

KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



Kaspersky Anti-Virus® 5.0 for Windows Workstations

Manual del administrador

KASPERSKY ANTI-VIRUS[®] 5.0
FOR WINDOWS WORKSTATIONS

Manual del administrador

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

Fecha de revisión: Octubre, 2004

Contenido

CAPÍTULO 1. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS	6
1.1. Novedades de la versión 5.0	7
1.2. Requisitos hardware y software del sistema	8
1.3. Presentación del producto	9
1.4. Servicio para usuarios registrados.....	10
1.5. Convenciones tipográficas	10
CAPÍTULO 2. INSTALACIÓN Y DESINSTALACIÓN DEL SOFTWARE	12
2.1. Instalación del software	12
2.2. Desinstalación del software	15
CAPÍTULO 3. INTRODUCCIÓN A LA ADMINISTRACIÓN DE APLICACIONES	16
3.1. Introducción a la administración de software	18
3.2. Interfaz local.....	19
3.2.1. Icono de la barra del sistema	19
3.2.2. Menú contextual	19
3.2.3. Ventana principal de la aplicación: estructura general	21
3.2.3.1. <i>Ficha Protección</i>	23
3.2.3.2. <i>Ficha Configuración</i>	24
3.2.3.3. <i>Ficha Soporte</i>	25
3.2.4. Ventana Analizando	27
3.2.5. Sistema de ayuda	28
CAPÍTULO 4. PROTECCIÓN PREDETERMINADA DEL EQUIPO	29
4.1. Configuración predeterminada	29
4.2. Niveles de protección antivirus	31
CAPÍTULO 5. ADMINISTRACIÓN DE LA APLICACIÓN DESDE LA INTERFAZ LOCAL	33
5.1. Actualización de la base antivirus y de los módulos de aplicación	33
5.1.1. Elección de la hora de actualización.....	34
5.1.2. Actualizaciones manuales y proceso de actualización	34
5.1.3. Configuración de las tareas de actualización	35
5.1.3.1. Actualización las bases antivirus.....	36

5.1.3.2. Actualización de módulos del programa	40
5.2. Protección en tiempo real	41
5.2.1. Análisis del sistema de archivos	43
5.2.2. Análisis del correo	48
5.2.3. Análisis del correo en MS Outlook	52
5.2.4. Análisis de secuencias de comandos VBScript y JavaScript	53
5.2.5. Análisis de macros	54
5.3. Análisis a petición	56
5.3.1. Análisis de compilaciones	61
5.3.2. Procesado diferido de objetos	63
5.4. Tareas del usuario	65
5.4.1. Lectura de los resultados de las tareas	65
5.4.2. Crear una nueva tarea	67
5.5. Funciones avanzadas	71
5.5.1. Zonas de cuarentena y respaldo	71
5.5.1.1. Configuración del respaldo	72
5.5.1.2. Trabajar con la cuarentena	74
5.5.1.3. Trabajar con la zona de respaldo	76
5.5.2. Trabajar con informes	77
5.5.3. Configuración adicional	81
CAPÍTULO 6. CONTROL DE LA APLICACIÓN CON KASPERSKY ADMINISTRATION KIT	83
6.1. Control de directivas	83
6.1.1. Creación de una directiva	83
6.1.2. Examen y modificación de la configuración de la directiva	86
6.1.2.1. Información de la aplicación	87
6.1.2.2. Análisis a petición	88
6.1.2.3. Protección constante del sistema de archivos	92
6.1.2.4. Análisis del correo	95
6.1.2.5. Análisis de secuencias de comandos	99
6.1.2.6. Análisis de macros	101
6.1.2.7. Actualización de bases antivirus y módulos de aplicación	105
6.1.2.8. Operaciones con tareas del sistema	106
6.1.2.9. Configuración de las zonas de Cuarentena y Respaldo	106
6.1.2.10. Generación de un informe de actividad de la aplicación	108
6.1.2.11. Parámetros avanzados	111

6.1.2.12. Examen de los resultados del control de directiva	113
6.2. Administración de tareas.....	114
6.2.1. Creación de tarea	114
6.2.1.1. Creación de una tarea local.....	115
6.2.1.2. Creación de una tarea de grupo	119
6.2.1.3. Creación de una tarea global	120
6.2.2. Examen y modificación de la configuración de la tarea y supervisión del rendimiento de tarea	121
6.2.3. Inicio y detención de tareas.....	122
6.3. Configuración de los parámetros de la aplicación	122
6.3.1. Información de la aplicación	124
6.3.2. Configuración adicional de la aplicación.....	124
6.3.3. Trabajar con la zonas de cuarentena y respaldo	125
6.3.4. <i>Mostrar información de llaves de licencia</i>	127
6.3.5. <i>Parámetros de generación de informes</i>	128
CAPÍTULO 7. PRUEBAS DE FUNCIONAMIENTO DE KASPERSKY ANTI- VIRUS	129
7.1. Prueba con el "virus" EICAR y sus modificaciones.....	129
7.2. Pruebas de funcionamiento correcto de Kaspersky Anti-Virus	131
CAPÍTULO 8. CONTROL DE LA LLAVE DE LICENCIA.....	133
8.1. Trabajar con llaves de licencia desde la interfaz local	134
8.2. Trabajar con llaves de licencia desde la interfaz de Kaspersky Administration Kit	135
CAPÍTULO 9. PREGUNTAS FRECUENTES	136
ANEXO A. CONTACTO CON EL SOPORTE TÉCNICO.....	140
ANEXO B. GLOSARIO.....	142
ANEXO C. KASPERSKY LAB	149
C.1. Otros productos Kaspersky Lab.....	150
C.2. Cómo encontramos	154
ANEXO D. ÍNDICE.....	155
ANEXO E. CONTRATO DE LICENCIA.....	156

CAPÍTULO 1. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (al que nos referimos también en esta documentación como Kaspersky Anti-Virus, o la aplicación) 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 otros destinatarios. La aplicación 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 en modo supervisión:* análisis de las secuencias de comandos antes de su ejecución por el intérprete del S.O. y Microsoft Internet Explorer; 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: le recomendamos actualizar la base antivirus cada hora para disponer de un producto actualizado.

- *La diferencia de permisos para administradores de seguridad y usuarios de estaciones de trabajo queda reflejada en dos interfaces:* una interfaz de usuario con un conjunto reducido de funciones necesarias, y una interfaz de administración ampliada con posibilidades de configuración flexible.
- *Control centralizado del sistema de protección antivirus* desde una interfaz de administración adicional proporcionada por Kaspersky Administration Kit.

1.1. Novedades de la versión 5.0

Los cambios siguientes han sido introducidos en **Kaspersky Anti-Virus 5.0 for Windows Workstations** a partir de las versiones 4.x:

- Un nuevo núcleo antivirus y la utilización de las tecnologías iChecker™ e iStreams™ reduce a la mitad el uso de memoria y multiplica por tres el rendimiento de la protección antivirus comparada con la versión 4.0.
- La velocidad de la actualización de la base antivirus ha aumentado gracias a la detección automática de los servidores con menor sobrecarga de Kaspersky Lab; incluye un algoritmo que permite descargar tan sólo las actualizaciones restantes en caso de desconexión; las actualizaciones recibidas ahora pueden ser copiadas hacia un recurso local para ser compartidas.
- Es posible ajustar la configuración antivirus mediante la selección de tres niveles de protección predeterminados, con parámetros específicos

elegidos por Kaspersky Lab: *máxima protección, recomendado y máxima velocidad.*

- Se incluye la capacidad para desinfectar compilaciones ZIP, ARJ, CAB y RAR.
- Ahora es posible analizar el tráfico de correo electrónico que utiliza los protocolos SMTP/POP3, sin tener en cuenta el cliente utilizado, y se incluye además una función para desinfectar las bases de correo de Microsoft Outlook y Microsoft Outlook Express.
- Se crea una zona de respaldo para conservar copias de las versiones originales de objetos sospechosos o infectados, creadas antes de desinfectarlos o eliminarlos.
- Mejoran las operaciones de cuarentena: ahora es posible limitar el tiempo de almacenamiento de objetos sospechosos en cuarentena. Se incluya la posibilidad de enviar estos objetos, desde la interfaz de la cuarentena, a Kaspersky Lab para su análisis.

1.2. Requisitos hardware y software del sistema

El funcionamiento óptimo de la estación de trabajo depende de los requisitos siguientes:

- MS Windows® 98/Me/NT Workstation 4.0 con Service Pack 6 instalado:
 - Intel Pentium®133 MHz o superior para Windows98/NT;
 - Intel Pentium®150 MHz o superior Windows Me;
 - 32 Mb de memoria RAM libre;
 - 50 Mb de espacio disponible en disco;
 - Unidad de CDROM.
- MS Windows® 2000 Professional con Service Pack 2 instalado:
 - Intel Pentium®133 MHz o superior;
 - 64 Mb de memoria RAM libre;
 - 50 Mb de espacio disponible en disco;
 - Unidad de CDROM.

- MS Windows® XP Home Edition y XP Professional:
 - Intel Pentium® 300 MHz o superior;
 - 128 Mb de memoria RAM libre;
 - 50 Mb de espacio disponible en disco;
 - Unidad de CDROM.



Kaspersky Anti-Virus 5.0 for Windows Workstations requiere Microsoft Internet Explorer versión 5.0 o superior.

1.3. 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 Web, podrá descargarlo desde el sitio Web de Kaspersky Lab; su copia también contiene 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.

1.4. 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 con tecnologías no fabricadas por Kaspersky.

1.5. 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
 Nota.	Información o notas adicionales
 ¡Advertencia!	Información que requiere especial atención

Estilo	Descripción
 <p><i>Para completar la acción,</i></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 2. INSTALACIÓN Y DESINSTALACIÓN DEL SOFTWARE

La instalación de Kaspersky Anti-Virus ofrece dos opciones principales: instalación local, e instalación remota, a través de un equipo de administración centralizada con Kaspersky Administration Kit 5.0. Este manual describe la instalación local de Kaspersky Anti-Virus en una estación de trabajo. Para obtener más detalles acerca de la instalación remota del producto, consulte el Manual del administrador de Kaspersky Administration Kit 5.0.

2.1. Instalación del software



Le recomendamos cerrar todas las aplicaciones activas antes de instalar Kaspersky Anti-Virus.

Para instalar la aplicación, ejecute el archivo ejecutable *setup.exe* incluido en el paquete de distribución. La instalación se ejecuta en modo interactivo. Cada cuadro de diálogo contiene botones que permiten controlar el proceso de instalación. Se utilizan cuatro tipos básicos de botones:

- **Aceptar:** acepta las acciones sugeridas;
- **Cancelar:** cancela las acciones sugeridas;
- **Siguiente:** se desplaza a la etapa siguiente;
- **Anterior:** regresa a etapa anterior.

Paso 1. Lectura del contrato de licencia

El cuadro de diálogo **Contrato de licencia** contiene el texto del contrato de licencia. Léalo con atención y haga clic en **Sí**, si está de acuerdo con sus términos. Para cancelar la instalación del software, haga clic en **No**.

Paso 2. Información del usuario

Escriba la información del usuario en el cuadro de diálogo **Información de usuario**. Escriba el nombre del usuario en el campo **Nombre de usuario**, y el

de su organización en el campo **Organización**. La información predeterminada se toma del Registro de Windows.

Paso 3. Selección del directorio de destino

El directorio de destino de la instalación de Kaspersky Anti-Virus se especifica en el cuadro de diálogo **Elija la ubicación del destino**. Puede modificar el directorio de destino con **Examinar...**

Paso 4. Información importante sobre la aplicación

Durante esta etapa del proceso de instalación, se le pregunta si desea leer información importante acerca de la aplicación antes de comenzar a utilizarla.

El cuadro de diálogo le informa acerca de características o funciones importantes de Kaspersky Anti-Virus.

Tras leer esta información, haga clic en **Siguiente**.

Paso 5. Instalación de la llave de licencia

En el cuadro de diálogo **Llave de licencia**, especifique la llave de licencia que Kaspersky Anti-Virus debe utilizar para comprobar la aceptación y validez del contrato de licencia.



La llave de licencia es su "llave" personal, y contiene información operativa requerida para habilitar las funciones completas del software, en concreto:

- Información de soporte técnico (proveedor de soporte e información de contacto).
- título, número y fecha de caducidad.

El aspecto de la ventana **Llave de licencia** puede variar según la forma de especificar la llave; la llave puede haber sido incluida en el paquete de instalación, o puede tener que descargarla de Internet.

En el primer caso, el programa de instalación agrega el archivo de licencia automáticamente, si lo encuentra en el disco de instalación o en el directorio de destino especificado. Durante el proceso de instalación, se mostrará en pantalla información sobre la llave instalada.

En el segundo caso, el programa ofrece las opciones siguientes:



Llave de licencia local: selecciona una llave en disco.

- **Llave de licencia Internet:** recuperar la llave en Internet, desde el sitio Web de Kaspersky Lab.

La primera opción abre una ventana desde la que puede indicar su archivo llave de licencia, con extensión `.key`, a partir del botón **Examinar...**

La selección de la **Llave de licencia Internet** abre un cuadro de diálogo donde puede completar los campos de información y entrar su código de activación (suministrado durante la compra del producto). Después de indicar estos datos, haga clic en **Siguiente** para continuar,

Paso 6. Escritura de la contraseña del administrador



Esta ventana aparece tan sólo durante una instalación de Kaspersky Anti-Virus bajo sistema operativo MS Windows 98/ME.

Utilice esta etapa para especificar la contraseña del administrador que permite cambiar entre las dos interfaces disponibles para usuarios ofimáticos y administradores de seguridad antivirus.

Para indicar la contraseña, escriba su contraseña en el campo **Contraseña** y vuelva a escribirla en el campo **Confirmar contraseña**.

Si deja los campos vacíos y continúa con la instalación, se utilizará una línea vacía como contraseña para cambiar entre las dos interfaces. Más tarde, puede agregar la contraseña o modificarla si ya la ha definido durante el proceso de instalación (ver sección 3.2.2 pág. 19).

Paso 7. Finalización del proceso de instalación

La ventana **Fin del asistente de instalación** muestra información de resumen sobre la instalación de Kaspersky Anti-Virus en su equipo. Cualquiera de las dos opciones siguientes es posible, dependiendo de la versión del sistema operativo utilizado.



Si instala Kaspersky Anti-Virus en un equipo bajo sistema operativo MS Windows 98/ME:

El fin del programa de instalación requiere registrar servicios en el sistema: se le invita por tanto a reiniciar su equipo. Esto es **NECESARIO** para completar correctamente la instalación del producto.

Seleccione cualquiera de las siguientes variantes:

- **Sí, quiero reiniciar mi equipo ahora.**

 **No, reiniciaré mi equipo más tarde.**

Haga clic en **Terminar**.



Si instala Kaspersky Anti-Virus en un equipo con otro sistema operativo:

El fin de la instalación no requiere reiniciar el equipo. Si no desea activar la protección antivirus del equipo inmediatamente después de instalar el producto, desactive la casilla **Iniciar Kaspersky Anti-Virus 5.0 for Windows Workstations**. Haga clic en **Terminar**.



