos directorios de origen antes de ser movidos a cuarentena, o en una carpeta de destino especificada (en función de la configuración del administrador). Para restaurar un objeto, selecciónelo en la lista y haga clic en [Restaurar](#).



Recomendamos restaurar tan sólo los objetos con indicador de *falsa alarma*, porque la restauración de otros objetos puede causar una infección en su equipo.

- Enviar objetos sospechosos a los expertos de Kaspersky Lab para su examen. Recomendamos enviar un objeto para su examen experto tan sólo cuando su indicador no varía después de varios intentos de análisis y desinfección. Utilice el vínculo [Enviar a Kaspersky Lab para examen](#), para ello.
- Eliminar de la cuarentena cualquier objeto o grupo de objetos seleccionados. Eliminar tan sólo los archivos que no se pueden desinfectar. Para eliminar un archivo, selecciónelo en la lista y haga clic en [Eliminar](#).

5.4.1.2. Trabajar con la zona de respaldo

Kaspersky Anti-Virus siempre crea una copia de respaldo de un objeto infectado o sospechoso antes del primer intento de desinfección o de eliminación; la copia se conserva en el directorio de respaldo.

Cuando sea necesario, puede restaurar cualquier objeto si, por ejemplo, su desinfección produce una pérdida de datos, si el objeto ha sido eliminado por error o si prevé reintentar la desinfección con la base antivirus actualizada.

El trabajo con copias de respaldo se realiza en la ventana de **Copia de Respaldo** (ver Figura 12), que se abre con un clic en el vínculo [Respaldo](#) de la ficha **Protección** (ver Figura 2) de la ventana principal de la aplicación.

Puede realizar las acciones siguientes en la ventana de respaldo:

- Restaurar objetos en los directorios de origen de donde fueron copiados a la zona de respaldo, o en una carpeta de destino especificada (en función de la configuración del administrador). Para restaurar un objeto, selecciónelo en la lista y haga clic en [Restaurar](#).
- Eliminar archivos de la zona de respaldo. Para eliminar un archivo, selecciónelo en la lista y haga clic en [Eliminar](#).

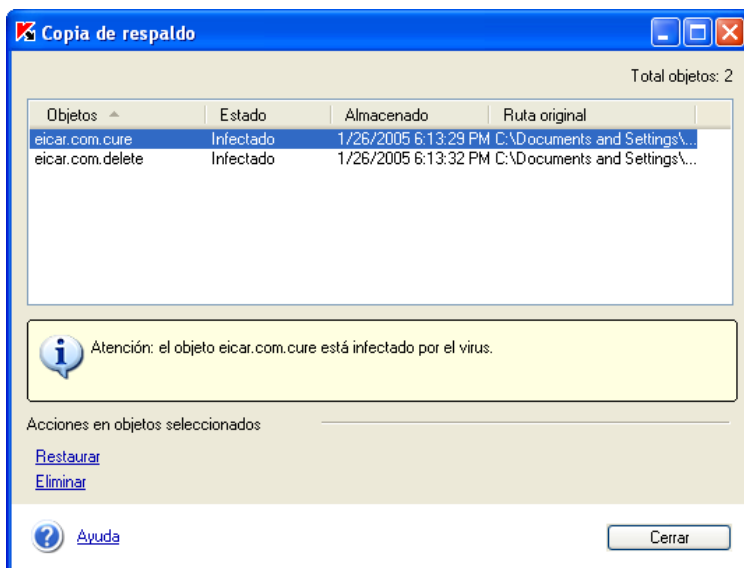


Figura 12. Zona de respaldo (ventana)

5.4.2. Trabajar con informes

La aplicación crea informes cuando realiza un análisis completo del equipo o actualiza la base antivirus y durante la protección en tiempo real, agrega líneas al informe con los resultados del análisis de objetos, así como estadísticas.

Kaspersky Anti-Virus mantiene un informe completo de las tareas realizadas (ver Figura 13), que puede abrir con un clic en el vínculo [Informes](#) del panel izquierdo de la ficha **Protección** (ver Figura 2). Queda registrado el estado de cada tarea, con su fecha y hora de terminación.

La información de estado acerca del objeto procesado puede presentar las variantes siguientes:

- *Notificaciones de éxito* (por ejemplo, el objeto está limpio, fue desinfectado o eliminado).
- *Un mensaje de información* (por ejemplo, la tarea ha sido iniciada, completada, está en curso o en pausa).
- *Advertencia* (por ejemplo, se ha encontrado un objeto sospechoso o una compilación de archivos protegidos con contraseña).
- *Evento grave* (por ejemplo, se detectó un virus) o *Fallo* (por ejemplo, porque el periodo de licencia ha caducado).
- *Fallo de funcionamiento* (por ejemplo, porque el periodo de validez de la licencia ha caducado).

Como regla general, los informes de éxito y los mensajes de información sólo tienen interés informativo y no tienen importancia esencial. Puede deshabilitar la presentación de informes de tareas que sólo contengan mensajes de ese tipo. Para ello, desactive la casilla **Mostrar líneas de información**.

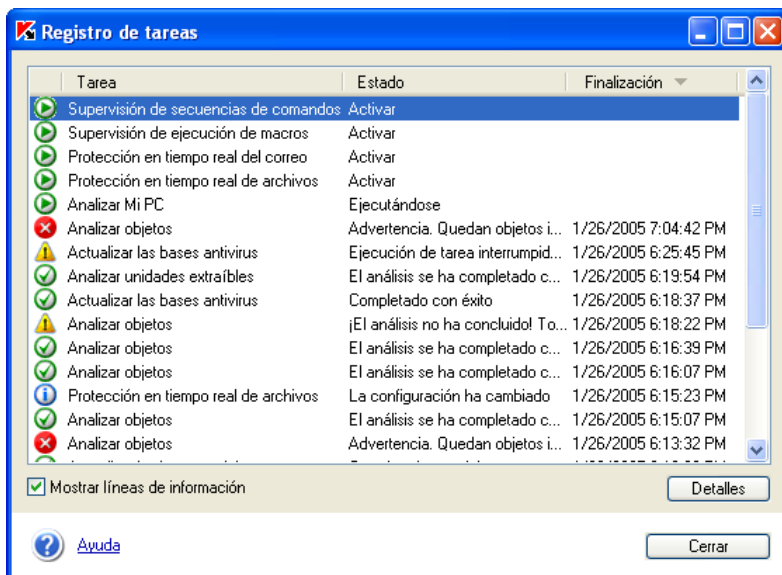


Figura 13. Registro de tareas

Es posible revisar la configuración, las estadísticas y un informe acerca de los objetos detectados por cualquier tarea bajo las fichas correspondientes que selecciona en el informe. Haga clic en **Detalles** para ello.

Haga clic en el botón para abrir una ventana con información detallada de la tarea, bajo las fichas **Estadísticas**, **Informe** y **Configuración**.

Así, la ficha **Estadísticas** (ver Figura 14) permite examinar la información general acerca del trabajo realizado por la tarea terminada: la fecha y hora de inicio de la tarea, el número total de archivos analizados y el número de objetos infectados, desinfectados y en cuarentena.