Si desactiva la casilla, la protección antivirus de su equipo sólo se activará automáticamente después de reiniciarlo. Puede activar manualmente la protección antivirus desde el menú principal de Windows (**Inicio → Archivos de programa → Kaspersky Anti-Virus 5.0 for Windows Workstations**).



Nota: después de actualizar MS Windows 98/ME a NT 4.0/2000/XP, es necesario reinstalar Kaspersky Anti-Virus 5.0 for Windows Workstations.

2.2. Desinstalación del software

Si por cualquier razón necesita desinstalar Kaspersky Anti-Virus, ejecute **Inicio → Archivos de programa → Kaspersky Anti-Virus 5.0 for Windows Workstations → Desinstalar Kaspersky Anti-Virus** o utilice el diálogo estándar **Agregar o quitar programas** en el Panel de control.

Deberá confirmar la desinstalación. Haga clic en **Aceptar** para iniciar el proceso de desinstalación. El programa desinstalador abrirá un diálogo para decidir si quiere que elimine o conserve los objetos dentro de la cuarentena y la zona de respaldo, así como los informes y los archivos llave de licencia.

Esto comenzará el proceso de eliminación de archivos del disco duro del equipo.



Si el software detecta archivos utilizados por otros programas durante el proceso de desinstalación, un cuadro de diálogo le preguntará si desea eliminarlos también. Haga clic en el vínculo **Sí** para eliminar el archivo.

Tras completar la desinstalación de la aplicación, el proceso le invitará a reiniciar su estación de trabajo. Seleccione la variante preferida y haga clic en **Terminar**.

CAPÍTULO 3. INTRODUCCIÓN A LA ADMINISTRACIÓN DE APLICACIONES

Kaspersky Anti-Virus se instala en estaciones de trabajo y puede ser administrado en local, o en remoto desde Kaspersky Administration Kit si el equipo está incluido dentro de un sistema de control centralizado.

Numerosas categorías de usuarios pueden trabajar con Kaspersky Anti-Virus:

- *Usuario de estación de trabajo* es el usuario del equipo donde se instala la aplicación.
- *Administrador de seguridad antivirus* (designado como el administrador): asegura el control local de la aplicación.
- *Administrador de red lógica*: controla el funcionamiento del Kaspersky Anti-Virus a través del sistema centralizado de control remoto de Kaspersky Administration Kit.

Cada categoría tiene asignada su propia interfaz que ofrece acceso a todas las funciones del software autorizadas para dicha categoría en función de los permisos correspondientes.

La **interfaz de usuario** está optimizada para ser eficiente y sencilla y permite ejecutar las tareas siguientes:

- examen de estado de información correspondiente a la protección antivirus;
- ejecución de tareas para analizar objetos del sistema de archivos;
- actualización de la base antivirus;
- lectura de los resultados de las tareas ejecutadas y del registro de eventos;
- examen del contenido de las zonas de cuarentena y respaldo y envío de los archivos en cuarentena a Kaspersky Lab para su examen.

La **interfaz del administrador** ampliada permite configurar de forma sencilla y con flexibilidad el funcionamiento de la aplicación y realizar las tareas siguientes:

- modificación de la configuración de las tareas de protección antivirus en tiempo real;

- creación de tareas de análisis de objetos del sistema de archivos tareas de actualización, con su administración y planificación;
- actualización de la base antivirus y de los módulos de aplicación;
- examen de estado de información correspondiente a la protección antivirus;
- lectura de los resultados de las tareas realizadas y del registro de eventos;
- examen del contenido de las zonas de cuarentena y respaldo y envío de los archivos en cuarentena a Kaspersky Lab para su examen.

Cuando el control está centralizado por Kaspersky Administration Kit, la aplicación es administrada en remoto desde un equipo instalado con la *consola de administración*.

La consola de administración es una **interfaz estándar integrada dentro de MMC** que permite al administrador de red ejecutar las funciones siguientes:

- instalación remota de la aplicación en equipos clientes;
- actualización de la base antivirus y de los módulos de aplicación;
- aplicar directivas y administrar tareas en equipos clientes;
- instalar llaves de licencia en equipos clientes;
- ver informes de actividad de la aplicación en equipos clientes.

Para obtener más detalles acerca de la administración centralizada, consulte el Manual del administrador de Kaspersky Administration Kit 5.0.

El permiso de acceso a la interfaz ampliada se otorga a los administradores de seguridad de Kaspersky Anti-Virus incluidos en el grupo **Administradores de Kaspersky Anti-Virus** que inician su sesión en MS Windows con sus nombres y contraseñas. El grupo de **Administradores de Kaspersky Anti-Virus** se crea durante la instalación en una estación de trabajo. Puede agregar o eliminar usuarios del grupo desde la ventana **Administración de equipos**. De forma predeterminada, los administradores locales también son administradores de seguridad antivirus.

Si el software es instalado de forma remota con Kaspersky Administration Kit, dicho grupo se constituye automáticamente a partir de los usuarios incluidos en el grupo de administradores de la red lógica, con el nombre "KL Admins".

Las personas no incluidas en el grupo de administradores de seguridad antivirus son usuarios normales que cuando inician su sesión en Windows, sólo tienen acceso a la interfaz de usuario.



Los usuarios MS Windows 98/ME pueden cambiar de la interfaz de usuario a la interfaz de administración ampliada desde el menú contextual (clic derecho) del icono de Kaspersky Anti-Virus en la barra del sistema (ver detalles en la sección 3.2.2 pág. 19).

3.1. Introducción a la administración de software

Cuando se administra en local, el administrador configura la protección de Kaspersky Anti-Virus a partir de cambios en la configuración de la aplicación y en las tareas.

Una **tarea** es una acción específica ejecutada por la aplicación. Las tareas se dividen de acuerdo con su finalidad (tarea de análisis completo del sistema, tarea de actualización de bases de datos antivirus y de módulo de software, etc.). Cada tarea cuenta con un conjunto de parámetros que controlan su ejecución, y que define la *configuración de la tarea*.



Parámetros de la aplicación- conjunto de parámetros que determinan el funcionamiento de la aplicación, así como opciones propias de los servicios de cuarentena, respaldo o generación de informes, etc.

Cuando prepara la administración centralizada desde Kaspersky Administration Kit, el administrador también define la configuración de la aplicación y de las tareas, pero en este caso, se aplica a una instancia de Kaspersky Anti-Virus instalada en un equipo remoto de la red.

Una característica notable de la administración centralizada es la posibilidad de organizar los equipos en grupos, y de modificar su configuración mediante la creación y definición de directivas de grupo.

Una **directiva** es un conjunto de parámetros que determina el funcionamiento de la aplicación dentro de un grupo de la red lógica, así como el conjunto de restricciones aplicables a la redefinición de estos parámetros para configurar una directiva, aplicación o tarea subordinada. Una directiva incluye todos los parámetros necesarios para ejecutar cada una de las funciones implementadas en la aplicación, tanto en la aplicación como en todos los tipos de tareas, con la excepción de aquellos que no son reutilizables, es decir, que son definidos cada vez que se inicia la tarea.





Para desactivar la modificación de la directiva, defina un "bloqueo" en los parámetros: . Los parámetros que pueden modificarse están señalados por .




3.2. Interfaz local

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

3.2.1. Icono de la barra del sistema

Después de iniciar la aplicación, el icono del antivirus aparece en la barra del sistema; su apariencia 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) .

La  parpadea 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, un cuadro con un mensaje informativo y la recomendación de los expertos de Kaspersky Lab aparece durante un momento por encima del icono (esta característica no está disponible en Windows98/NT).

3.2.2. 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 en busca de virus, de acuerdo con el nivel de protección definido.
- **Actualizar las bases antivirus**: ejecuta la descarga de actualizaciones de la base antivirus.

- **Tareas en ejecución:** lista de las tareas planificadas en ejecución. Esta opción aparece en el menú contextual cuando el programa antivirus inicia cualquier tarea planificada (ver la sección 5.4 pág. 65).
- **Activar la protección en tiempo real / Desactivar la protección en tiempo real :** activa o desactiva la protección en tiempo real de su equipo. El icono cambia en función del estado de la protección en tiempo real. Si desactiva la protección en tiempo real en el menú contextual, se restablecerá en el siguiente reinicio de Windows.

Este elemento de menú sólo está disponible para administradores de Kaspersky Anti-Virus. Los usuarios normales no pueden activar o desactivar la protección en tiempo real de un equipo.

- **Acerca de la aplicación:** abre una ventana de ayuda con información acerca de Kaspersky Anti-Virus.
- **Cambiar a modo usuario/ Cambiar a modo administrador** (sólo para Windows 98): permite cambiar entre una interfaz para usuario de ofimática y otra ampliada para el administrador, respectivamente. La opción **Cambiar a modo administrador** abre un cuadro de diálogo solicitando la contraseña del administrador de seguridad antivirus.

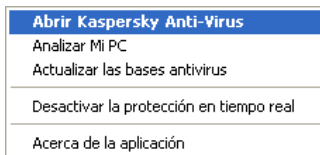


Figura 1. Menú contextual

Si utiliza MS Windows 98/ME, el menú contextual incorpora otra opción adicional: **Cambiar a modo usuario / Cambiar a modo administrador**.

Si hace clic en esta opción, puede cambiar entre la interfaz disponible para usuarios y la interfaz de administrador mejorada. Si selecciona **Cambiar a modo administrador**, se abre un cuadro de diálogo (ver Figura 2) donde indicar la contraseña del administrador de seguridad antivirus (esta contraseña se establece durante la instalación del producto (ver Paso 6. pág. 14).

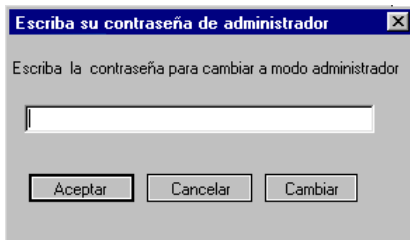


Figura 2. Escritura su contraseña de administrador

Si por cualquier razón no estableció la contraseña del administrador durante instalación de Kaspersky Anti-Virus, o si desea ahora modificarla, haga clic en **Cambiar...** en el cuadro de diálogo. Rellene los campos necesarios en la siguiente ventana (ver Figura 3).

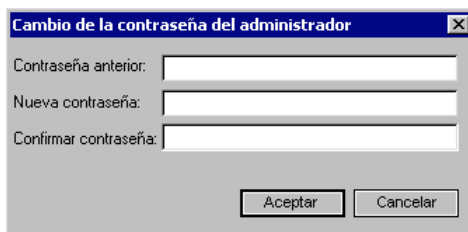


Figura 3. Cambio de la contraseña del administrador

3.2.3. Ventana principal de la aplicación: estructura general

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

- ajustar los parámetros de protección antivirus;
- crear y administrar tareas de protección antivirus;
- descarga de actualizaciones de la base antivirus y de los módulos de aplicación;
- 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.
- **Configuración:** estado y tareas que configuran lo principal de la protección antivirus.
- **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, mientras la ficha **Configuración** incluye los parámetros de estas tareas.
- **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). Así, la ficha **Protección** indica el estado de la protección antivirus, mientras la ficha **Configuración** da acceso a su configuración.

Existen tres variantes en el estado de protección antivirus, indicadas 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 si un error aparece 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 o varias tareas 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.

3.2.3.1. Ficha Protección

La ficha **Protección** (ver Figura 4) 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 y ver informes acerca de las tareas iniciadas. 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.
- [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 en los niveles crítico y medio de protección antivirus. Para aumentar el nivel de protección antivirus, la aplicación puede invitarle, por ejemplo, a modificar su configuración actual, a regresar a la configuración recomendada por los expertos, o a ejecutar una tarea. Todas las recomendaciones se presentan como vínculos en los que puede hacer clic para ejecutar las acciones correspondientes.



Figura 4. Ficha Protección

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 (ver sección 5.3.2 pág. 63).

3.2.3.2. Ficha Configuración

La ficha **Configuración** (ver Figura 5) le ayuda a evaluar la configuración de la aplicación sin revisar realmente cada parámetro; puede crear y administrar tareas personalizadas; definir y modificar los principales parámetros de funcionamiento de la aplicación, o definir su propia configuración personalizada.



La configuración adicional permite ampliar las funciones del producto funcionamiento respecto de las características predeterminadas.

El panel derecho de la ficha muestra la configuración actual de la protección en tiempo real, del análisis completo del equipo, de la actualización automática de

la base antivirus, con comentarios detallados y consejos para modificar la configuración. Por ejemplo, si la base antivirus ha sido actualizada manualmente, la aplicación le invita a automatizar el proceso de actualización mediante la planificación de esta tarea.

Los vínculos del panel izquierdo de la ficha permiten definir y modificar la configuración de la protección en tiempo real de su equipo, de los análisis completos y de las actualizaciones de la base antivirus.

También puede configurar la cuarentena y la zona de respaldo, así como la configuración adicional de Kaspersky Anti-Virus. La ficha también le permite crear tareas de usuario, planificar su ejecución y administrarlas.



Figura 5. Configuración

3.2.3.3. Ficha Soporte

Desde la ficha **Soporte** (ver Figura 6), 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 requieren una ayuda experta. La información relativa a la aplicación, su llave de licencia y el sistema operativo de su equipo se muestra en la parte derecha de la 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 uno o varios objetos sospechosos por correo electrónico a Kaspersky Lab para su análisis.
- [Llaves de licencia](#): cobertura de la licencia para utilizar Kaspersky Anti-Virus o para agregar un llave de reserva.

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 producto.
- [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 6. Ficha Soporte

3.2.4. Ventana Analizando

Cuando se inicia un análisis del equipo o de objetos individuales (discos, archivos o carpetas), dicho proceso aparece en pantalla (ver Figura 7).

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 **Ver 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 último análisis o sobre el actual.

El vínculo [Ver cuarentena](#) abre la ventana Cuarentena (ver sección 5.5.1.2 pág. 74). 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 5.3.2 pág. 63).



Figura 7. Ventana Analizando

3.2.5. 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. [Cómo...](#) contiene una descripción detallada de las tareas clave para la protección antivirus realizadas por Kaspersky Anti-Virus así como una lista de preguntas más 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 4. PROTECCIÓN PREDETERMINADA DEL EQUIPO

La aplicación asegura la protección antivirus inmediatamente después de la instalación, con la configuración predeterminada. Esta configuración es la recomendada por los expertos de Kaspersky Lab para garantizar una protección óptima de su equipo.

Puede además modificar fácilmente la configuración; para ello, seleccione uno de los tres niveles predeterminados de protección definidos por los expertos de Kaspersky Lab: *máxima protección, recomendado y máxima velocidad*.

4.1. Configuración predeterminada

La configuración predeterminada a continuación corresponde a cada tarea de protección:

PROTECCIÓN EN TIEMPO REAL EN MODO SUPERVISIÓN

Se define de forma predeterminada este *nivel recomendado* de protección con los parámetros siguientes, para la protección en tiempo real:

- las tecnologías iChecker™ e iStreams™ están habilitadas;
- La aplicación analiza archivos abiertos para su lectura, escritura o ejecución, especialmente:
 - archivos en discos duros, unidades extraíbles, sectores de arranque;
 - archivos en unidades de red
 - archivos comprimidos, objetos OLE y flujos NTFS alternativos;
- las tecnologías iChecker™ e iStreams™ están habilitadas;
- en presencia de un objeto infectado, la aplicación intenta desinfectarlo y lo elimina si esto falla; si detecta un objeto sospechoso, lo mueve a cuarentena;

- La aplicación analiza los mensajes de correo:
 - Se habilita el análisis de mensajes entrantes mediante protocolo POP3, y de archivos presentes dentro de compilaciones de datos;
 - Se deshabilita el análisis del correo enviado con el protocolo SMTP.
- La aplicación analiza las macros escritas en VBA empleadas en la suite Microsoft Office; en presencia de una secuencia de comandos sospechosa, Anti-Virus bloqueará su ejecución;
- La aplicación analiza las secuencias de comandos VBScript y JavaScript dinámicas procesadas por Microsoft Internet Explorer o el intérprete de secuencias comandos del sistema Windows. Si detecta una secuencia sospechosa, el antivirus bloqueará su ejecución.

ANÁLISIS ANTIVIRUS A PETICIÓN

El *nivel recomendado* predeterminado de protección para el análisis del sistema completo es el siguiente:

- Un análisis completo está planificado a las 20:00 cada viernes;
- las tecnologías iChecker™ e iStreams™ están habilitadas;
- La aplicación analiza los archivos siguientes:
 - archivos en discos duros y sectores de arranque;
 - los archivos en RAM, los objetos ejecutados automáticamente con a carga del sistema operativo (objetos de arranque), y los flujos NTFS alternativos;
 - archivos comprimidos, compilaciones de datos, autoextraíbles y objetos OLE.
- Los objetos siguientes no son analizados: objetos en discos de red; bases de correo y archivos de correo en formato texto;
- Si detecta un objeto infectado o sospechoso, el programa espera a finalizar el análisis para procesarlo.

ACTUALIZACIÓN DE BASES ANTIVIRUS Y DE MÓDULOS DE APLICACIÓN

La configuración predeterminada para actualizar la base antivirus y la aplicación son:

- la ejecución del proceso de actualización está planificada cada tres horas, a partir de la instalación de Kaspersky Anti-Virus;
- se habilita la actualización de las bases antivirus y de las actualizaciones urgentes.

AISLAMIENTO DE OBJETOS SOSPECHOSOS

La configuración predeterminada de la cuarentena es:

- los objetos en cuarentena son analizados de nuevo después de cada actualización de la base antivirus;
- el tamaño de la cuarentena es ilimitado;
- los objetos en cuarentena son conservados de forma indefinida.

CONSERVACIÓN DE UNA COPIA del OBJETO INFECTADO

Antes de intentar desinfectar o eliminar un objeto, se realiza una copia de respaldo. La configuración predeterminada es:

- el tamaño de la zona de respaldo es ilimitado;
- los objetos en la zona de respaldo con conservados sin límite de tiempo.

4.2. Niveles de protección antivirus

Para permitir una modificación sencilla de la configuración de la protección antivirus, la aplicación propone tres niveles de configuración predeterminados (ver Tabla 1).

- **Máxima protección:** nivel de seguridad del equipo que corresponde a la máxima protección antivirus posible, a cambio de una relativa disminución de rendimiento.
- **Recomendado:** nivel de protección antivirus que utiliza la configuración recomendada por Kaspersky Lab, y asegura una protección óptima de su equipo.
- **Máxima velocidad:** nivel de seguridad del equipo, que optimiza el rendimientos del sistema, a cambio de una menor protección relativa.

Si modifica los parámetros de cualquiera de estos niveles, el valor cambia **Configuración personalizada**. Es por tanto el cuarto nivel de protección, que utiliza una configuración personalizada por el usuario.

La tabla siguiente presenta los parámetros de las tareas de protección en tiempo real (**protección**) y de análisis a petición (**análisis**) correspondientes a los niveles de seguridad predeterminados.

Convenciones:

- + activado;
- desactivado;
- x no incluido con esta tarea.

Listas 1. Protección Niveles Parámetros

Parámetro	Máxima protección		Recomendado		Máxima velocidad	
	protección	analizar	protección	analizar	protección	analizar
utilizar IChecker	+	+	+	+	+	+
utilizar IStreams	+	+	+	+	+	+
nivel de análisis	archivos del formato indicado	todos los archivos	archivos del formato indicado	todos los archivos	archivo con extensión especificada	archivos del formato indicado
tamaño del objeto analizado, no más de (Mb)	x	–	x	–	x	8
tiempo de análisis, no más de (sec.)	60	–	60	–	60	60
discos duros	+	x	+	x	+	x
unidades extraíbles	+	x	+	x	+	x
unidades de red	+	x	+	x	–	x
Flujos NTFS	+	+	+	+	+	+
sectores de arranque del disco	+	+	+	+	+	+
archivos comprimidos	+	+	+	+	+	+
compilaciones de datos	x	+	x	+	x	–
archivos autoextraíbles	+	+	–	+	–	+
bases de correo	x	+	x	–	x	–
archivos de correo en formato texto	x	+	x	–	x	–
objetos OLE	+	+	+	+	–	+

CAPÍTULO 5. ADMINISTRACIÓN DE LA APLICACIÓN DESDE LA INTERFAZ LOCAL

Este capítulo contiene información detallada acerca del funcionamiento y configuración de las principales tareas de Kaspersky Anti-Virus, así como de las funciones avanzadas de control del programa desde la interfaz local.

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

Kaspersky Anti-Virus permite realizar actualizaciones automáticas tanto de la base antivirus, con descripciones de virus y métodos de desinfección, como de los módulos de aplicación, a partir de los servidores de actualizaciones de Kaspersky Lab.



Las actualizaciones de la base antivirus son una exigencia básica para la protección antivirus de su equipo. Muchos virus nuevos aparecen cada día y los expertos de Kaspersky Lab introducen a diario información sobre ellos en la base antivirus. Le recomendamos actualizar la base antivirus todas las horas.

La herramienta de actualizaciones descarga la base antivirus actualizaciones y los componentes de aplicación desde los servidores de actualizaciones de Kaspersky Lab, en una carpeta local, o en una carpeta de actualizaciones en el servidor de administración donde se ejecuta Kaspersky Administration Kit dentro de la red.

Puede ejecutar la herramienta de actualizaciones manualmente, o planificar su ejecución. Para descargar versiones actualizadas de la base de datos antivirus a tiempo, le recomendamos configurar un calendario de ejecuciones automáticas de la herramienta.

5.1.1. Elección de la hora de actualización

La aplicación le informará de cuándo es necesario actualizar la base de datos. También puede tomar personalmente la decisión de actualizar tras examinar los indicadores en el panel derecho de la ficha **Protección** (ver Figura 4).

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. Actualizaciones manuales y 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](#) en la descripción de 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 de la aplicación en la barra del sistema.

Haga clic en un vínculo para abrir una ventana (ver Figura 8) 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. La aplicación recibe una lista con información sobre el tamaño de las actualizaciones de los servidores 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 8) puede ver el tamaño total de las actualizaciones necesarias para las bases antivirus. 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 queda reflejado por el indicador y 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 antivirus son instaladas automáticamente.

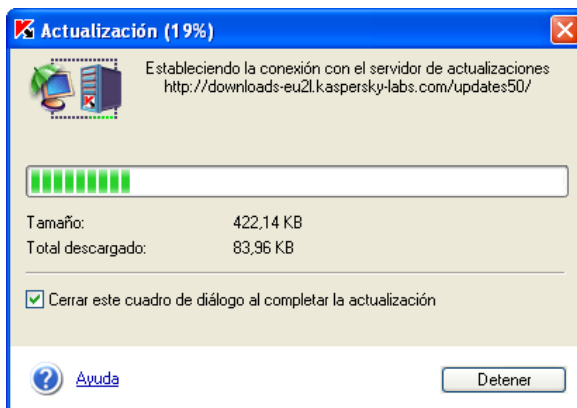


Figura 8. Actualización de la base antivirus y de los componentes de aplicación

5.1.3. Configuración de las tareas de actualización

Durante la instalación de Kaspersky Anti-Virus, se crean dos tareas sistema de actualización: actualización de la base antivirus y actualización de los módulos de aplicación.

Además, con Kaspersky Administration Kit, puede crear tareas de actualización para actualizaciones simultáneas de las bases de datos antivirus y de los módulos de aplicación.

Puede modificar los parámetros de estas tareas y planificar su inicio automático.



Los expertos de Kaspersky Lab le recomiendan planificar la actualización de los paquetes antivirus con intervalos de una hora.

5.1.3.1. Actualización las bases antivirus



Para configurar la tarea de actualización de las bases antivirus:

haga clic en el vínculo [Actualizaciones](#) en el panel izquierdo de la ficha **Configuración**.

o:

en el vínculo [Tareas del usuario](#) en el panel izquierdo de la ficha **Configuración**. En este caso, se abre una ventana que muestra la lista de tareas del usuario: elija la tarea *Actualizar las bases antivirus*, y haga clic en **Propiedades**.

Se abre una ventana con la configuración de las tareas de actualización, con dos fichas: la ficha **Configuración** (ver Figura 9) y la ficha **Planificación** (ver sección 5.4 pág. 65):

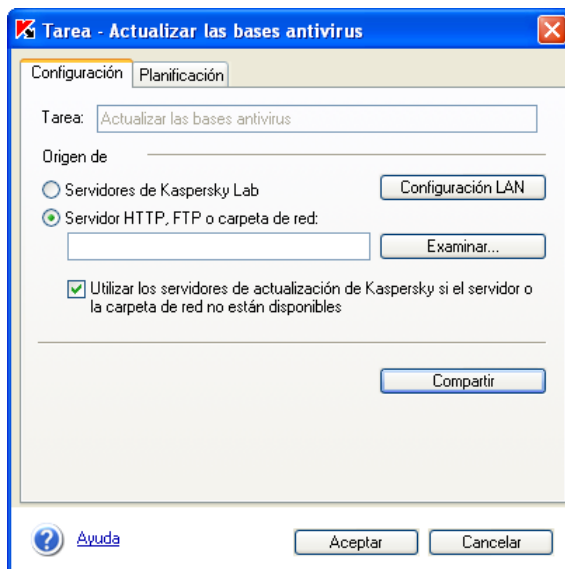


Figura 9. Configuración de la tarea de actualización de las bases antivirus

En la sección **Origen de** (ver Figura 9) elija el origen de las actualizaciones planificadas. Puede ser uno de los siguientes:

- **Servidores de Kaspersky Lab:** recuperar las actualizaciones desde los servidores de actualización HTTP o FTP de Kaspersky Lab.
- **Servidor HTTP, FTP o carpeta de red** las actualizaciones se realizarán a partir de una carpeta de red, o de servidores HTTP- o FTP-. Escriba la dirección del servidor HTTP- o FTP- o la ruta de acceso a la carpeta de red con el botón **Examinar**.
- **Utilizar los servidores de actualización de Kaspersky si el servidor o la carpeta de red no están disponibles:** active esta casilla para recuperar actualizaciones desde los servidores Internet de actualización de Kaspersky Lab si falla la actualización desde la carpeta especificada
- Configurar las conexiones de red en la ventana que aparece cuando hace clic en **Configuración LAN** (ver Figura 10).

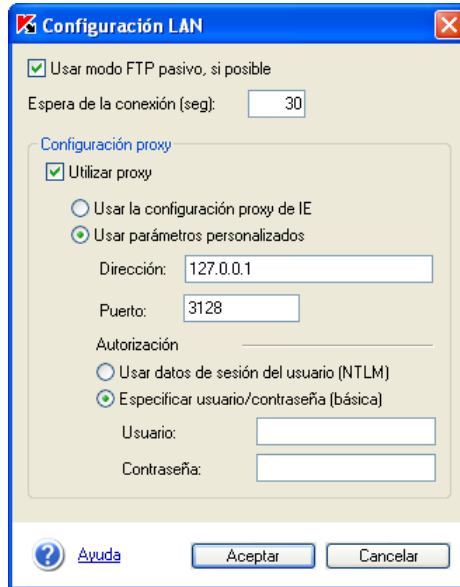


Figura 10. Configuración de red

- Usar modo FTP pasivo, si posible.** Le recomendamos activar esta casilla si su servidor tiene instalado un cortafuegos y no puede conectar con un sitio FTP en modo activo.

Espera de la conexión (seg.) límite de tiempo para establecer la conexión con un servidor de actualización Kaspersky Lab.
- Utilizar proxy.** Active esta casilla si se conecta a Internet a través de un servidor proxy y elija la configuración de su conexión:
 - Usar la configuración proxy de IE** fuerza el uso de la configuración de Internet Explorer para trabajar con un servidor proxy.
 - Usar parámetros personalizados.** Si decide utilizar parámetros personalizados, indique los datos necesarios en los campos **Dirección** y **Puerto**.

En la sección **Autorización** seleccione el tipo de autorización utilizada: **NTLM** o **Basic**. Si selecciona la autorización Basic, complete los campos **Nombre de usuario** y **Contraseña**.



Tan sólo está disponible la autenticación Basic si Kaspersky Anti-Virus se ejecuta bajo sistema operativo Windows 98/ME.

Haga clic en **Compartir** (ver Figura 9) para definir el funcionamiento del servicio de actualizaciones compartidas (ver Figura 11). El servicio permite guardar en una carpeta local las actualizaciones de las bases antivirus y de los módulos de aplicación descargadas de los servidores de Kaspersky Lab, donde son recuperadas más tarde por otros equipos de la red local, con la consiguiente reducción de tráfico Internet.

Active la casilla **Copiar a carpeta compartida** para utilizar el servicio de actualizaciones compartidas, y especifique la ruta a la carpeta.

Especifique a continuación los tipos de actualizaciones que vayan a incluirse en la carpeta local, que será compartida:

- Copiar actualizaciones de bases antivirus a carpeta compartida** significa que las actualizaciones de bases antivirus recibidas son guardadas en la carpeta compartida que contiene las actualizaciones.
- Copiar actualizaciones de módulos de aplicación a carpeta compartida**; las actualizaciones de componentes de la aplicación recibidas se guardarán en la carpeta de actualizaciones compartidas:

 - Actualizaciones disponibles** se compartirán todas las actualizaciones de la aplicación.
 - Actualizaciones urgentes**: tan sólo se comparten las actualizaciones urgentes (importantes) de los módulos de aplicación.

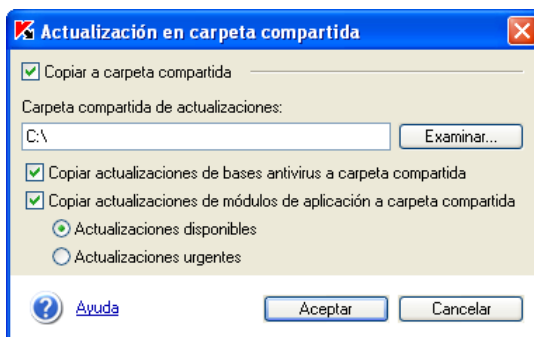


Figura 11. Configuración del servicio de actualizaciones compartidas

5.1.3.2. Actualización de módulos del programa



Para configurar la tarea de actualización de los módulos de aplicación,

haga clic en el vínculo [Tareas del usuario](#) en el panel izquierdo de la ficha **Configuración**. A continuación, se abre una ventana con la lista de tareas del usuario: elija la tarea *Actualizar las bases antivirus*, y haga clic en **Propiedades**.