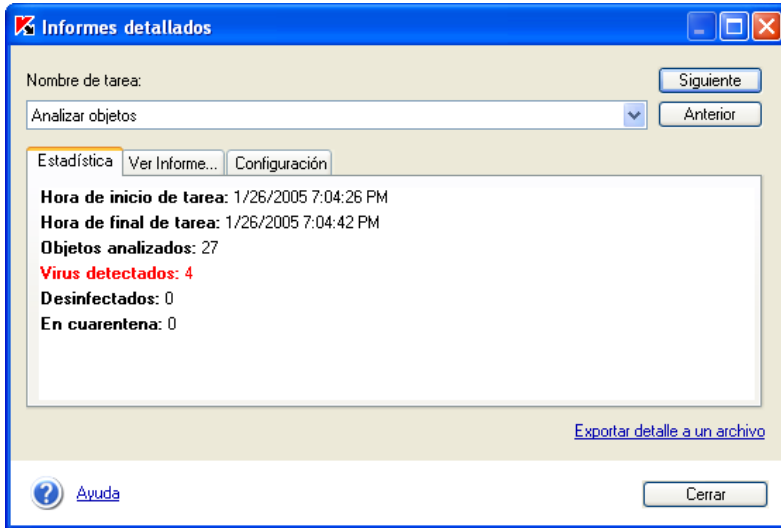


Figura 14. Ficha Estadísticas

La ficha **Ver Informe** (Figura 15) contiene información detallada acerca de cada objeto analizado.

La ficha **Configuración** (Figura 16) muestra los parámetros de tarea utilizados para el análisis. Muestra tanto la cobertura y el nivel de protección definido para tarea, como las acciones que el programa debe realizar en presencia de archivos infectados o sospechosos. La ficha también muestra los objetos excluidos del análisis si han sido definidos.

Seleccione las tareas que desea examinar en el **Nombre de tareas** o directamente en la ventana de informe detallado con los botones **Siguiete** y **Anterior**, o con un clic en el nombre de tarea dentro de la lista.

También puede obtener el informe en formato texto, para ello haga clic en el vínculo [Exportar detalle a un archivo](#). Haga clic en el vínculo para abrir una ventana estándar. Escriba el nombre del archivo, seleccione el directorio donde desea guardarlo, y haga clic en **Guardar**.

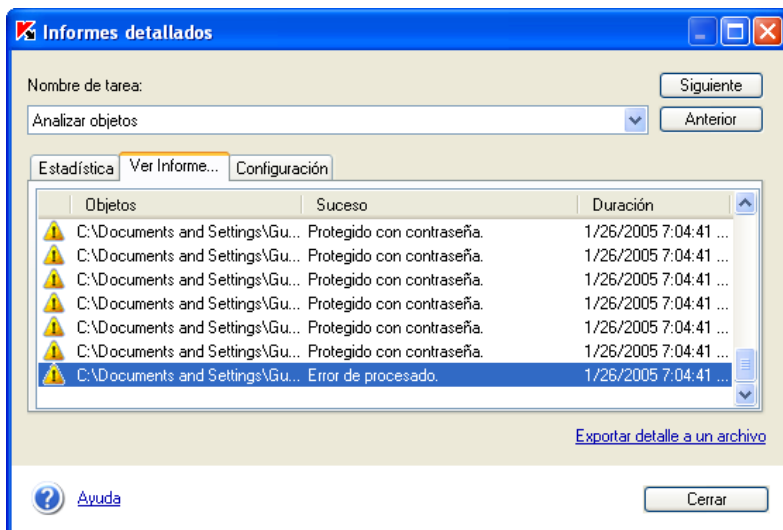


Figura 15. Ficha Informe

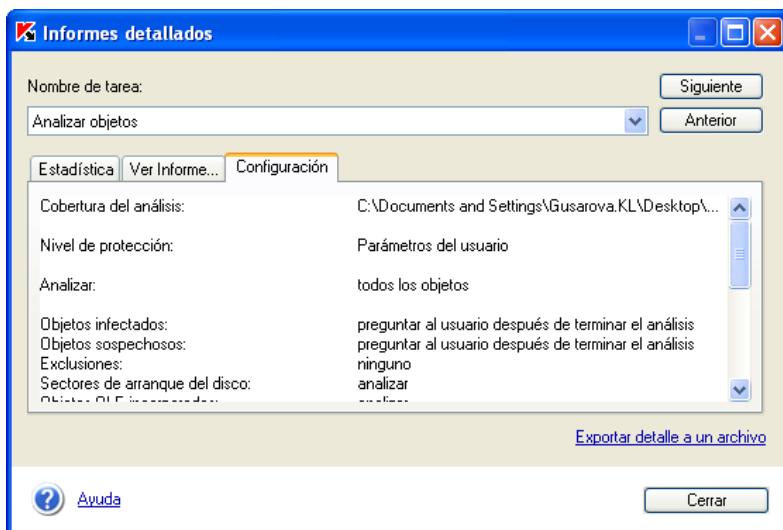


Figura 16. Configuración

ANEXO A. PREGUNTAS FRECUENTES

Este capítulo contiene las preguntas más frecuentes de los usuarios en relación con la instalación, la configuración y el funcionamiento de Kaspersky Anti-Virus. Intentaremos contestarlas aquí en detalle.



Pregunta: *¿Es posible utilizar Kaspersky Anti-Virus junto software antivirus de otros fabricantes?*

Para evitar conflictos, recomendamos desinstalar el software antivirus de otros fabricantes antes de instalar Kaspersky Anti-Virus.



Pregunta: *¿No repite Kaspersky Anti-Virus el análisis de los archivos ya analizados? Por qué*

Es cierto. Kaspersky Anti-Virus no analiza de nuevo los objetos que no han cambiado desde el análisis anterior.

Esto se consigue gracias a la utilización de nuevas tecnologías: iChecker e iStreams. Estas tecnologías permiten comprobar las sumas de control de los archivos en los flujos NTFS adicionales.



Pregunta: *¿Por qué Kaspersky Anti-Virus reduce ligeramente el rendimiento del equipo e impone una carga considerable en el procesador?*

La detección de virus es una operación de computación matemática intensiva que supone analizar estructuras, calcular sumas de control y convertir matemáticamente los datos. El principal recurso consumido por el programa antivirus es el tiempo de procesador y cada nuevo virus agregado a la base antivirus aumenta el tiempo de análisis general. Esto supone un sacrificio necesario para garantizar la seguridad de sus datos.

Para acelerar el análisis, otros fabricantes de antivirus excluyen de sus bases antivirus los virus menos fáciles de detectar, los menos frecuentes en la zona geográfica del distribuidor o los formatos de archivo más complicados (archivos PDF, por ejemplo).

Al contrario, en Kaspersky Lab pensamos que un antivirus debe ofrecer seguridad completa y real a sus usuarios. Creemos que la "protección parcial" es incluso peor que la falta de protección, en la que los usuarios adoptan precauciones personales.

Kaspersky Anti-Virus ofrece a sus usuarios la máxima protección. Por supuesto, los usuarios experimentados pueden acelerar el análisis

antivirus en detrimento de la seguridad global, ya que pueden desactivar el análisis de diferentes tipos de archivos, pero no recomendamos hacerlo a los usuarios que desean la mejor protección posible.

Con el fin de garantizar una máxima protección, Kaspersky Anti-Virus reconoce más de 40 tipos de archivos y programas de instalación y es capaz de detectar virus en más de 350 formatos de archivos diferentes. Esto es esencial para la seguridad antivirus, porque es posible encontrar código dañino escondido en cualquier formato de archivo conocido. Sin embargo, a pesar del incremento diario del número de virus encontrados por Kaspersky Anti-Virus (aproximadamente 30 nuevos virus diarios) y del número en aumento de formatos de archivos conocidos, esta nueva versión de nuestro producto funciona más rápido que las anteriores. Esto se consigue gracias a nuevas tecnologías exclusivas, como iChecker™ e i-Stream™, desarrolladas por Kaspersky Lab. Esta tecnología permite que un archivo sea comprobado tan sólo durante el primer análisis. En los análisis siguientes, el archivo no vuelve a ser comprobado, mientras no haya sido modificado desde entonces. Esto permite al programa antivirus aumentar drásticamente su rendimiento tras un primer análisis de los archivos.