Se abre una ventana con la configuración de las tareas de actualización de los módulos de aplicación, con dos fichas: la ficha **Configuración** (ver Figura 12) y la ficha **Planificación** (ver sección 5.4 pág. 65).

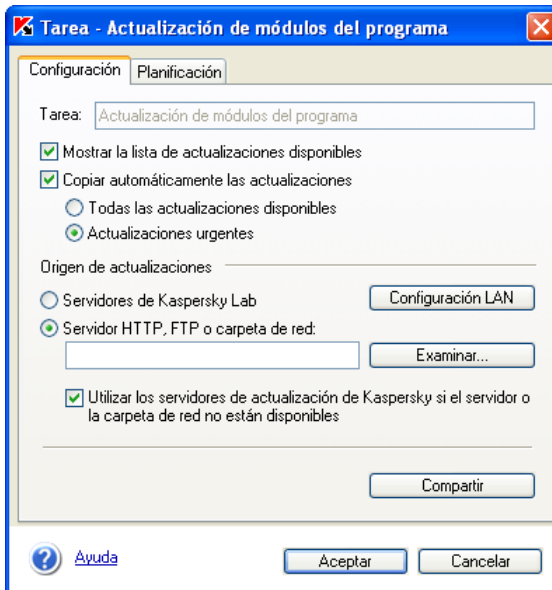


Figura 12. Configuración de tarea para la actualización de los módulos de aplicación

En la ventana de configuración de las tareas de actualización de los módulos de aplicación, seleccione el origen de las actualizaciones (**servidor HTTP, FTP o carpeta de red** o **Servidores de Kaspersky Lab**) y especifique los parámetros del servicio de actualizaciones compartidas. Estos parámetros son los mismos que para la tarea de actualización de las bases antivirus (ver sección 5.1.3.1 pág. 36).

Además, puede seleccionar el método de descarga e instalación de las actualizaciones de los módulos de aplicación:

- Mostrar la lista de actualizaciones disponibles:** active la casilla para recibir un archivo en formato XML con la lista de actualizaciones disponibles. Tan pronto como es descargado, la ventana **Actualización de módulos del programa** le proporciona con información acerca de las actualizaciones del programa y le permite instalarlas. El cuadro de diálogo contiene información acerca de la versión actual de la aplicación. Utilice la lista desplegable inferior para indicar a qué versión desea actualizar la aplicación. También puede ver el tamaño de la actualización planificada, además de la descripción de sus funciones.

A continuación, puede aparecer información acerca de la necesidad de reiniciar el equipo, dependiendo del tipo de actualizaciones.

Para actualizar los módulos de aplicación, haga clic en **Aceptar**. En otro caso, haga clic en **Cancelar** para terminar el proceso de actualización.

- Copiar automáticamente las actualizaciones:** active esta casilla para habilitar la descarga e instalación automáticas de los módulos de aplicación:
 - Todas las actualizaciones disponibles;** se instalarán automáticamente todas las actualizaciones de la aplicación.
 - Actualizaciones urgentes:** tan sólo se instalan automáticamente las actualizaciones urgentes (importantes) de módulos de aplicación.

5.2. Protección en tiempo real


En el modo de *protección en tiempo real*, el antivirus reside en memoria, y supervisa los componentes siguientes: todas las llamadas a objetos del sistema de archivos, mensajes de correo entrantes y salientes, acciones de secuencias de comandos VBScript y JavaScript potencialmente peligrosas, y comandos de macro empleadas 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.

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.





Puede activar y desactivar la protección en tiempo real manualmente. Para ello:

elija **Activar/Desactivar la protección en tiempo real** en el menú contextual  en la barra del sistema.

o:

si la protección en tiempo real está desactivada, haga clic en [activar la protección en tiempo real](#) en el panel derecho de la ficha **Protección**.

El icono de actividad  (rojo) cambia al icono de inactividad  (gris) confirma que la protección en tiempo real está desactivada.



Desactivar la protección en tiempo real aumenta considerablemente los riesgos de infección de virus en su equipo. Sin embargo, puede desactivar la protección en tiempo real para realizar determinadas operaciones (por ejemplo, durante la desfragmentación de discos con sistema de archivos FAT32) para ahorrar tiempo.



Para examinar o modificar la configuración de la protección en tiempo real:

1. Haga clic en el vínculo [Protección en tiempo real](#) en el panel izquierdo de la ficha **Configuración** (ver Figura 5).
2. Puede modificar el nivel definido de protección antivirus o ajustar sus parámetros en la ventana **Configurar la protección en tiempo real**, que se abre a continuación (ver Figura 13).

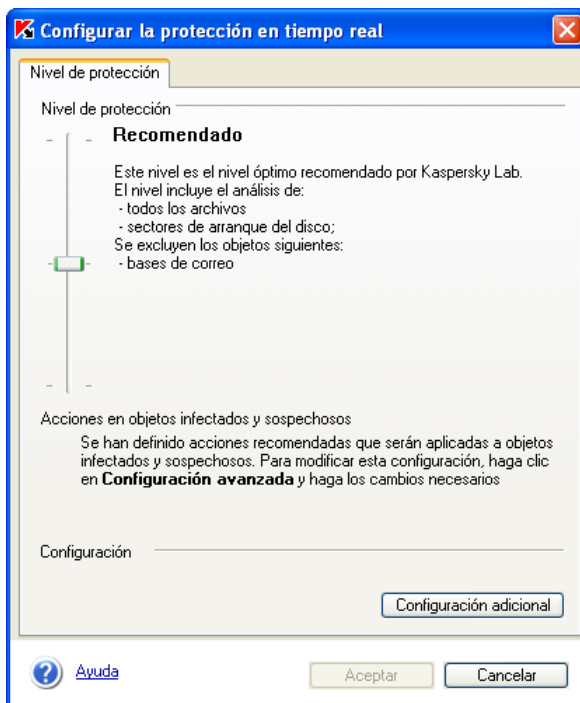


Figura 13. Selección del nivel de protección en tiempo real

Con el cursor del **Nivel de protección**, puede establecer uno de los tres niveles de protección antivirus (vea 4.2 página 31).

Haga clic en **Configuración adicional** para abrir una ventana donde revisar la configuración correspondiente al nivel seleccionado y definir parámetros personales. El nivel de protección cambiará entonces a **Personalizado**.

Elija las fichas correspondientes en la ventana **Configurar la protección en tiempo real** para ajustar la configuración de protección para el sistema de archivos, el correo electrónico y las aplicaciones ofimáticas así como la protección contra secuencias de comandos peligrosas. Encontrará más detalles acerca de la configuración de estos parámetros en las secciones siguientes.

5.2.1. Análisis del sistema de archivos

En el modo de protección en tiempo real, la aplicación analiza las llamadas al sistema de archivos del equipo, en busca de código dañino.

La configuración de la protección en tiempo real del sistema de archivos se realiza en la ventana **Configurar la protección en tiempo real** desde la ficha **Archivos** (ver Figura 14).

Esta ventana permite activar o desactivar la protección en tiempo real del sistema de archivos, definir el análisis objetos y de acciones ejecutadas sobre objetos infectados o sospechosos, y seleccionar los tipos de archivos excluidos de los análisis.

- Activar la protección en tiempo real del sistema de archivos:** la protección está activada de forma predeterminada. Desactive esta casilla para desactivar la protección en tiempo real de los objetos del sistema de archivos.

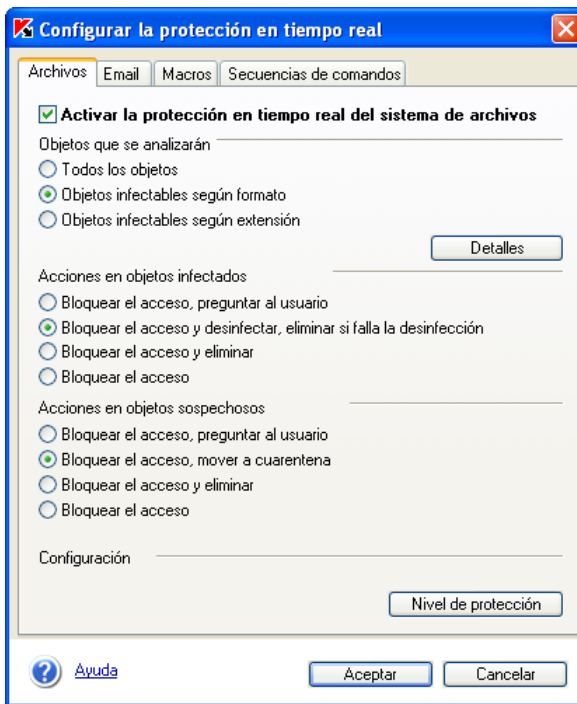


Figura 14. Parámetros de la tarea de protección de objetos del sistema de archivos

Seleccione los objetos en la sección **Objetos que se analizarán:**

- *Todos los objetos:* todos los objetos del sistema de archivos serán analizados.

- *Objetos infectables según formato*: se analizan los objetos potencialmente infectados, el proceso de análisis toma en cuenta la estructura interna de los archivos.
- *Objetos infectables según extensión*: se analizan los objetos potencialmente infectados y la aplicación utiliza las extensiones de archivos para determinar si un archivo debe ser analizado.

En las secciones consagradas a **Acciones en objetos infectados/sospechosos**, elija el tipo de acción aplicada en estos casos:

- *Bloquear el acceso, preguntar al usuario*: bloquea el acceso a un objeto infectado o sospechoso desde aplicaciones externas; la aplicación mostrará varias opciones entre las que el usuario podrá elegir.
- *Bloquear el acceso y desinfectar, eliminar si falla la desinfección*: la aplicación intenta desinfectar el objeto y si no lo consigue, lo elimina.
- *Bloquear el acceso, mover a cuarentena*: mueve un objeto sospechoso a la cuarentena, para poder analizarlo posteriormente con una base antivirus actualizada, restaurarlo, enviarlo a Kaspersky Lab par su examen, o eliminarlo.
- *Bloquear el acceso y eliminar*: - elimina un objeto. Si selecciona esta acción, la aplicación creará una copia del objeto en la zona de respaldo. La copia le permite reparar el archivo o enviarlo para su examen por Kaspersky Lab.
- *Bloquear el acceso*: bloquea el acceso a un objeto infectado o sospechoso desde aplicaciones externas.

Utilice el botón **Detalles** (ver Figura 15) para abrir una ventana donde definir los archivos y los tipos de archivos que deben ser ignorados durante el análisis del sistema de archivos; para activar o desactivar las tecnologías iChecker™ e iStreams™, y para establecer un límite al tiempo de análisis:

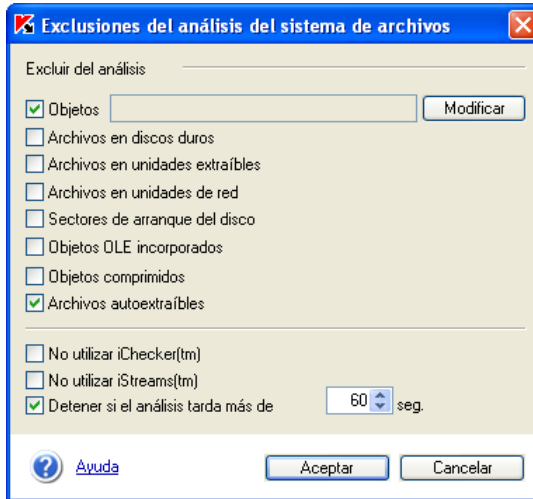


Figura 15. Exclusiones del análisis del sistema de archivos

En la sección **Excluir del análisis**, active las casillas correspondientes a los objetos que no deben ser analizados en el modo de protección en tiempo real; para ignorar el análisis de algunos objetos con una máscara, defina esta máscara en la zona asociada.

Para abrir la ventana donde definir las excepciones, active la casilla **Objetos** y haga clic en **Modificar**. En la ventana abierta (ver fig. 16), modifique la lista de exclusiones con **Agregar**, **Modificar** y **Quitar**.

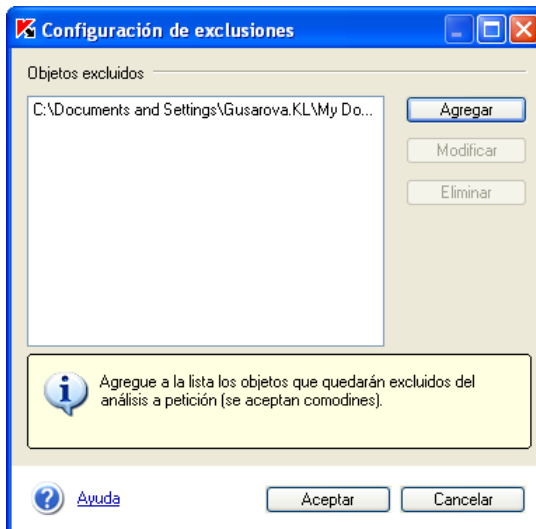


Figura 16. Creación de la lista de excepciones

Haga clic en **Agregar** para abrir un cuadro de diálogo estándar de selección de archivos, y especifique un directorio, carpeta o archivo excluido de la cobertura. Puede introducir objetos en el campo Nombre de archivo mediante máscaras.

Cuando utiliza máscaras para agregar objetos, puede utilizar varias máscaras separadas por un espacio. Si el nombre del archivo contiene espacios, debe escribirlo entre comillas.

- Máscaras sin ruta:
 - ***.exe**: todos los archivos con máscara *.exe;
 - ***.ex?** – todos los archivos con máscara *.ex? ;
 - **test**: todos los archivos con nombre test.
- Máscaras con rutas absolutas:
 - **C:\dir*.***: todos los archivos en el directorio C:\dir\;
 - **C:\dir*.exe**: todos los archivos con máscara *.exe en el directorio C:\dir\directorio;
 - **C:\dir*.ex?** – todos los archivos que coinciden con la máscara *.ex? en el directorio C:\dir\;
 - **C:\dir\test**: el archivo C:\dir\test sólo;

- **C:\dir**: todos los archivos en el directorio *C:\dir* y subdirectorios.
- Máscaras con rutas relativas:
 - **dir*.***: todos los archivos en todos los directorios de *dir*;
 - **dir\test**: todos los archivos con nombre *test* en todos los directorios *dir*;
 - **dir*.exe**: todos los archivos con máscara **.exe* en todos los directorios *dir*;
 - **dir*.ex?** – todos los archivos con máscara **.ex?* en todos los directorios *dir*;
 - **dir**: todos los archivos de todos los directorios *dir* y todos sus subdirectorios.



La escritura de máscaras sin ruta de acceso o que consisten tan sólo en símbolos "?" y "*" no está permitida.



Para asegurarse de que los objetos seleccionados con máscaras son procesados correctamente, el nombre de los archivos excluidos de la cobertura del análisis deben cumplir la regla siguiente: no más de 8 símbolos en el nombre de archivo y no más de tres símbolos en su extensión.



No utilizar iChecker™, No utilizar iStreams™: active estas casillas si no desea utilizar estas tecnologías para el análisis antivirus.



Detener si el análisis tarda más de... sec.: fija la duración máxima del análisis del archivo (en segundos).

5.2.2. Análisis del correo

En el modo de protección en tiempo real, la aplicación analiza los mensajes entrantes y salientes, controla la entrada de código dañino en los buzones, así como el envío de objetos sospechosos o infectados hacia interlocutores de su libreta de direcciones.

Kaspersky Anti-Virus ofrece las características siguientes:

- interceptación de los mensajes entrantes y salientes mediante los protocolos SMTP y POP3 para cualquier cliente de correo;
- interceptación de los mensajes entrantes y salientes en MS Outlook sin consideración de los protocolos utilizados;
- detección de objetos sospechosos o infectados tanto en el cuerpo del mensaje como en los objetos adjuntos con cualquier nivel de imbricación.

El análisis predeterminado se realiza de acuerdo con la configuración predeterminada, donde la aplicación comprueba los elementos siguientes:

- correo entrante mediante protocolo POP3;
- archivos y compilaciones de datos adjuntos en mensajes de correo.



Observe que el correo enviado con el protocolo SMTP NO es analizado de forma predeterminada.

Puede modificar el estado de análisis del correo desde la ventana **Configurar la protección en tiempo real** bajo la ficha **Email** (ver Figura 16).



Activar la protección en tiempo real del correo: la protección está activada de forma predeterminada. Desactive esta casilla para deshabilitar el análisis en tiempo real del correo.

Utilice las secciones **Analizar el correo entrante** y **Analizar el correo saliente** para activar/desactivar el análisis de los mensajes entrantes y salientes transmitidos con cualquier protocolo reconocido en MS Outlook, así como con los protocolos SMTP y POP3 en cualquier otro cliente de correo.



El paquete contiene un módulo especial integrado con MS Outlook para controlar los mensajes de correo. Cuando se instala el programa antivirus, una ficha adicional aparece en la ventana de configuración de MS Outlook (ver detalles en 5.3.2 página 63).

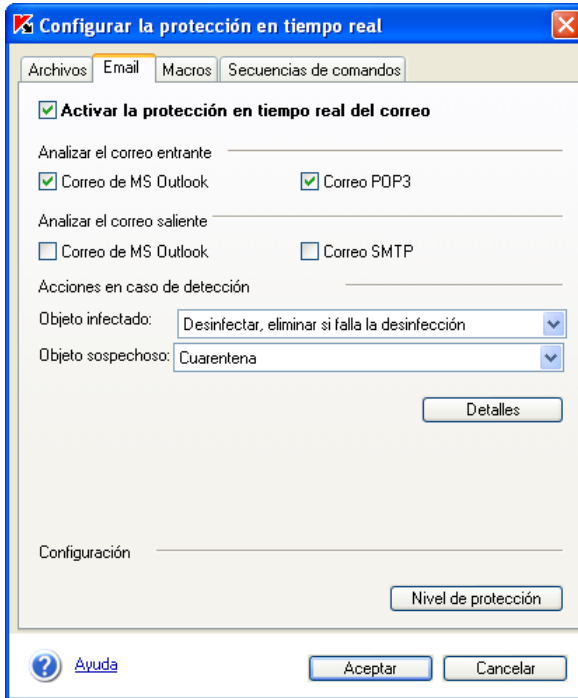


Figura 16. Configuración de tareas de protección de correo

En la sección **Acciones en caso de detección**, elija el tipo de acción aplicada en caso de objeto infectado o sospechoso:

- *Desinfectar, eliminar si falla la desinfección*: la aplicación intenta desinfectar el objeto y si no lo consigue, lo elimina.
- *Cuarentena*: mueve un objeto sospechoso a la cuarentena, para poder analizarlo posteriormente con una base antivirus actualizada, restaurarlo, enviarlo a Kaspersky Lab par su examen, o eliminarlo.
- *Eliminar*: elimina un objeto. Si selecciona esta acción, la aplicación creará una copia del objeto en la zona de respaldo. La copia le permite reparar el archivo o enviarlo para su examen por Kaspersky Lab.

La ventana abierta por el botón **Detalles** permite definir qué objetos deben ser ignorados durante el análisis del sistema, especificar puertos SMTP y POP3, y establecer algunas restricciones (ver Figura 17).

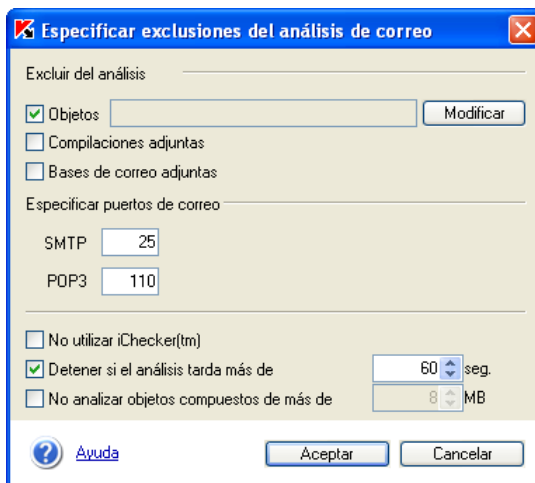


Figura 17. Configuración de excepciones en el correo

En la sección **Excluir del análisis**, active las casillas necesarias para excluir los adjuntos de correo y las bases de archivos durante el proceso de análisis.



Observe que la exclusión de compilaciones de datos adjuntas no tiene influencia en el análisis de archivos autoextraíbles, que siempre son analizados en cualquier nivel de anidación.

Para cambiar a la ventana de creación de la lista de exclusiones, active la casilla **Objetos** y haga clic en **Modificar**. El procedimiento para agregar objetos a la lista de exclusiones es similar al descrito en la sección 5.2.1, p. 46.

Ejemplos de excepciones aceptadas:

- **exe**: todos los archivos con máscara *.exe;
- ***.ex?** – todos los archivos con máscara *.ex? ;
- **test**: todos los archivos con nombre test.



Las máscaras sin rutas relativas o absolutas, o que contienen tan sólo símbolos "?" y "*" no son aceptadas.

En la sección **Especificar puertos de correo**, escriba los números de puerto utilizados para analizar los mensajes de correo transferidos con los protocolos SMTP y POP3.



No utilizar iChecker™: active esta casilla si no desea utilizar esta tecnología para acelerar el análisis antivirus.

- ✓ **Detener si el análisis tarda más de... seg.:** fija la duración máxima del análisis del archivo (en segundos).
- ✓ **No analizar objetos compuestos de más de... Mb:** limita el tamaño máximo de los objetos compuestos analizados.

5.2.3. Análisis del correo en MS Outlook

El correo en MS Outlook es analizado mediante un módulo especial integrado dentro de MS Outlook. Está diseñado para analizar todo el correo entrante (mensajes y adjuntos) antes de su lectura, y el correo saliente antes de ser transmitido.

Para abrir la ventana de análisis de correo, elija **Herramientas / Opciones...** en el menú principal de MS Outlook. En la ventana **Opciones**, cambie a la ficha **Kaspersky Anti-Virus** (ver Figura 18).

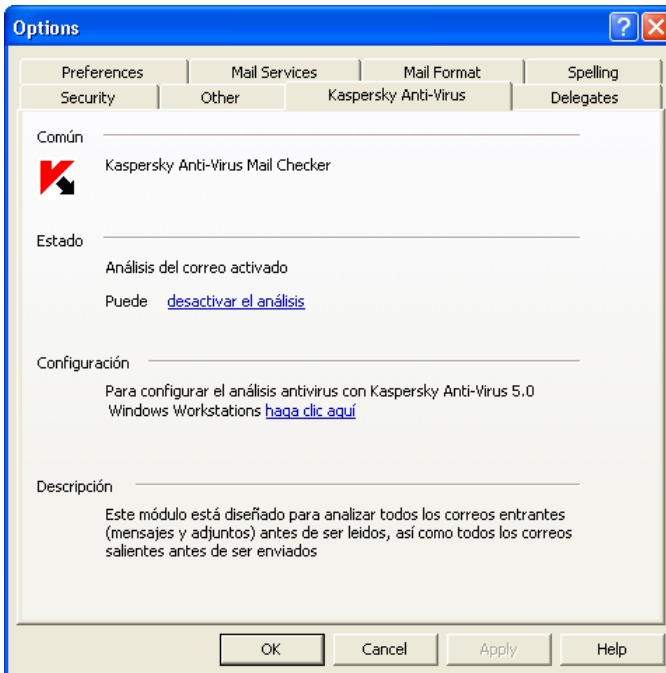


Figura 18. Ficha Kaspersky antivirus en MS Outlook

La sección **Estado** muestra el estado del módulo de análisis de correo. Los mensajes siguientes son posibles, según la condición:

- *Análisis del correo activado.* Puede [desactivar el análisis](#). Este mensaje aparece cuando la aplicación está en ejecución y el análisis bajo MS Outlook está activado.
- *Análisis del correo desactivado.* Puede [activar el análisis](#). Este mensaje aparece cuando la aplicación ha sido iniciada pero el análisis de correo en MS Outlook está desactivado. El modo de análisis del correo se activa automáticamente cuando hace clic en [activar el análisis](#).
- *Análisis del correo desactivado.* Para activar el análisis antivirus, *Kaspersky Anti-Virus 5.0 for Windows Workstations debe estar en ejecución y la protección en tiempo real debe estar activada.* Este mensaje aparece cuando la aplicación no ha sido iniciada, y el análisis de correo en MS Outlook está desactivado.

Para configurar el análisis del correo, utilice el vínculo [haga clic aquí](#) en la sección de **Configuración**. Si utiliza la configuración de alguno de los niveles de protección, se abrirá una ventana (ver Figura 13) donde es posible modificar el nivel de protección antivirus con un cursor. Si utiliza una configuración personalizada, se abrirá una ventana con las opciones de protección en tiempo real en la ficha **E-mail** (ver Figura 16).



Los usuarios de la versión para estaciones de trabajo sólo pueden ver el estado **Análisis del correo activado/desactivado** en la ventana anterior. La sección de configuración no está disponible.

5.2.4. Análisis de secuencias de comandos VBScript y JavaScript

En el modo de protección en tiempo real, la aplicación analiza las secuencias de comandos VBScript y JavaScript antes de ser ejecutadas por el intérprete de comandos del sistema operativo, para evitar la ejecución de código dañino.

La configuración predeterminada es de protección activada. Puede modificar el estado de análisis desde la ventana **Configurar la protección en tiempo real** bajo la ficha **Secuencias de comando** (ver Figura 19).



Activar la supervisión en tiempo real de secuencias de comandos:
Desactive esta casilla para desactivar el análisis en tiempo real de las secuencias de comandos.

En la sección **Acciones**, seleccione qué tipo de acción se aplicará en presencia de una secuencia de comandos potencialmente peligrosa:

- *Preguntar al usuario*: muestra una advertencia acerca de la detección de una secuencia de comandos potencialmente peligrosa y pregunta al usuario acerca de acciones futuras;
- *Bloquear la ejecución*;
- *Permitir la ejecución*.

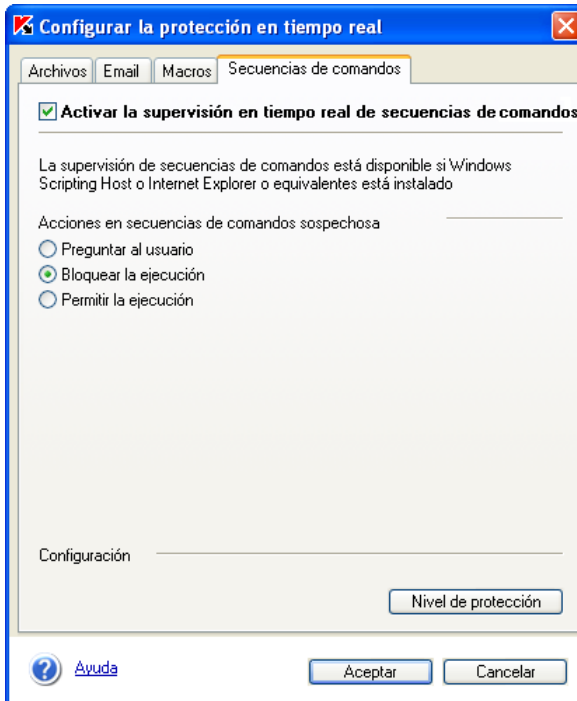


Figura 19. Parámetros de análisis de secuencias de comandos

5.2.5. Análisis de macros

En el modo de protección en tiempo real la aplicación analiza la macro VBA y evita la ejecución de código dañino.

La configuración predeterminada es de protección activada. Puede modificar el estado de análisis desde la ventana **Configurar la protección en tiempo real** bajo la ficha **Macros** (ver Figura 20).

- Activar la supervisión en tiempo real de macros VBA:** Desactive esta casilla para desactivar el análisis en tiempo real de los comandos de macro.

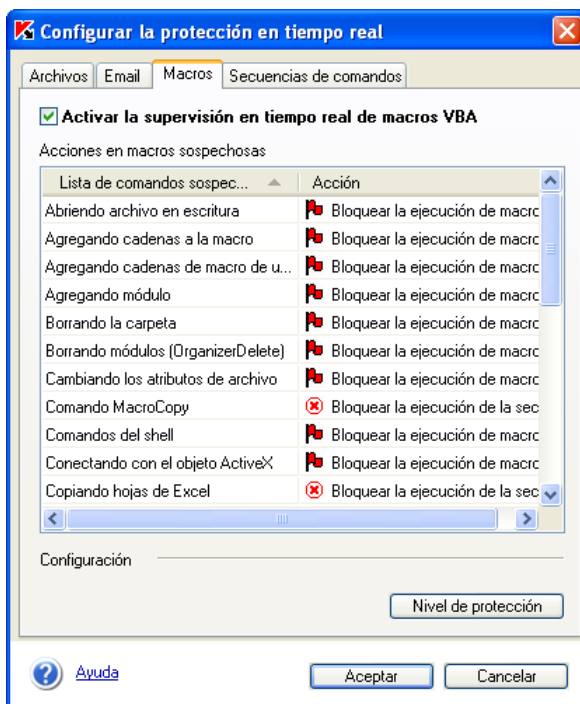


Figura 20. Parámetros de análisis de macros

La tabla **Acciones en macros sospechosas**, permite examinar la lista de macros sospechosas. Utilice la columna **Acción** para especificar qué tipo de acción aplicará el programa antivirus cuando detecte un comando de macro sospechoso:


- Habilitar la ejecución de macros:** (bandera verde).
- Preguntar al usuario:** el icono que representa una campana señala que el programa pedirá al usuario que elija otras acciones posibles.
- Bloquear la ejecución de macros:** (bandera roja).
- Bloquear la ejecución de la secuencia de comandos:** pone fin a la ejecución de la macro ().

5.3. Análisis a petición

El modo de *análisis a petición* es el modo diseñado para buscar código dañino, desinfectar o eliminar objetos así como poner en cuarentena objetos sospechosos a petición del usuario o del administrador de la estación de trabajo.



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

- [Analizar Mi PC](#) ejecuta un análisis completo del sistema de acuerdo con la configuración actual (ver adelante). El mismo resultado puede conseguirse con el vínculo [realizar un análisis completo](#) en el panel derecho de la ficha **Protección**, y con el elemento del menú contextual **Analizar Mi PC** abierto con un clic derecho en  en la barra del sistema.
- [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 21) que contiene una lista de objetos disponibles para análisis, con botones para agregar elementos a la lista e iniciar el análisis.