Pregunta: *¿Por qué necesito la llave de licencia? ¿Funcionará mi copia de antivirus sin esta llave?*

No, Kaspersky Anti-Virus no puede funcionar sin una llave de licencia.

Si no se ha decidido todavía en comprar Kaspersky Anti-Virus, podemos proporcionarle una llave temporal (de demostración), que funcionará durante dos semanas (o un mes). La llave quedará bloqueada al finalizar este plazo.



Pregunta: *¿Qué ocurre cuando caduca mi licencia?*

Cuando su licencia caduque, Kaspersky Anti-Virus seguirá funcionando pero se deshabilitará la actualización de la base antivirus. La aplicación antivirus seguirá desinfectando objetos, pero sólo a partir de la antigua base antivirus.

En esta situación, póngase en contacto con su administrador de sistemas y con la organización donde adquirió Kaspersky Anti-Virus, o directamente con Kaspersky Lab, para obtener una ampliación de su licencia.



Pregunta: *Mi aplicación antivirus no funciona.*

¿Qué debo hacer?

En primer lugar, busque una solución a su problema en la documentación, en particular en esta sección o en nuestro sitio Web.

También le recomendamos contactar con el servicio de asistencia del distribuidor donde adquirió Kaspersky Anti-Virus, o escribir al servicio de soporte de Kaspersky Lab (support@kaspersky.com) o a la dirección que aparece en la información de la llave de licencia.

Para asegurarse de que recibirá una respuesta lo antes posible, siga estas sugerencias:

1. En el encabezado del mensaje, indique su sistema operativo, el nombre del componente que le causa problemas y describa brevemente el problema. Por ejemplo:
MS Windows 2000, Kaspersky Anti-Virus 5.0 for Windows Workstations, antivirus database updates do not work.
2. Escriba su mensaje en formato de texto plano. Evite enviar mensajes HTML.
3. Al principio del mensaje, especifique la versión exacta del sistema operativo y del paquete de distribución de Kaspersky Anti-Virus e indique su número de licencia.
4. Describa brevemente el problema con claridad. Tenga en cuenta que, cuando lee su correo, el personal del servicio de soporte no está informado de su problema. Tan sólo podrá intervenir si lo comprende plenamente y es capaz de reproducirlo.
5. Envíe los datos siguientes, comprimidos en un archivo único, al servicio de asistencia técnica:
 - Archivo registro del antivirus (ver sección 5.4.2 pág. 40);
 - Llave de licencia.
6. Asegúrese de especificar en su correo si su sistema contiene cualquiera de estos componentes:
 - Controladora SCSI;
 - Una marca de procesador muy antigua o muy reciente, o varios procesadores;
 - Menos de 64 Mb o más 2 GB de RAM.



Pregunta: ¿Por qué son necesarias las actualizaciones?

Hace varios años, los virus informáticos se propagaban a través de disquetes, y era suficiente instalar un programa antivirus y actualizar la base antivirus de vez en cuando para garantizar una protección segura de su equipo. Sin embargo, las últimas epidemias de virus se propagan en todo el mundo en pocas horas, y si las bases antivirus están desfasadas uses este comportamiento puede resultar inútil contra nuevas amenazas. Para poder resistir a los nuevos virus, es necesario actualizar la base antivirus de forma diaria.

Kaspersky Lab aumenta cada año la frecuencia de actualización de la base antivirus. Actualmente, es actualizada cada tres horas.

Además, se actualizan los módulos de aplicación, lo que permite corregir vulnerabilidades detectadas y aumenta las prestaciones del programa.



Pregunta: ¿Qué novedades aporta la versión 5.0?

La suite de productos Kaspersky Lab 5.0 incorpora un nuevo servicio de actualizaciones desarrollado de acuerdo con las necesidades de nuestros usuarios. Se realizó con el fin de aumentar la flexibilidad del proceso completo de actualización, desde la preparación de las actualizaciones en Kaspersky Lab hasta el momento en que los archivos pertinentes son actualizados en los equipos clientes.

Las ventajas del nuevo servicio de actualizaciones comprenden:

- *Las descargas existentes son guardadas cuando falla la conexión.* Ahora no es necesario volver a descargar las actualizaciones, cuando pierde y reanuda su conexión internet;
- *Una reducción a la mitad del tamaño de las actualizaciones acumulativas.* Una actualización acumulativa contiene la base antivirus completa, de forma que su tamaño supera de forma considerable el tamaño normal de las actualizaciones. El nuevo servicio utiliza una tecnología especial que permite aprovechar la base existente dentro de una actualización acumulativa.
- *Descarga acelerada desde Internet.* Kaspersky Anti-Virus selecciona al servidor de actualizaciones Kaspersky Lab más cercano geográficamente. Además, los servidores son valorados de acuerdo con su rendimiento, de forma que no tenga que conectarse a un servidor sobrecargado cuando otro está disponible y en espera.
- *"Listas negras" de llaves.* Se impide ahora a los usuarios sin la licencia de Kaspersky Anti-Virus utilizar el servicio de

actualizaciones. Los usuarios con licencia ya no sufren de la imposibilidad de conectarse a servidores de actualización sobrecargados.

Las organizaciones corporativas ahora pueden crear un servidor local de actualizaciones. Esta característica está diseñada para organizaciones en las que la red local permite unificar a los equipos protegidos por productos de Kaspersky Lab. En esta caso, cualquier equipo de la red local puede ser convertido en servidor de actualizaciones: recupera las actualizaciones en Internet y las comparte con los demás equipos de la red.



Pregunta: *¿Es posible para un intruso sustituir la base antivirus?*

Cada base antivirus utiliza una firma exclusiva que Kaspersky Anti-Virus comprueba cada vez que la consulta. Si la firma es incorrecta, o si su fecha es posterior a la de la fecha de caducidad de la licencia, Kaspersky Anti-Virus no utilizará la base de datos.

ANEXO B. CONTACTO CON EL SOPORTE TÉCNICO

El servicio de soporte de Kaspersky Lab está disponible para todos los usuarios registrados de Kaspersky Anti-Virus Personal en los casos siguientes:

- Piensa que la aplicación funciona de forma anormal o incorrecta.
- Kaspersky Anti-Virus ha detectado un archivo sospechoso con información valiosa pero lo mantiene bloqueado. Necesita continuar trabajando con este archivo.



Para enviar un mensaje al servicio de soporte acerca de cualquier fallo encontrado durante el funcionamiento del programa,

haga clic en [Escribir al servicio de soporte](#) en el panel izquierdo de la ficha **Soporte** (Figura 3) de la ventana principal de la aplicación.

Haga clic en el vínculo para abrir automáticamente una ventana del cliente de correo instalado en su equipo, por ejemplo MS Outlook, y cree un mensaje de correo con un archivo de texto con la descripción de su sistema y todas las informaciones necesarias relativas a Kaspersky Anti-Virus. Describa en detalle el problema que encontró mientras trabajaba con Kaspersky Anti-Virus y envíe el mensaje. El equipo de soporte se pondrá en contacto con Usted tan pronto como sea posible.

Si Kaspersky Anti-Virus colocó en cuarentena un archivo sospechoso, puede actualizar la base antivirus e intentar desinfectarlo (ver sección 5.4.1.1 pág. 37). Sin embargo, si no es posible desinfectar el objeto, pero desea recuperarlo tan pronto como sea posible, envíe el objeto para su examen en Kaspersky Lab. El archivo puede estar infectado por un virus desconocido, o resultar una falsa alarma.