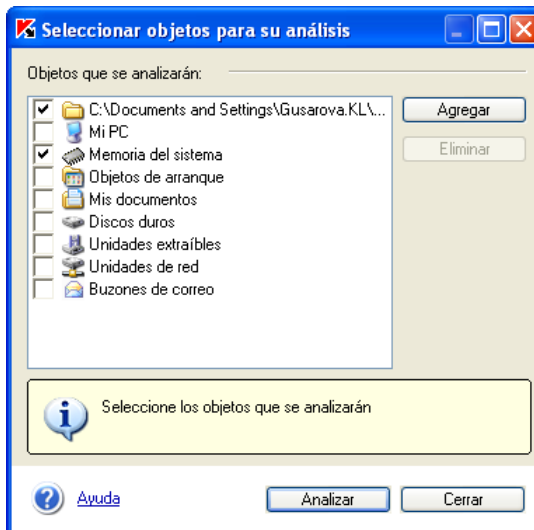


Figura 21. Seleccionar objetos para su analisis

Los objetos también pueden seleccionarse con los medios estándar de Windows, por ejemplo, en la ventana del **Explorador** o desde el **Escritorio**. Para ello, sitúe el cursor sobre el nombre del objeto seleccionado, haga clic derecho para abrir el menú contextual de Windows y seleccione el comando **Buscar virus** (ver Figura 22).

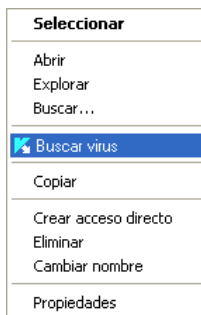


Figura 22. Análisis de un objeto seleccionado con el menú de Windows



Asegúrese de que Kaspersky Anti-Virus está cargado antes de iniciar el análisis de un objeto seleccionado con los medios de Windows.



Para examinar o modificar la configuración del análisis a petición del equipo:

1. Haga clic en el vínculo [Análisis de mi PC](#) en el panel izquierdo de la ficha **Configuración** (ver Figura 5). El programa abre una ventana con la configuración de la tarea para análisis completos. Haga clic en **Configurar el análisis** para cambiar a la ventana de configuración.
2. Se abre la nueva ventana **Configurar el análisis a petición** (ver Figura 23) en la pantalla. Puede modificar el nivel de protección antivirus o ajustarla mediante parámetros avanzados.

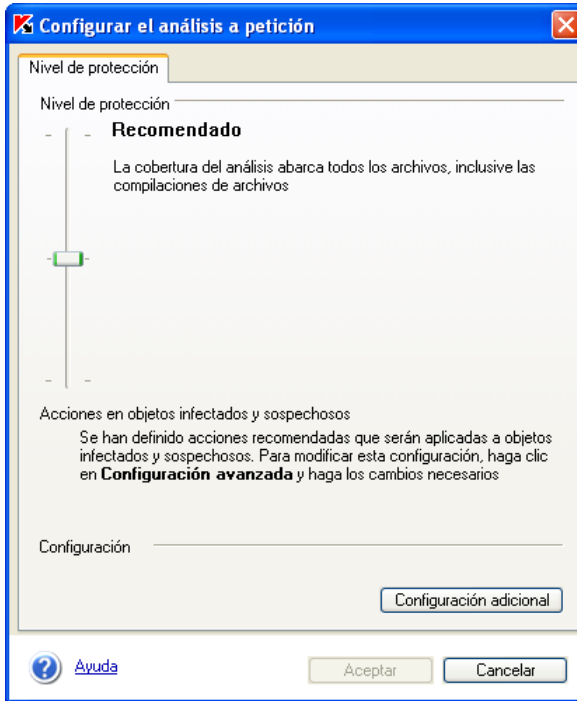


Figura 23. Selección del nivel de protección para el análisis a petición

Con el cursor **Nivel de protección**, establezca uno de los tres niveles de protección antivirus (ver detalles en la sección 4.2 pág. 31).

El botón **Configuración adicional** permite abrir la ventana (ver Figura 24) donde revisar la configuración correspondiente al nivel seleccionado, o utilizar ésta como modelo para su propia configuración personalizada. El nivel de protección cambiará en ese caso a **Personalizado**.

La ventana de configuración permite definir objetos para su análisis, así como qué tipo de acciones aplicar en presencia de objetos infectados o sospechosos; también puede establecer excepciones.

Seleccione los objetos en la sección **Objetos que se analizarán**:

- *Todos los objetos*: todos los objetos del sistema de archivos serán analizados.
- *Objetos infectables según formato*: se analizan los objetos potencialmente infectados. El proceso de análisis toma en cuenta el formato de archivo.

- **Objetos infectables según extensión:** se analizan los objetos potencialmente infectados. La aplicación utilizará la extensión para determinar si un archivo debe ser analizado.

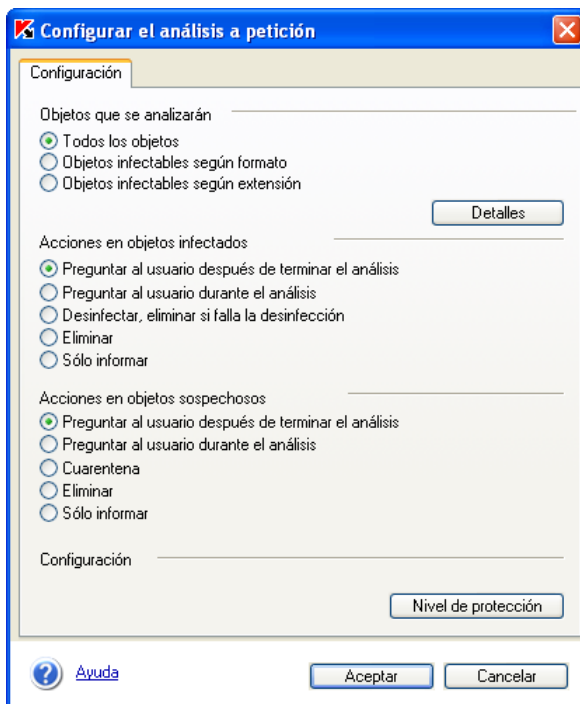


Figura 24. Configuración del análisis a petición. **Configuración**

En las secciones consagradas a **Acciones en objetos infectados/sospechosos**, elija el tipo de acción aplicada en estos casos:

- *Preguntar al usuario después de terminar el análisis:* se pospone al final del análisis la decisión sobre las acciones tomadas en presencia de archivos infectados o sospechosos. Una vez terminado, Kaspersky Anti-Virus presenta la lista de todos los objetos infectados o sospechosos, y recomienda una acción para cada objeto de la lista.
- La opción *Preguntar al usuario durante el análisis* permite preguntar por las acciones a tomar en objetos infectados o sospechosos durante el análisis. Una pregunta contiene todas las acciones disponibles para un objeto, y una de ellas corresponde a la acción recomendada por los expertos de Kaspersky Lab. Seleccione este modo de actuación si no tiene previsto separarse del equipo mientras realiza el análisis.

- *Desinfectar, eliminar si falla la desinfección:* la aplicación intenta desinfectar el objeto y si no lo consigue, lo elimina.
- *Cuarentena:* mueve un objeto sospechoso a la cuarentena, para poder analizarlo posteriormente con una base antivirus actualizada, restaurarlo, enviarlo a Kaspersky Lab para su examen, o eliminarlo.
- *Eliminar:* elimina un objeto. Si selecciona esta acción, la aplicación creará una copia del objeto en la zona de respaldo. La copia le permite reparar el archivo o enviarlo a Kaspersky Lab para su examen.
- *Sólo informar:* no se toma ninguna acción sobre los objetos infectados o sospechosos, la aplicación sólo registra su detección. Le recomendamos no utilizar este modo ya que los archivos infectados o sospechosos permanecerán en su equipo, lo que hace prácticamente imposible evitar la infección.

Preguntar al usuario después de terminar el análisis: es la acción recomendada para todos los niveles de protección en presencia de objetos sospechosos o infectados durante el análisis a petición.

El botón **Detalles** permite abrir una ventana donde definir los archivos y los tipos de archivos que deben ser ignorados durante el análisis a petición, así como activar/desactivar el uso de las tecnologías iChecker™ e iStreams™ (ver Figura 25).

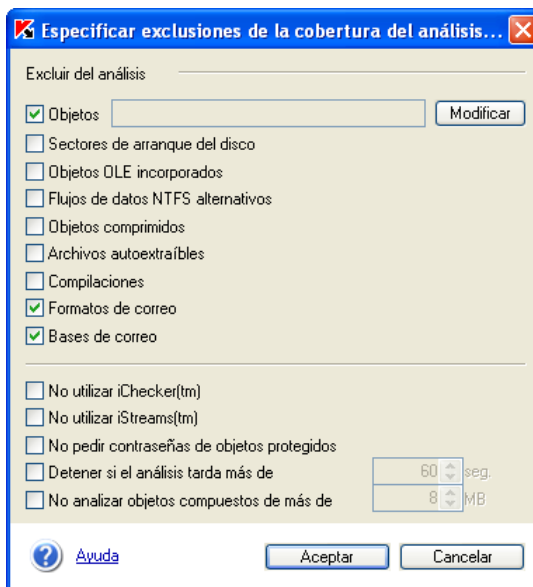


Figura 25. Configuración de excepciones para el análisis a petición

En la sección **Excluir del análisis**, active las casillas correspondientes a los objetos que no deben ser analizados en el modo de protección a petición.

Para cambiar a la ventana de creación de la lista de exclusiones, active la casilla **Objetos** y haga clic en **Modificar**. El procedimiento para agregar objetos a la lista de exclusiones es similar al descrito en la sección 5.2.1 pág. 43.

- No utilizar iChecker™, No utilizar iStreams™**: active estas casillas si no desea utilizar estas tecnologías para acelerar el análisis antivirus.
- La opción **No pedir contraseñas de objetos protegidos** – desactivará la pregunta por la contraseña de los objetos protegidos. Estos objetos serán ignorados durante el proceso de análisis.
- Detener si el análisis tarda más de... seg.:** especifica el tiempo máximo de análisis de un archivo único (en segundos).
- No analizar objetos compuestos de más de... Mb:** limita el tamaño máximo de los objetos compuestos analizados.

5.3.1. Análisis de compilaciones

Kaspersky Anti-Virus analiza compilaciones de datos en el modo a petición tan sólo en los niveles de **Máxima protección** y **Recomendado**, siempre que no se establezcan exclusiones.

Puede comprobar la configuración de exclusiones para un análisis completo del equipo en la ventana **Configuración de exclusiones** (ver Figura 25). Asegúrese de que la casilla **Compilaciones** está desactivada.



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 26).

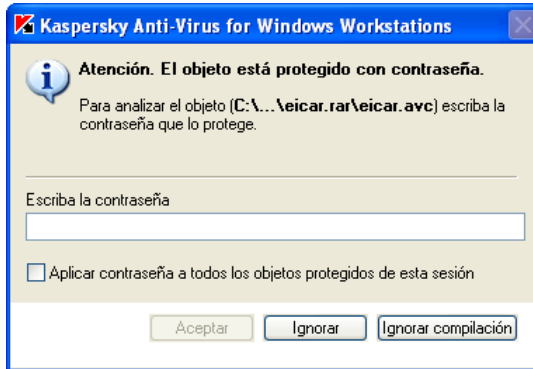


Figura 26. Escritura de contraseña para analizar un archivo protegido

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

Para analizar otra compilación de datos protegida, Kaspersky Anti-Virus utiliza automáticamente la contraseña de la primera compilación en la segunda. Sólo deberá indicar otra contraseña si la primera no es válida.

Si desconoce la contraseña, el programa no podrá analizar el contenido de compilaciones de datos protegidas. Le recomendamos que haga clic en **Ignorar** y continúe con el análisis.

Si una compilación contiene asimismo otra compilación protegida por contraseña, haga clic en **Ignorar compilación** para excluirla del análisis actual. todos los demás objetos dentro de la compilación 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 ha activado 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**, la aplicación intentará aplicar la misma contraseña a todos los restantes objetos que estén cifrados, sin mostrar ningún cuadro de diálogo.

5.3.2. Procesado diferido de objetos

Los objetos infectados deben ser tratados manualmente si eligió la opción predeterminada *Preguntar al usuario después de terminar el análisis* como acción del antivirus (ver Figura 24) y si se detectan posteriormente objetos infectados o sospechosos durante el análisis.

Después de terminar el análisis, el antivirus abre la ventana **Control de objetos infectados** (ver Figura 28), 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 7) 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 27) mostrado 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...**

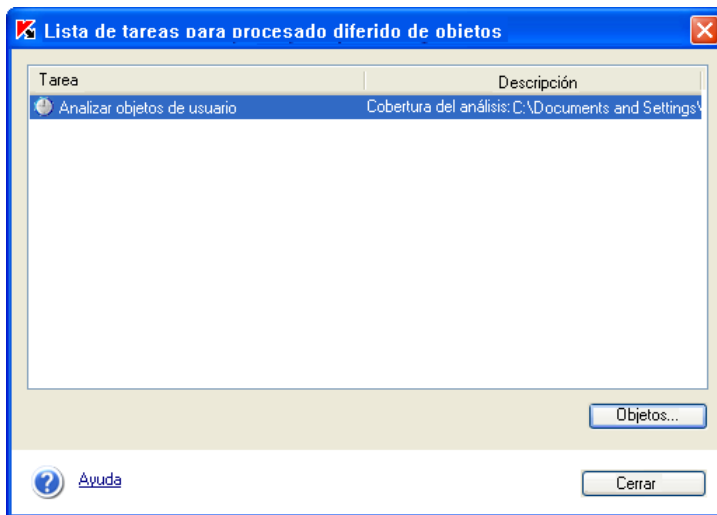


Figura 27. Lista de tareas para procesado diferido de objetos

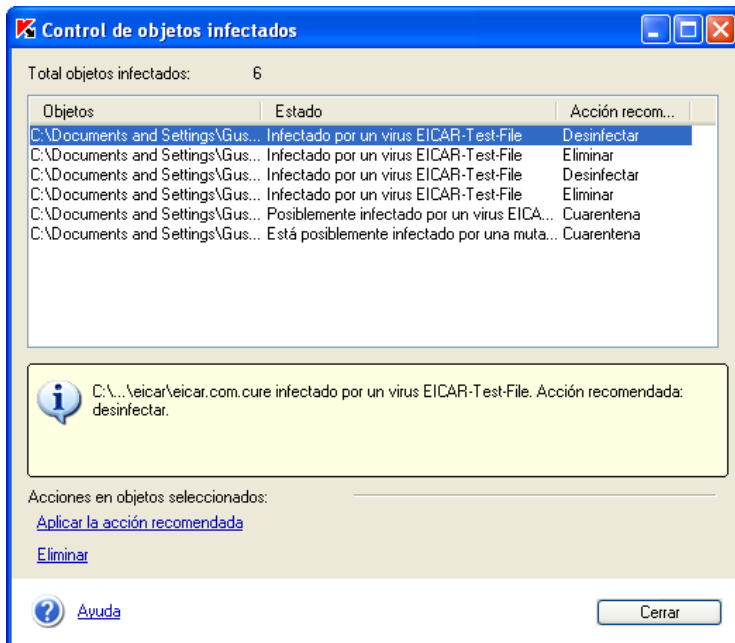


Figura 28. Control de objetos infectados y sospechosos



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 28). 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 los expertos de 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 son retirados de la lista. Una vez procesados todos los objetos de la lista, haga clic en **Cerrar**.

5.4. Tareas del usuario

Una lista de tareas sistema es creada en el momento de la instalación del antivirus. Esta lista incluye tanto las tareas actualización (actualización de bases antivirus, actualización de módulos de aplicación, anulaciones de bases de datos) como las tareas de análisis (análisis completo de Mi PC, análisis automático al iniciar la aplicación, análisis de unidades extraíbles, y análisis de la cuarentena).

Puede iniciar las tareas sistema predeterminadas, y configurar sus parámetros y planificación. Estas tareas no pueden ser eliminadas.



El proceso de configuración de tareas de actualización de la base antivirus y de los componentes de aplicación se describe en Capítulo 5 pág. 33. La tarea de anulación de las actualizaciones más recientes no tiene una configuración específica.

Mientras trabajan con el programa antivirus, los administradores pueden crear tareas de diferentes tipos y administrar su funcionamiento.



Los usuarios de estaciones de trabajo no tienen acceso a la creación y configuración de tareas. Pueden ver una lista de tareas creadas por el administrador en el panel izquierdo de la ficha **Protección** (ver Figura 4) y ejecutar estas tareas.

5.4.1. Lectura de los resultados de las tareas

Para mostrar la lista de tareas disponibles en una estación de trabajo, haga clic en el vínculo [Tareas del usuario](#) en el panel izquierdo de la ficha **Configuración** (ver Figura 5). El vínculo abre una ventana **Lista de tareas del usuario** (ver Figura 29) con la lista de tareas de protección existentes para el equipo.

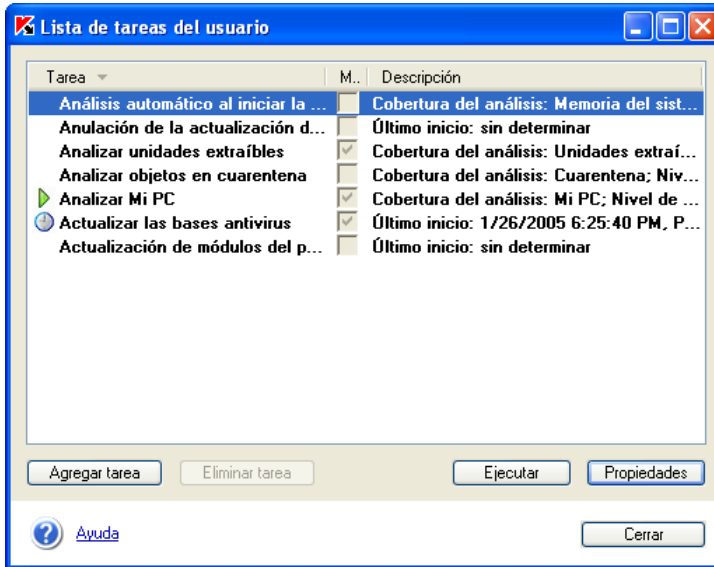





Figura 29. Lista de tareas del usuario

Una breve descripción se incluye para cada tarea de la lista: cobertura, nivel de protección y fecha de próximo inicio. Cada tarea posee una casilla **Mostrar en la ventana principal**, que determina su presentación en la ficha **Protección**: los usuarios de estaciones de trabajo verán la tarea en el panel izquierdo de la ficha si la casilla está activada; en ese caso, los usuarios podrán ejecutar la tarea.

La lista puede también incluir tareas creadas con Kaspersky Administration Kit (vea la sección 6.2 pág. 114).

En función de la situación, los iconos siguientes pueden aparecer a la izquierda del nombre de tarea:

-  : la tarea ha sido planificada y se ejecutará automáticamente de acuerdo con su calendario.
-  : la tarea ha sido iniciada por el usuario y está en ejecución en este momento.
-  : la tarea ha sido iniciada de acuerdo con su planificación y está en ejecución en este momento.

Bajo la lista de tareas existen botones de control que permiten al usuario crear nuevas tareas, eliminar de la lista o ejecutar tareas, así como examinar o modificar la configuración y la planificación de las tareas. Para realizar

cualquiera de las acciones anteriores, seleccione la tarea en la lista y haga clic en el botón correspondiente.

Para eliminar una tarea, selecciónela y haga clic en **Eliminar tarea**. Observe sin embargo que sólo puede quitar de la lista los objetos agregados manualmente. No se pueden eliminar las tareas sistema.

Para ejecutar una tarea, selecciónela y haga clic en **Ejecutar**. Se abrirá una ventana representando el avance de la tarea.

Cuando una tarea planificada está en ejecución (ver Figura 1), la opción **Tareas en ejecución** aparece en el menú contextual. La selección de esta opción abre un submenú con la lista de todas las tareas planificadas en ejecución en ese instante. seleccione la tarea deseada en la lista (ver Figura 7) para mostrar información sobre su avance.

Para revisar o modificar las propiedades de tarea, haga clic en **Propiedades** o haga doble clic en el nombre de la tarea en la lista.

En el caso de las tareas sistema predeterminadas, puede examinar la información acerca de los objetos comprobados durante la ejecución de una tarea específica. En el caso de tareas de usuario, es posible seleccionar o modificar el nombre de la tarea, agregar o modificar una lista de objetos que serán analizados durante la ejecución de una tarea, y configurar sus parámetros.

5.4.2. Crear una nueva tarea

Si desea crear una nueva tarea personalizada, utilice el botón **Agregar tarea**. Se abrirá una ventana (ver Figura 30) que contiene dos fichas: **Configuración** y **Planificación**.

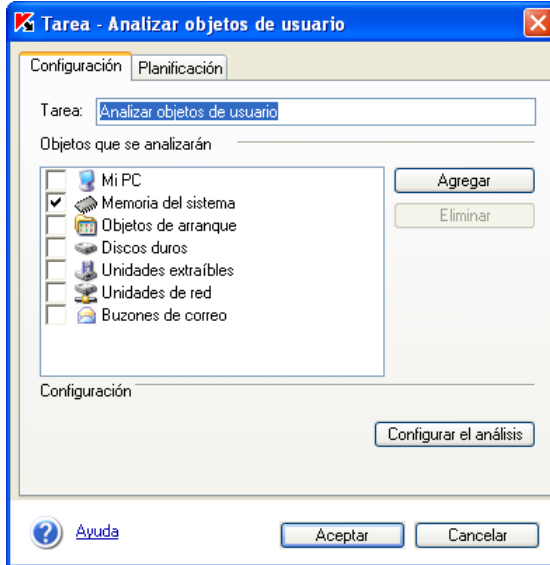


Figura 30. Creación de nueva tarea, ficha **Configuración**

En la casilla **Tarea** de la ficha **Configuración** (ver Figura 30), escriba el nombre de la nueva tarea. En la sección **Objetos que se analizarán**, cree una lista de objetos que deben ser analizados al iniciar la tarea, con los botones **Agregar** y **Eliminar**. Puede modificar la configuración del modo de análisis a petición con el botón **Configurar el análisis** (ver sección 5.3 pág. 56).

En la ficha **Planificación** (ver Figura 31) puede configurar la ejecución automática de la tarea. Para ello, active la casilla **Planificar la tarea**. Deberá iniciar la tarea manualmente, si la casilla está desactivada.

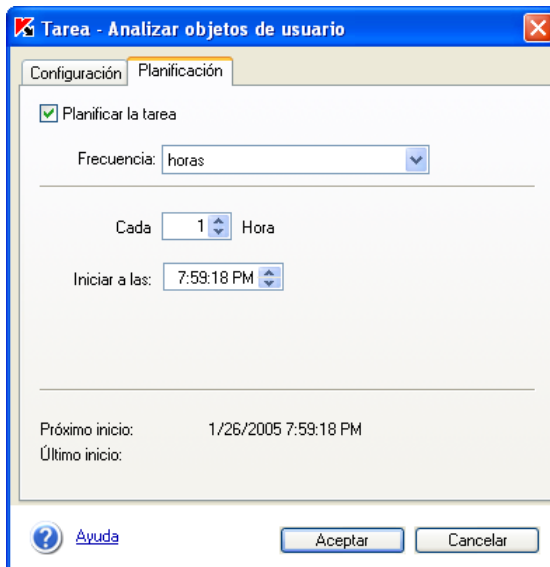
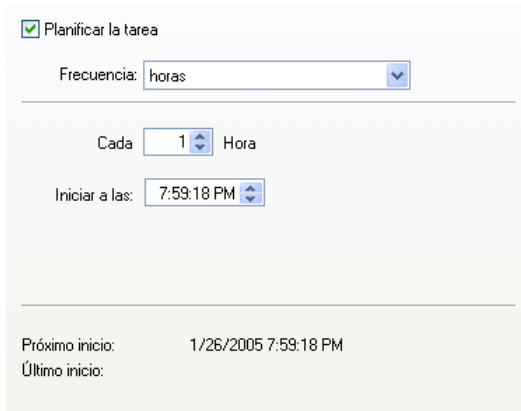


Figura 31. Creación de nueva tarea, ficha **Planificación**

Utilice el campo **Frecuencia** para definir la periodicidad de la tarea. Las opciones siguientes están disponibles: *horas*, *días*, *semanas*. Dependiendo de la opción seleccionada, la parte central de la ventana que contiene los campos de entrada irá variando su apariencia:

- *Horas*: la tarea se ejecutará, de acuerdo con lo planificado, cada x horas. Defina la frecuencia (en horas) así como la fecha y hora de primera ejecución.



Planificar la tarea

Frecuencia: horas

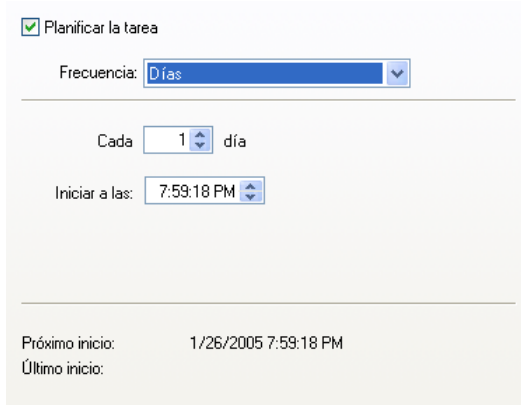
Cada 1 Hora

Iniciar a las: 7:59:18 PM

Próximo inicio: 1/26/2005 7:59:18 PM
Último inicio:

Figura 32. Planificación de tarea con frecuencia horaria

- **Días:** la tarea se ejecutará, de acuerdo con lo planificado, cada x días. Defina la frecuencia (en días) así como la hora de primera ejecución.



Planificar la tarea

Frecuencia: Días

Cada 1 día

Iniciar a las: 7:59:18 PM

Próximo inicio: 1/26/2005 7:59:18 PM
Último inicio:

Figura 33. Planificación de tarea con frecuencia diaria

- **Semanas:** la tarea se ejecutará, de acuerdo con lo planificado, cada x semanas. Defina la frecuencia (en semanas) y seleccione el día de semana y la hora de ejecución de la tarea.

Planificar la tarea

Frecuencia:

Cada semana

Iniciar a las:

Día de semana:

Próximo inicio: 1/30/2005 7:59:18 PM
Último inicio:

Figura 34. Planificación de tarea con frecuencia semanal

5.5. Funciones avanzadas

Kaspersky Anti-Virus dispone de numerosas opciones adicionales de ajuste y utilización del producto, incluyendo:

- Operaciones con objetos sospechosos desplazados a cuarentena.
- Operaciones con copias de respaldo de objetos eliminados o modificados por el programa antivirus, y colocadas en la zona de respaldo.
- Examen del registro de actividad de la aplicación.
- Configuración adicional.

5.5.1. 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 guarda en un directorio de respaldo, desde el cual es posible restaurar más tarde el objeto, si éste contiene datos importantes.

5.5.1.1. Configuración del respaldo



Para examinar o modificar la configuración de la cuarentena o de la zona de respaldo,

haga clic en el vínculo [Cuarentena y respaldo](#) en el panel izquierdo de la ficha **Configuración**.

Puede definir los parámetros de los dos directorios de almacenamiento con las fichas de la ventana **Configuración de cuarentena y respaldo**.

Escriba la ruta del directorio de cuarentena en la ficha **Cuarentena** (ver Figura 35). Haga clic en **Examinar** para modificar la ruta.

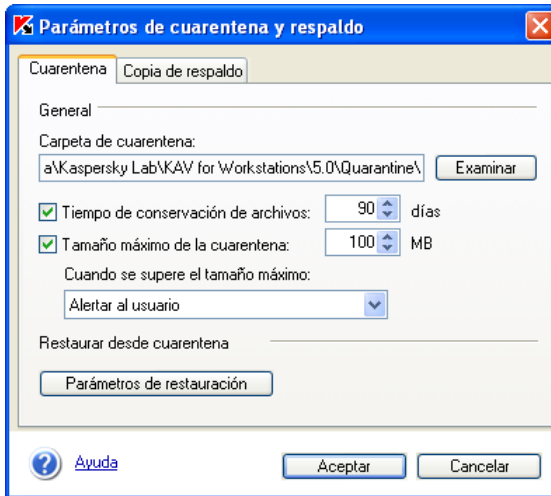


Figura 35. Parámetros de cuarentena y respaldo

Tiempo de conservación de archivos: desactive la casilla si no quiere limitar el tiempo de conservación. La casilla está activada de forma predeterminada y el tiempo de conservación es de 90 días. Puede modificar el periodo de conservación en el campo asociado.

Tamaño máximo de la cuarentena: active la casilla para restringir el tamaño total de los archivos en el almacén. De forma predeterminada, el tamaño de almacenamiento es ilimitado.


Seleccione la acción realizada por la aplicación cuando el almacén esté lleno:


- *Eliminar los archivos más antiguos:* se eliminan los archivos en cuarentena anteriores al resto.

- **Alertar al usuario:** la aplicación mostrará un mensaje con las acciones posible cuando se supera el tamaño de la cuarentena.

Defina los parámetros para restaurar los objetos del almacén en la ventana (ver Figura 36) que se abre cuando hace clic en **Parámetros de restauración**.

La casilla carpeta **de restauración** contiene de forma predeterminada la ruta del directorio donde son colocados los objetos durante su restauración.

Con el fin de restaurar los archivos en un directorio determinado, seleccione  **Restaurar todos los objetos en la carpeta de restauración**. Puede elegir la opción **Restaurar en la ubicación de origen, si se conoce** para restaurar los archivos al directorio donde se encontraban antes de ser movidos a cuarentena.

Para confirmar la ruta antes de restaurar cada objeto individualmente, active la casilla  **Confirmar la ruta antes de restaurar**.