Para enviar un archivo sospechoso individual para su examen por Kaspersky Lab,

Seleccione el archivo sospechoso en la ventana de **Cuarentena** (ver sección 5.4.1.1 pág. 37) y utilice el vínculo [Enviar a Kaspersky Lab para examen](#).

]-Haga clic en el vínculo para abrir automáticamente una ventana del cliente de correo instalado en su equipo, por ejemplo MS Outlook, y cree un mensaje de correo con el archivo sospechoso adjunto. Envíe el mensaje. Los expertos de Kaspersky Lab examinarán con atención el archivo transmitido e intentará recuperar todos los datos que contiene. Recibirá un informe completo de los resultados del examen.



Recuerde que no puede enviar más de tres archivos para su examen por Kaspersky Lab dentro del mismo día. Cada archivo debe haber sido analizado por Kaspersky Anti-Virus con una base de datos actualizada tres días antes como mucho antes de enviarlo.

Puede ocurrir que Kaspersky Anti-Virus no detecte archivos de los que está seguro que contienen un nuevo tipo de virus durante el análisis. Estos archivos pueden enviarse también a Kaspersky Lab para ser examinados.



Para enviar archivos que sospecha están infectados para su examen por Kaspersky Lab,

haga clic en [Enviar archivo para análisis](#) en el panel izquierdo de la ficha **Soporte** (ver Figura 3). Indique los archivos sospechosos en la ventana de exploración estándar.

El proceso de envío de un mensaje de correo a Kaspersky Lab es idéntico al que permite enviar objetos sospechosos en cuarentena.

ANEXO C. GLOSARIO

Este documento utiliza términos y conceptos propios del campo de la protección antivirus. Este glosario sirve de diccionario, con definiciones de estos conceptos. Para mayor comodidad, el glosario se presenta en orden alfabético.

A

Archivos comprimidos: Archivos que contienen un programa con instrucciones para ser ejecutadas por el sistema operativo.

Análisis a petición: Modo de funcionamiento de la aplicación, es iniciado por el usuario y realiza un análisis de los archivos de todo tipo que residen en su equipo.

Actualización: proceso que sustituye o completa nuevos archivos (la base antivirus o los módulos de aplicación) descargados de los servidores de actualización de Kaspersky Lab.

B

Base antivirus: Una base de datos creada por Kaspersky Lab que contiene una descripción detallada de todos los virus existentes hasta el momento, junto con los métodos de detección y desinfección utilizados. Nuestra base antivirus es actualizada regularmente con información de virus nuevos, a medida que aparecen; para mantener su equipo constantemente protegido, es necesario *actualizar* su base antivirus con la mayor frecuencia posible.

Bases de correo: Bases de datos en formato especial que permiten almacenar mensajes de correo en su equipo. Cada mensaje entrante/saliente se conserva en la base después de su recepción o envío. Estas bases son examinadas durante un análisis completo del equipo. En el modo de protección en tiempo real, Kaspersky Anti-Virus analiza todos los correos entrantes y salientes a medida que son enviados o recibidos.

C

Compilaciones de archivos: Archivos que contienen uno o más archivos los cuales pueden ser, a su vez, otras compilaciones de archivos.

Copia de seguridad: Creación de una copia de seguridad de un archivo en la carpeta BACKUP antes de procesarlo (desinfección o eliminación). Este archivo puede ser posteriormente restaurado desde su copia de seguridad, por ejemplo, para ser analizado con una versión actualizada de la base antivirus.

Cuarentena: Carpeta en la que Kaspersky Anti-Virus desplaza todos los *objetos posiblemente infectados* encontrados durante un *análisis completo del equipo* o en modo de *protección en tiempo real*.

Cuarentena (desplazar a la carpeta de cuarentena): Tratamiento aplicado a un *objeto infectado* o *posiblemente infectado* que bloquea el acceso al objeto y lo mueve a una carpeta de cuarentena para su tratamiento posterior.

D

Desinfección: Método de cura de objetos infectados. La desinfección se traduce por la supresión parcial o completa del código dañino dentro de los datos infectados, o por un diagnóstico según el cual no es posible desinfectarlos. Los objetos son desinfectados a partir de registros incluidos en la *base antivirus*.

Desinfección de objetos al reiniciar: método de cura de objetos infectados que otros programas están utilizando cuando la aplicación intenta desinfectarlos. La aplicación crea una copia del objeto infectado, desinfecta la copia y la utiliza para sustituir el objeto original durante el arranque siguiente. En sistemas operativos MS Windows 9x, la desinfección de objetos con nombres largos durante el arranque obliga a reemplazarlos con objetos desinfectados con nombres de archivos cortos. Esto puede causar un funcionamiento incorrecto de las aplicaciones que utilizan objetos desinfectados de esta forma.

E

Eliminación de objeto: Método de cura de un objeto. Eliminar un objeto significa suprimirlo físicamente de su equipo. Este método es recomendado para objetos que no pueden ser desinfectados por una razón u otra.

Exclusiones: Configuración del usuario que permite excluir algunos objetos del análisis. Es posible personalizar las reglas de exclusión de la *protección en tiempo real* y del *análisis a petición*. Por ejemplo, puede excluir las compilaciones de archivos del alcance del análisis durante un análisis completo, o especificar con máscaras los tipos de archivos que no desea analizar.

F

Falsa alarma: Situaciones en las que la aplicación antivirus marca un objeto como infectado, debido a que el código que contiene se parece a un virus.

Falso positivo: vea *falsa alarma*

H

Heurístico (analizador de código): Tecnología de gran eficacia que permite a un programa antivirus detectar virus desconocidos. Los

objetos sospechosos de infección por un virus desconocido o por la mutación de un virus existente son identificados gracias a esta tecnología.

I

Ignorar: Tratamiento que prohíbe el acceso al objeto (con la protección en tiempo real activa) y registra información acerca del objeto en el informe de operaciones de programa, pero sin realizar ninguna otra acción sobre el objeto.

Indicador de protección antivirus: El estado actual de la protección antivirus que caracteriza el nivel de seguridad de su equipo.

Infectado (objeto): Objeto que contiene un virus. Le recomendamos no intentar abrir estos objetos, porque pueden producir una infección de su equipo. Si se encuentra un objeto infectado, le recomendamos *desinfectarlo* con Kaspersky Anti-Virus y, si esto no es posible, eliminarlo.

L

Llave de licencia – Archivo con extensión *.key* que sirve de "llave" personal, necesaria para el funcionamiento correcto de Kaspersky Anti-Virus. La llave de licencia se incluye dentro del kit de distribución si adquiere su copia de Kaspersky Anti-Virus en un distribuidor de Kaspersky Lab. Si adquiere su producto en línea, recibirá su llave de licencia por correo electrónico. Kaspersky Anti-Virus NO FUNCIONARÁ sin la llave de licencia.

Llave de licencia de reserva: llave de licencia instalada para permitir el funcionamiento de Kaspersky Anti-Virus, pero que todavía no está activada. La llave de reserva es activada en cuanto caduca la llave de licencia actual.

M

Malware: la palabra es la contracción de "software malicioso" (en inglés, "malicious software") y designa de forma genérica tanto virus, gusanos como troyanos.

Máxima protección: Nivel que ofrece la máxima protección posible por parte de Kaspersky Anti-Virus. En este modo de protección, todos los archivos almacenados en discos fijos, extraíble o de red (que estén conectados a su equipo) son analizados en busca de virus.

Máxima velocidad: Nivel de protección que permite analizar tan sólo los *objetos susceptibles de ser infectados*. Esto reduce el tiempo de análisis de forma significativa.

Memoria del equipo: Memoria RAM instalada en su equipo.

Módulos de programa: Archivos incluidos en la distribución de Kaspersky Anti-Virus. Cada uno de estos módulos corresponde a una función

específica de Kaspersky Anti-Virus, como la *protección en tiempo real*, *el análisis a petición*, *la actualización*.

O

Objetos ejecutados al iniciar el sistema operativo- Un conjunto de programas necesarios para iniciar y mantener en funcionamiento el sistema operativo y otros programas instalados en su equipo. Su sistema operativo ejecuta estos objetos en cada inicio. Algunos virus infectan los objetos utilizados en el inicio del sistema, e impiden la carga del sistema operativo.

Objeto sospechoso: objeto que contiene código modificado de un virus conocido, o que recuerda a un virus, pero no está actualmente fichado por Kaspersky Lab.

OLE (objeto): Objeto vinculado o incorporado en otro archivo. Kaspersky Anti-Virus analiza estos objetos en busca de virus. Por ejemplo, una hoja de cálculo Microsoft Excel incorporada en un documento Microsoft Word es un objeto OLE analizado por Kaspersky Anti-Virus.

P

Periodo de licencia: Periodo durante el cual goza del derecho de uso de Kaspersky Anti-Virus. El periodo de licencia viene definido por la llave de licencia y es, como regla general, de un año a contar de la fecha de compra. Tras caducar la licencia, el producto seguirá funcionando pero no podrá actualizar la *base antivirus*.

Posiblemente infectado (objeto): Objeto que contiene el código de un virus desconocido o que recuerda a otro conocido. Los objetos posiblemente infectados son detectados por el *analizador de código heurístico*.

Potencialmente infectable (objeto): Objeto susceptible de ser infectado. Estos objetos son normalmente archivos ejecutables, por ejemplo los archivos con extensiones *com*, *exe* y otras.

Prevención: Un conjunto de medidas que deben tomarse para evitar la penetración de virus en su equipo. La prevención de virus abarca la protección antivirus completa y la obtención de actualizaciones para la aplicación.

Protección en tiempo real: Modo de funcionamiento de Kaspersky Anti-Virus que se inicia automáticamente con el sistema, en el que todos los objetos son analizados cuando son leídos, escritos o ejecutados. Si un objeto está identificado como *infectado* o *sospechoso*, Kaspersky Anti-Virus prohíbe su acceso e intenta curarlo (por desinfección, cuarentena, eliminación, etc.) o pregunta al usuario por la acción que debe tomar.

R

Recomendado: Nivel de protección antivirus que utiliza la configuración recomendada por Kaspersky Lab, y asegura una protección óptima de su equipo. Este nivel corresponde al de la configuración predeterminada.

Recuperación, restauración: Desplazamiento de un archivo de la *Cuarentena* a su carpeta original, donde estaba ubicado antes de pasar a cuarentena, de ser desinfectado o eliminado.

Respaldo: Directorio que contiene copias de seguridad de los objetos eliminados y desinfectados.

Revisión (Parche): Compilación de archivos empleados para la actualización de programas. Las revisiones son descargadas de Internet e instaladas en su equipo.

S

Sector de arranque: Un área especial del disco donde se encuentra la aplicación cargador del sistema operativo.

Sector de arranque del disco: Una zona del disco duro o de cualquier soporte extraíble (por ejemplo, un disquete o un CD-ROM). Existen *virus de arranque* que infectan los sectores de arranque del disco. Kaspersky Anti-Virus analiza los sectores de arranque y los *desinfecta* en caso de detectar una infección.

Secuencias de comandos: Una aplicación con secuencias de instrucciones que es posible incorporar dentro de una página Web, por ejemplo, para su ejecución por el navegador Web (Microsoft Internet Explorer, por ejemplo), o también presentar como archivo independiente, par su ejecución por el sistema operativo Windows. En el modo de protección en tiempo real, Kaspersky Anti-Virus supervisa la ejecución de las secuencias de comandos, las desactiva y las analiza en busca de virus. En función de los resultados del análisis, puede por ejemplo autorizar o prohibir la ejecución de las secuencias de comandos.

Servidores de actualizaciones: Una lista de servidores HTTP- y FTP- actualizados regularmente por Kaspersky Lab, desde los que la aplicación recupera la versión más reciente de la base antivirus para su equipo.

Sólo informar: en este modo, cuando la aplicación detecta objetos infectados o sospechosos, los bloquea (en el modo de protección en tiempo real) e informa de su detección en el diario de informes de tareas.

Sospechoso (objeto): ver *objeto posiblemente infectado*.

U

Unidades virtuales (discos RAM): zona de memoria RAM dentro de un equipo personal que simula la presencia de un disco físico dentro del equipo.

V

Virus de arranque: Un virus que infecta los *sectores de arranque* de los discos y del sistema operativo instalado en su equipo. Durante un arranque del sistema, el virus obliga al sistema a cargarlo en memoria y a traspasar el control desde el cargador original al código del virus.

Virus desconocido: Virus nuevo que no aparece registrado en la *base antivirus*. En general, Kaspersky Anti-Virus detecta los virus desconocidos con el *analizador de código heurístico*: los objetos infectados por estos virus son marcados como *posiblemente infectados*.

ANEXO D. KASPERSKY LAB

Fundado en 1997, Kaspersky Lab se ha convertido en un líder reconocido en tecnologías de seguridad de la información. Es fabricante de una amplia gama de productos software para la seguridad de los datos, y aporta soluciones completas de alto rendimiento para la protección de equipos y redes contra todo tipo de programas dañinos, correo no solicitado o indeseable, y ataques de red.

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

Hoy día, Kaspersky Lab tiene contratados a más de 250 especialistas, cada uno de los cuales es un experto en tecnología antivirus, con 9 de ellos en posesión de un M.B.A., otros 15 con grado de Doctor, y dos expertos miembros permanentes de la CARO (Computer Anti-Virus Researcher's Organization).

Kaspersky Lab ofrece soluciones punteras en seguridad, de acuerdo con su experiencia y conocimiento acumulados en más de 14 años de lucha antivirus. Su análisis avanzado de la actividad vírica permite a la organización ofrecer una protección completa contra amenazas actuales e incluso futuras. La resistencia a ataques futuros es la directiva básica de todos los productos Kaspersky Lab. Constantemente, sus productos superan los de muchos otros fabricantes a la hora de asegurar una cobertura antivirus integral tanto a los usuarios domésticos, como a los usuarios corporativos.

Años de duro trabajo han convertido la empresa en uno de los fabricantes líderes de software 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 componentes conectados en red: estaciones de trabajo, servidores de archivos, sistemas de correo, cortafuegos y pasarelas Internet, así como equipos portátiles. Sus herramientas de administración adaptadas y sencillas utilizan los avances de la automatización para una rápida protección antivirus de toda la organización. Numerosos fabricantes conocidos utilizan el núcleo de Kaspersky Anti-Virus®: Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israel), Sybari (EEUU), G Data (Alemania), Deerfield (EEUU), Alt-N (EEUU), Microworld (India), BorderWare (Canadá), etc.

Los clientes de Kaspersky Lab se benefician de un amplio abanico de servicios adicionales que garantizan no sólo un funcionamiento estable de nuestros productos sino también la compatibilidad con cualquier necesidad específica de negocios. La base antivirus de Kaspersky Lab se actualiza en tiempo real cada 3 horas. Nuestra organización ofrece a sus usuarios un servicio de asistencia

técnica de 24 horas, disponible en numerosos idiomas, capaz de adaptarse a su clientela internacional.

D.1. Otros productos Kaspersky Lab

Kaspersky Anti-Virus[®] Personal

Kaspersky Anti-Virus[®] Personal protege los equipos domésticos bajo Windows 98/ME/2000/NT/XP contra todo tipo de virus conocidos, incluyendo software de interceptación ilegal ("Riskware"). La aplicación vigila en permanencia todos los posibles canales de penetración de virus, como el correo electrónico, Internet, los disquetes, los CD, etc. Los virus desconocidos son detectados con eficacia y procesados mediante un sistema de análisis de datos heurístico. Puede utilizar (de forma conjunta o por separado) dos modos de funcionamiento de la aplicación, que son:

- **Protección antivirus en tiempo real:** análisis antivirus de todos los objetos que son ejecutados, abiertos o guardados dentro del equipo protegido.
- **Análisis a petición:** análisis y desinfección del equipo completo, o de discos, archivos o carpetas seleccionados. El análisis a petición puede ser iniciado manualmente desde la interfaz de usuario, o automáticamente, de acuerdo con una planificación.

Kaspersky Anti-Virus Personal no examina los objetos ya analizados que no han cambiado desde el análisis anterior. Esta regla se aplica ahora no sólo en la protección en tiempo real sino también en el análisis a petición. Esta característica **mejora considerablemente la velocidad y rendimiento de la aplicación.**

Kaspersky Anti-Virus Personal ofrece una protección segura contra los virus que intentan penetrar en los equipos por medio de mensajes electrónicos. La aplicación se hace cargo automáticamente del análisis y desinfección de todos los mensajes de correo entrantes (POP3) y salientes (SMTP) y detecta con eficacia los virus presentes en bases de correo.

Kaspersky Anti-Virus Personal reconoce más de 700 formatos de compilaciones y archivos comprimidos y se hace cargo automáticamente del análisis del contenido y eliminación de código dañino en archivos comprimidos **ZIP, CAB, RAR y ARJ.**

Es posible establecer la configuración de la aplicación de acuerdo con uno de los tres niveles predeterminados: **Máxima protección, Recomendado y Máxima velocidad.**

La base antivirus es actualizada cada tres horas. La entrega de la base de datos está garantizada incluso si se interrumpe o cambia de conexión internet durante la descarga.

Kaspersky Anti-Virus® Personal Pro

Este paquete ha sido diseñado para ofrecer una protección antivirus completa a equipos domésticos con Windows 98/ME, Windows 2000/NT, Windows XP, así como aplicaciones MS Office. Kaspersky Anti-Virus® Personal Pro incluye una aplicación de uso sencillo para la recuperación automática de las actualizaciones diarias de la base antivirus y de los módulos de aplicación. Un analizador heurístico de segunda generación es capaz de detectar incluso los virus desconocidos. Una interfaz sencilla y ergonómica para modificar fácilmente la configuración del programa, con una máxima comodidad para el usuario.

Kaspersky Anti-Virus® Personal Pro:

- **análisis a petición** de discos extraíbles iniciado por el usuario;
- **protección en tiempo real automática** que cubre el análisis de todos los archivos en ejecución;
- **filtro de correo**: analiza y desinfecta automáticamente todo el tráfico de correo entrante y saliente (POP3 y SMTP) y detecta eficazmente los virus en las bases de correo;
- **bloqueador de comportamiento** que garantiza una protección al 100% contra los virus de macro en aplicaciones MS Office.
- **análisis antivirus** de más de 900 formatos de compilaciones de datos y archivos comprimidos, y se hace cargo automáticamente del análisis del contenido y eliminación de código dañino en archivos con formato **ZIP, CAB, RAR y ARJ**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker es un cortafuegos personal diseñado para proteger un equipo con sistema operativo Windows. Protege su equipo contra el acceso no autorizado a datos y contra ataques externos a través de Internet o redes locales vecinas.

Kaspersky® Anti-Hacker monitoriza el comportamiento en red TCP/IP de todas las aplicaciones de su equipo. En presencia de cualquier acción sospechosa por parte de una aplicación, la aplicación bloquea su acceso a la red. Esto asegura una privacidad mejorada del 100% de los datos confidenciales almacenados en su equipo.

La tecnología SmartStealth™ impide que los piratas puedan detectar su equipo desde el exterior. En este modo invisible, la aplicación funciona de forma transparente para mantener su equipo protegido mientras navega por el Web: la

aplicación ofrece toda la transparencia y facilidad de acceso a la información que pueda esperar.

- Kaspersky[®] bloquea los ataques maliciosos más frecuentes, y monitoriza las tentativas de análisis de puertos de su equipo.
- La configuración de la aplicación se reduce a elegir entre 5 niveles de seguridad. De forma predeterminada, la aplicación se inicia en modo aprendizaje, que configura automáticamente su sistema de seguridad, en función de sus respuestas a diferentes eventos. De este modo, la protección se ajusta a sus preferencias específicas y a sus necesidades particulares.

Kaspersky[®] Security para PDA

Kaspersky[®] Security para PDA ofrece protección antivirus de los datos almacenados en equipos PDA con sistema operativo Palm o Windows CE. También protege contra daños en cualquier información que transfiera desde su PC o tarjeta de expansión, archivos ROM y bases de datos. El paquete software incluye una combinación óptima de las herramientas antivirus siguientes:

- **analizador antivirus** para analizar a petición los datos almacenados tanto en el PDA como en una tarjeta de expansión;
- **monitor antivirus** que intercepta los virus en archivos copiados de otros portátiles o transferidos mediante la tecnología HotSync[™].

Kaspersky[®] Security para PDA protege su portátil (PDA) contra intrusiones no autorizadas mediante técnicas de cifrado del acceso a los dispositivos y datos almacenados en tarjetas de memoria.

Kaspersky Anti-Virus[®] Business Optimal

Este paquete ofrece una solución de seguridad adaptada a redes corporativas de tamaño pequeño y medio.

Kaspersky Anti-Virus[®] Business Optimal incluye protección antivirus a todos los niveles¹ para:

- *Estaciones de trabajo* con Windows 98/ME, Windows NT/2000/XP Workstation y Linux;
- *Servidores de archivos y aplicaciones* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD y OpenBSD, y Linux;

¹ En función del tipo de kit de distribución.

- *Clientes de correo:* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail y Qmail;
- *Pasarelas Internet:* CheckPoint Firewall -1; MS ISA Server.

El kit de distribución de Kaspersky Anti-Virus® Business Optimal incluye Kaspersky® Administration Kit, una herramienta *exclusiva para operaciones automatizadas de despliegue y administración.*

Puede elegir cualquiera de estas aplicaciones antivirus de acuerdo con los sistemas operativos y aplicaciones que utiliza.

Kaspersky® Corporate Suite

Este paquete aporta protección antivirus completa y escalable a redes corporativas de cualquier complejidad. El paquete de componentes ha sido desarrollado para proteger cualquier integrante de una red corporativa, incluso en entornos mixtos. Kaspersky® Corporate Suite es compatible con la mayoría de los sistemas operativos y aplicaciones instalados en una empresa. Todos los componentes del paquete son administrados desde una consola con interfaz de usuario unificada. Kaspersky® Corporate Suite ofrece un sistema de protección seguro y de alto rendimiento que es totalmente compatible con las necesidades de su configuración de red.

Kaspersky® Corporate Suite ofrece protección antivirus para:

- *Estaciones de trabajo* Windows 98/ME, Windows NT/2000/XP y Linux;
- *Servidores de archivos y aplicaciones* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD y Linux;
- *Clientes de correo*, Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim y Qmail;
- *Pasarelas Internet:* CheckPoint Firewall -1; MS ISA Server;
- *Equipos portátiles (PDA)*, con Windows CE y Palm OS.

El kit de distribución de Kaspersky® Corporate Suite incluye Kaspersky® Administration Kit, una herramienta *exclusiva para operaciones automatizadas de despliegue y administración.*

Puede elegir cualquiera de estas aplicaciones antivirus de acuerdo con los sistemas operativos y aplicaciones que utiliza.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam es una aplicación avanzada diseñada para ayudar a las corporaciones con redes de tamaño pequeño o mediano a luchar contra la propagación de correos no deseados (spam). El producto combina una

tecnología revolucionaria de análisis lingüístico con todos los métodos modernos de filtrado del correo (incluyendo listas negras y rojas y funciones de análisis formal de los mensajes). Su combinación única de servicios permite a los usuarios identificar y destruir hasta un 95% del tráfico no deseado.

Kaspersky® Anti-Spam actúa como un filtro instalado a la entrada de la red, desde donde comprueba el tráfico entrante de mensajes, en busca de objetos identificados como correo basura. La aplicación es compatible con cualquier sistema de mensajería existente en las instalaciones del cliente, en un servidor de correo existente o dedicado.

El alto rendimiento de Kaspersky® Anti-Spam se garantiza con la actualización diaria de las bases de filtrado de contenidos, a partir de muestras proporcionadas por los especialistas del laboratorio lingüístico.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal está diseñado para proteger los usuarios de Microsoft Outlook y Microsoft Outlook Express contra los mensajes de correo no deseado (spam).

La aplicación Kaspersky® Anti-Spam Personal es una herramienta potente que asegura la detección del correo no deseado en el flujo de mensajes de correo entrantes por los protocolos POP3 y IMAP4 (sólo para Microsoft Outlook).

El filtrado incluye el análisis de todos los atributos del mensaje (direcciones y encabezados del emisor y receptor), el filtrado de contenidos (análisis del contenido del mensaje, con el asunto y los adjuntos), así como algoritmos lingüísticos y heurísticos exclusivos.

El alto rendimiento de la aplicación se garantiza con la actualización diaria de las bases de filtrado de contenidos, a partir de las muestras proporcionadas por los especialistas del laboratorio lingüístico.

D.2. Cómo encontrarlos

Si tiene cualquier pregunta, comentario o sugerencia, no dude en ponerse en contacto con nuestros distribuidores o directamente con el Soporte técnico de Kaspersky Lab. Estaremos encantados de atenderle por teléfono o por correo electrónico acerca de cualquier asunto relacionado con nuestros productos. Todas sus recomendaciones y sugerencias serán estudiadas con atención.

Asistencia técnica	Encontrará información de asistencia técnica en la dirección http://www.kaspersky.com/supportinter.html
--------------------	--

Información	<p>WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com</p>
-------------	---

ANEXO E. ÍNDICE

Actualización de la Base antivirus,
45

Contrato de licencia, 13

CUARENTENA

ENVIAR UN ARCHIVO PARA SU

EXAMEN EXPERTO, 49

Llave de licencia, 45

Presentación del producto

comprar en línea, 13

Respaldo

trabajar con archivos, 38

Servicio de soporte técnico, 14, 65

Software dañado

gusanos, 5

troyanos, 5

virus, 5

ANEXO F. CONTRATO DE LICENCIA

Contrato de licencia de usuario estándar

IMPORTANTE PARA TODOS LOS USUARIOS: LEA ATENTAMENTE EL SIGUIENTE CONTRATO DE LICENCIA ("CONTRATO") PARA EL SOFTWARE ESPECIFICADO ("SOFTWARE") PRODUCIDO POR KASPERSKY LABS. ("KASPERSKY LABS").

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

SI HA COMPRADO ESTE SOFTWARE EN UN MEDIO FÍSICO, Y ROTO EL ESTUCHE DEL CD, USTED ("UN INDIVIDUO O UNA ENTIDAD JURÍDICA") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. SI NO ACEPTA TODOS LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO NO ROMPA EL ESTUCHE DEL CD, NI COPIE, INSTALE O USE ESTE SOFTWARE. PUEDE DEVOLVER ESTE SOFTWARE Y OBTENER EL REINTEGRO DEL PRECIO. SU DERECHO DE DEVOLUCIÓN Y REINTEGRO EXPIRA 30 DÍAS DESPUÉS DE COMPRAR EL SOFTWARE DE UN DISTRIBUIDOR O VENDEDOR AUTORIZADO POR KASPERSKY LABS. EL DERECHO A DEVOLUCIÓN Y REINTEGRO SÓLO SE EXTIENDE AL COMPRADOR ORIGINAL.

De aquí en adelante en todas las referencias al "Software" se estimará que incluye la llave de activación de software ("Archivo Llave de Identificación") proporcionado por Kaspersky Lab como parte del Software.

1. Concesión de licencia. Si los gastos de licencia han sido pagados, y de acuerdo con los términos y condiciones de este Contrato, Kaspersky Lab le concede por el presente Contrato un derecho de uso no exclusivo y no transferible de una copia de la versión especificada del Software y documentación que la acompaña ("Documentación") únicamente para sus propios fines de negocio. Puede instalar una copia del Software en un equipo, puesto de trabajo, agenda personal u otro dispositivo electrónico para el que el Software ha sido diseñado (cada uno es un "Sistema cliente"). Si el Software se licencia bajo la forma de un conjunto de programas con más de un producto Software especificado, esta licencia se aplicará a todos los productos Software especificados, sin perjuicio de todas las limitaciones o condiciones de uso

especificadas en la lista de precios o en el embalaje correspondiente a cada uno de estos productos Software.

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

El Software está "en uso" en un Sistema cliente cuando está cargado en la memoria temporal (es decir, memoria de acceso-aleatorio o RAM) o instalado en la memoria permanente (ej. disco duro, CDRom, u otro dispositivo de almacenamiento) de ese Sistema cliente. 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. Usted mantendrá un registro con el número y ubicación de todas las copias del Software y Documentación y tomará las precauciones necesarias para impedir que el Software sea copiado o utilizado sin autorización.

1.1.2 Si vende el Sistema cliente en que el Software está instalado, se asegurará que se han borrado previamente todas las copias del Software.

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

1.1.4 No debe corregir errores, modificar, adaptar o traducir ni crear obras derivadas del Software ni autorizar a terceras partes a copiarlo (fuera de lo expresamente autorizado en este documento).

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

1.1.6 No deberá utilizar este Software con herramientas automáticas, semiautomáticas o manuales diseñadas para crear firmas de virus, rutinas de detección de virus, ni cualquier otra información o código para la detección de código o de datos dañinos.

1.2 Uso en Modo Servidor. Sólo puede usar el Software en un Sistema cliente o en un Servidor ("Servidor") dentro de un entorno multiusuario o en red ("Modo Servidor") si tal uso está autorizado en la lista de precios o en el embalaje del Software. Se requiere una licencia separada para cada Sistema cliente o "Terminal" que puedan conectarse al Servidor en un momento dado; esta

obligación no depende de si tales Sistemas Clientes o "terminales" autorizados se conectan simultáneamente, ni si acceden y usan el Software realmente. La utilización de herramientas software o hardware para reducir el número de Sistemas Cliente o "Terminales" que acceden o utilizan el Software directamente (por ejemplo, "multiplexación" o "agrupación" de software o hardware) no reduce el número de licencias requeridas, es decir: el número requerido de licencias será igual al número de entradas distintas del software o hardware multiplexado o agrupado. Si el número de Sistemas Cliente o "Terminales" que puedan conectarse al Software supera el número de licencias adquiridas, debe disponer de un mecanismo razonable para garantizar que el uso del Software cumple con las limitaciones especificadas para la licencia obtenida. Esta licencia le autoriza a crear e instalar copias autorizadas de la Documentación para cada sistema cliente o "puesto de trabajo" que lo necesite para su uso legítimo, con la condición de que cada copia contenga todos los avisos de la propiedad de Documentación.

1.3 Número de licencias: Si la licencia del Software se establece de acuerdo con las condiciones de un licencia por volumen, descritas en la factura del producto o en el paquete de Software, puede reproducir, usar o instalar tantas copias adicionales del Software en tantos Sistemas Cliente como está especificado en las condiciones de la licencia. Debe tener mecanismos razonables para garantizar que el número de Sistemas Cliente en que el Software está instalado no exceda el número de licencias que ha obtenido. Esta licencia le autoriza a reproducir o instalar una copia de la Documentación por cada copia adicional del software autorizada por la licencia por volumen, a condición de que cada copia contenga todos los avisos de propiedad del Documento.

2. Duración. Este Contrato es válido durante [un (1)] año si no y hasta que finalice antes de lo especificado en este documento. Este Contrato terminará automáticamente si no respeta cualquiera de las condiciones, limitaciones u otros requisitos especificados en este contrato. Si el Contrato carecerá de vigor o expirará, debe destruir inmediatamente todas las copias del Software y la Documentación. Puede terminar este Contrato en cualquier momento destruyendo todas las copias del Software y la Documentación.

3. Soporte.

(i) Kaspersky Lab le proporcionará los servicios de soporte ("Servicios de soporte") para un período de un año como está especificado abajo:

(a) Pago de la cuota del Soporte actual; y:

(b) Cumplimentación del Formulario de Suscripción para el servicio de soporte suministrado con este Contrato o disponible en el sitio Web de Kaspersky Lab que le exigirá que incluya el archivo Llave de Identificación proporcionado por Kaspersky Lab según este Contrato. Si usted ha satisfecho esta condición o no para el suministro de Servicios de soporte estará a la discreción absoluta de los servicios de soporte.

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

(iii) Al completar el Formulario de Suscripción de los Servicios de soporte acepta los términos de la Política de privacidad de Kaspersky Lab que acompaña este Contrato, y acepta explícitamente que los datos se transmitan a otros países como especificado en la Política de privacidad.

(iv) "Servicio de soporte" significa:

(a) Actualizaciones diarias de bases antivirus;

(b) Actualizaciones gratuitas del software, incluido actualizaciones de la versión de antivirus;

(c) Soporte técnico extendido a través de correo electrónico y teléfono proporcionados por Vendedor y/o Proveedor;

(d) Detección de virus y actualizaciones para su desinfección durante las 24-horas.

4. 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.

5. Confidencialidad. Usted acepta que el Software y la Documentación, incluidos el diseño y estructura de los programas individuales y el Archivo Llave de Identificación, constituyen información confidencial y propietaria de Kaspersky Lab. No debe desvelar, proporcionar u ofrecer la información confidencial en cualquiera de sus formas a terceras partes sin autorización escrita de Kaspersky Lab. Debe tomar medidas necesarias de seguridad para proteger la información confidencial, y proteger la seguridad del Archivo Llave de Identificación lo mejor posible.

6. Garantía limitada.

(i) Kaspersky Lab le garantiza que durante [90] días desde la primera instalación del Software éste funcionará seguro, de acuerdo con lo que se dice de su funcionalidad en la Documentación, si se ejecuta de forma apropiada y de la manera especificada en la Documentación.

(ii) Usted acepta toda la responsabilidad por la selección de este Software para que satisfaga todas sus necesidades. Kaspersky Lab no garantiza que el Software y/o la Documentación son adecuados para sus necesidades ni que su funcionamiento está libre de interrupciones o de errores;

(iii) Kaspersky Lab no garantiza que este Software identifique todos los virus conocidos, ni que 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 periodo de la garantía. Debe proporcionar toda la información que pueda ser necesaria para ayudar al Proveedor a determinar el objeto dañado;

(v) La garantía mencionada en (i) no se aplicará si usted (a) ha hecho cualesquiera modificaciones sobre este Software o las ha causado sin permiso de Kaspersky Lab, (b) use el Software de una manera no aplicable © use el Software de manera 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 la provisión o provisión intentada, ausencia o tardanza en la provisión del Software o la Documentación que puedan tener efecto entre Kaspersky Lab y usted, excepto los casos especificados en este párrafo (v), o se implicarían o se incorporarían a este Contrato o cualquier contrato colateral, si por el estatuto, derecho común o cualquier otra forma todos se excluyen por el presente (incluido, pero sin limitarse a, condiciones implícitas, garantías u otros términos acerca de la calidad satisfactoria, conveniencia o competencia y cuidado necesarios).

7. Responsabilidad

(i) Nada en este Contrato excluirá o limitará la responsabilidad de Kaspersky Lab por (i) acto delictuoso de engaño, (ii) muerte o daños personales debidos al incumplimiento de obligaciones de leyes sanitarias o violación negligente de este Contrato, (iii) cualquier violación de las obligaciones implicadas por s.12 Sale of Goods Act 1979 ó s.2 Supply of Goods and Services Act 1982; o (iv) cualquier responsabilidad que no puede excluirse por ley.

(iii) Según el párrafo (i), el Proveedor no será responsable (por contrato, acto delictuoso, devolución o cualquier otra razón) por cualquiera de las siguientes pérdidas o daños (incluso si tales pérdidas o daños fueron previstos, previsibles, conocidos, sin limitación):

(a) Pérdida de ingresos;

(b) Pérdida de beneficios actuales o anticipadas (incluido 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 de información, su daño o corrupción; o:

(j) Cualquier otra pérdida o daño incidental o consecuencial causado de cualquier forma (incluido, para quitar dudas, pérdida o daño del tipo especificado en el párrafo (ii), (a) - (ii), (i).

(iv) Según al párrafo (i), la responsabilidad de Kaspersky Lab (en el contrato, acto delictuoso, restitución o cualquier otra forma), que es resultado de o está conectada con la provisión del Software, se limitará en todas las circunstancias a un monto no mayor del que Usted pagó por el Software.

8. La lectura e interpretación de este Contrato se regirá de acuerdo con las leyes de Inglaterra y Gales. Las partes se someten por el presente a la jurisdicción de las cortes de Inglaterra y Gales y tanto Kaspersky Lab como el demandante tienen derecho a iniciar procedimientos en cualquier corte de jurisdicción competente.

9. (i) El Contrato contiene el acuerdo de las partes respecto al sujeto de este Contrato y sustituye todos los anteriores acuerdos, compromisos y promesas hechos oralmente o por escrito entre Usted y Kaspersky Lab o que pueden ser implicados de algo escrito o dicho en las negociaciones entre nosotros o nuestros representantes antes de firmar este Contrato. Este contrato contiene el pleno conocimiento de las partes en cuanto a su contenido y reemplaza todos y cualquier declaración, acuerdo o compromiso entre Usted y Kaspersky Lab, tanto oral o como por escrito o formulado en negociaciones entre nosotros o con nuestros representantes antes de este Acuerdo y para los contratos entre las partes respecto a las cuestiones antedichos que cesan a partir del momento en que este Contrato entre en vigor. Excepto lo especificado en los párrafos (ii) - (iii), no tiene derecho a ningún reembolso respecto a una declaración falsa en la que estaba basándose usted firmando este Contrato ("Falseamiento") y Kaspersky Lab no será responsable por algo que exceda los términos especificados en este Contrato.

(ii) Nada en este Contrato excluirá o limitará la responsabilidad de Kaspersky Lab por cualquier Falseamiento hecho por él sabiendo que era falso.

(iii) La responsabilidad de Kaspersky Lab por Falseamiento en un tema fundamental, incluida la capacidad del fabricante para cumplir sus obligaciones bajo este Contrato, estará sujeto a la limitación del conjunto de responsabilidades especificado en el párrafo 7(iii).