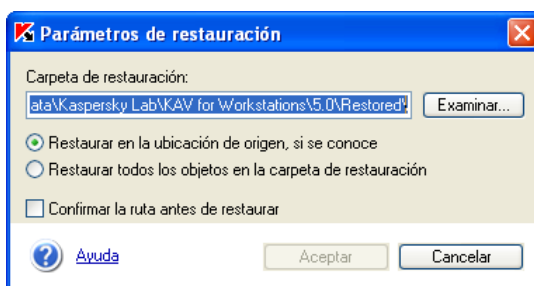


Figura 36. Parámetros de restauración

La configuración de la zona de respaldo puede realizarse desde la ficha **Respaldo** (ver Figura 37). Los parámetros son similares a la Cuarentena (ver anterior).

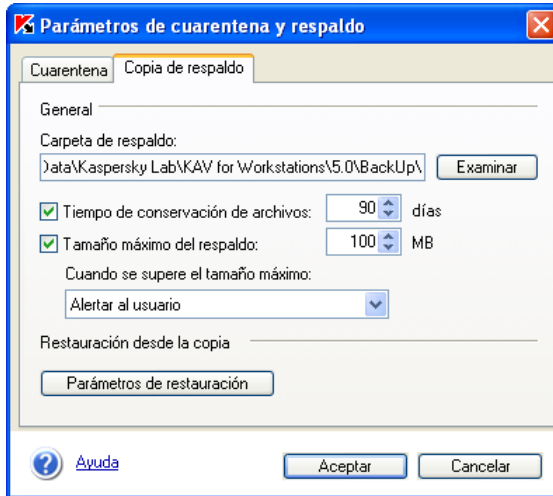


Figura 37. Configuración de la zona de respaldo

5.5.1.2. Trabajar con la cuarentena

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.)

Le recomendamos actualizar la base antivirus antes de analizar objetos en cuarentena. Es posible que la actualización contenga un registro de los virus que se sospecha están presentes en los archivos de cuarentena, que pueden así ser desinfectados.

Kaspersky Anti-Virus vuelve a analizar la cuarentena después de cada actualización de su base antivirus. Si necesita comprobar 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 38), que puede abrir con un clic en el vínculo [Cuarentena](#) de la ficha **Protección** (ver Figura 4) de la ventana principal de la aplicación o en el vínculo [Ver cuarentena](#) de la ventana de análisis terminado (ver Figura 7).

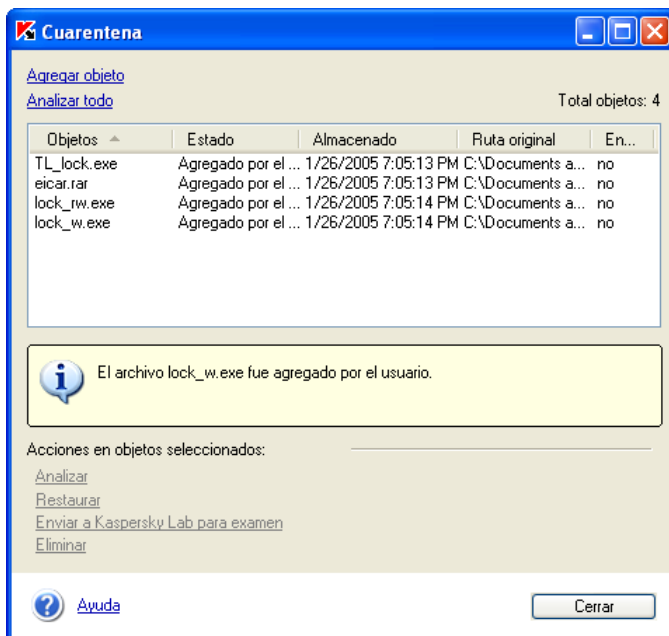


Figura 38. Ventana de cuarentena

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 la aplicación. 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*, *desinfectado* o *falsa alarma*. 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.



Los archivos en la carpeta 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, o en una carpeta de destino especificada. 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 posiblemente infectados a Kaspersky Lab para su examen. Recomendamos enviar un objeto para ser examinado por expertos 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](#).

5.5.1.3. Trabajar con la zona de respaldo

Kaspersky Anti-Virus 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 **Respaldo** (ver Figura 39), que se abre con un clic en el vínculo [Respaldo](#) de la ficha **Protección** (ver Figura 4) 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. Para restaurar un objeto, selecciónelo en la lista y haga clic en [Restaurar](#).
- Eliminar de la cuarentena cualquier archivo o grupo de archivos seleccionados. Para eliminar un archivo, selecciónelo en la lista y haga clic en [Eliminar](#).

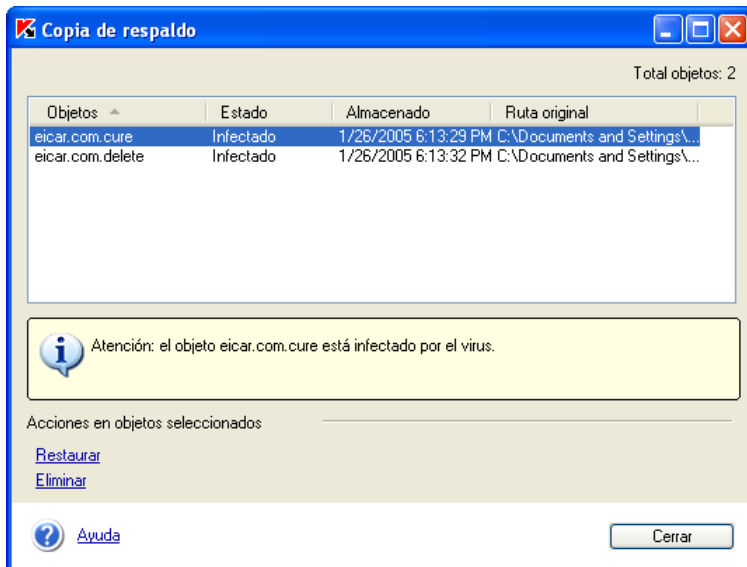


Figura 39. Zona de respaldo (ventana)

5.5.2. Trabajar con informes

La aplicación crea un informe cuando realiza un análisis completo del equipo o actualiza la base antivirus. 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 registro con los resultados de todas las tareas realizadas (ver Figura 40), que puede abrir con un clic en el vínculo [Informes](#) del panel izquierdo de la ficha **Protección** (ver Figura 4). Queda registrado el estado de cada tarea, con su fecha y hora de terminación.

La información de estado acerca del objeto procesado puede tener las categorías siguientes:

- ✔ *Notificaciones de éxito* (por ejemplo, el objeto está limpio, fue desinfectado o eliminado).
- ▶ o ⓘ *Un mensaje* informativo (por ejemplo, tarea iniciada, tarea terminada, tarea en ejecución, tarea interrumpida).
- *Advertencia* (por ejemplo, se ha encontrado un objeto sospechoso o una compilación de archivos protegidos con contraseña).
- *Evento grave* (por ejemplo, se ha detectado un virus).

- *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**.

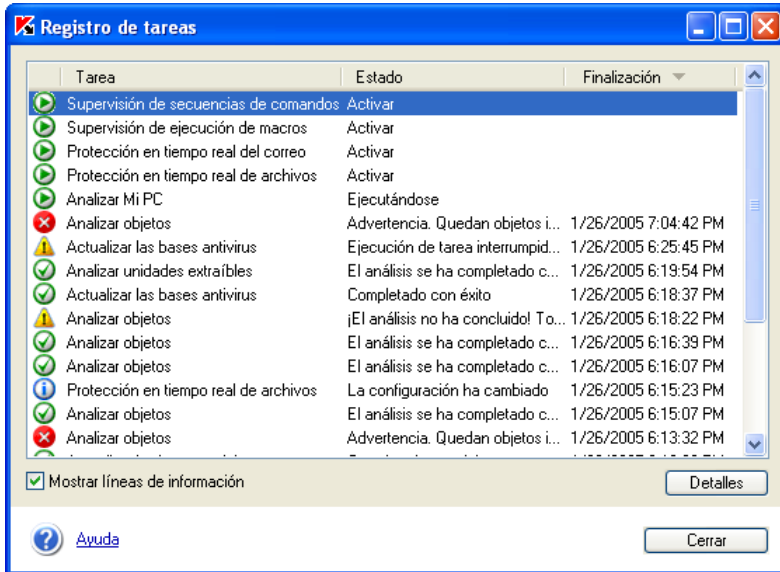


Figura 40. Registro de tareas

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 41) 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.

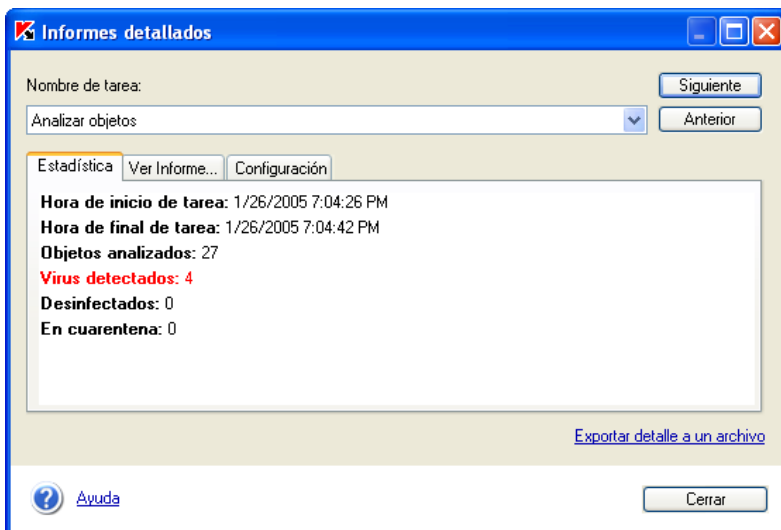


Figura 41. Ficha Estadísticas

La ficha **Ver Informe** (ver Figura 42) contiene información detallada acerca de cada objeto analizado.

La ficha **Configuración** (ver Figura 43) muestra los parámetros de tarea. Muestra tanto los objetos de análisis y el nivel de protección definido para tarea, como las acciones realizadas 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 Registro 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**.

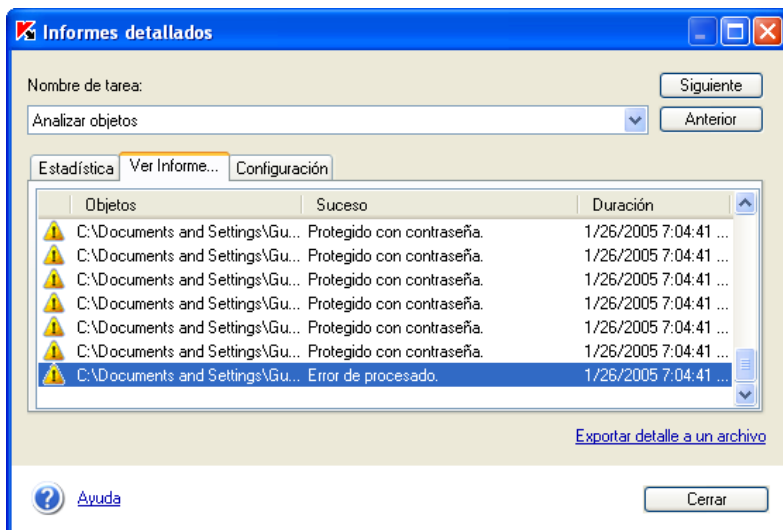


Figura 42. Ficha Ver Informe

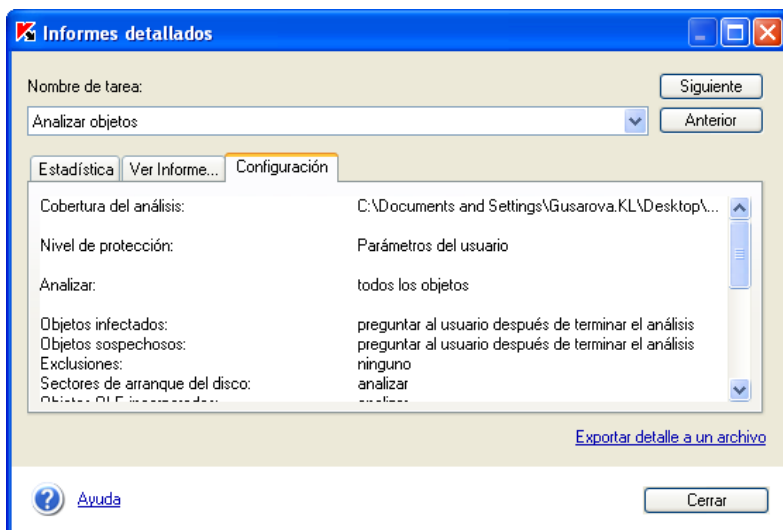


Figura 43. Configuración

Puede ajustar los parámetros del registro de tareas en la ventana **Configuración adicional** (ver Figura 44), abierta con un clic en el vínculo correspondiente en el panel izquierdo de la ficha **Configuración** (ver detalles en

la sección 5.5.3, p.83). También puede define el tiempo máximo de conservación de los informes y habilitar/deshabilitar la inclusión de mensajes informativos en el informe detallado.

5.5.3. Configuración adicional

Además de la posibilidad de configurar tareas específicas, Kaspersky Anti-Virus también cuenta con parámetros generales y de servicio. Para cambiar a la ventana de configuración adicional (ver Figura 44), haga clic en el vínculo [Configuración adicional](#) en el panel izquierdo de la ficha **Configuración** (ver Figura 5) y establezca las opciones necesarias:

- Mostrar el icono de la aplicación en la barra del sistema:** la casilla permite ejecutar Kaspersky Anti-Virus al arrancar el sistema operativo. Después de iniciar, el icono del antivirus aparece en la barra del sistema.
- Mostrar mensajes emergentes:** habilita la presentación de los mensajes emergentes que acompañan ciertas operaciones de Kaspersky Anti-Virus.
- Mostrar el estado del antivirus en la barra del sistema:** habilita la animación del icono de Kaspersky Anti-Virus en la barra del sistema mientras ejecuta las tareas de protección.
- Registrar todos los mensajes en el informe:** permite registrar los mensajes informativos en el archivo de informe detallado.
- Conservar los informes un máximo de... días.** Los informes se conservan de forma predeterminada por treinta días. Puede modificar el periodo indicando un número en el campo asociado.

La aplicación es compatible con la interfaz APM (Administración avanzada de energía) para poder trabajar con ordenadores portátiles. Cuando se habilita esta función, las tareas planificadas no son iniciadas si el indicador de carga de la batería está por debajo de un nivel determinado. La configuración se modifica desde la sección **Ahorro de energía** :

- No iniciar el análisis planificado si la batería es inferior a... %:** desactiva la ejecución de tareas en un portátil, si la carga de batería esté por debajo del nivel permitido. Utilice el cursor o el campo asociado para especificar el nivel mínimo de batería por debajo del cual la aplicación no ejecutará sus tareas antivirus.
- Iniciar la aplicación en el próximo arranque del equipo:** habilita la ejecución de Kaspersky Anti-Virus durante el inicio del sistema operativo.



Recomendamos fuertemente no desactivar el inicio automático de Kaspersky Anti-Virus, ya que esto puede causar la infección de su equipo.

El campo **Servicio de soporte** contiene la dirección de correo electrónico del servicio de soporte de Kaspersky Lab. La dirección se establece automáticamente cuando se instala la aplicación. Puede modificarla si le indicaron una dirección diferente cuando compró el antivirus.

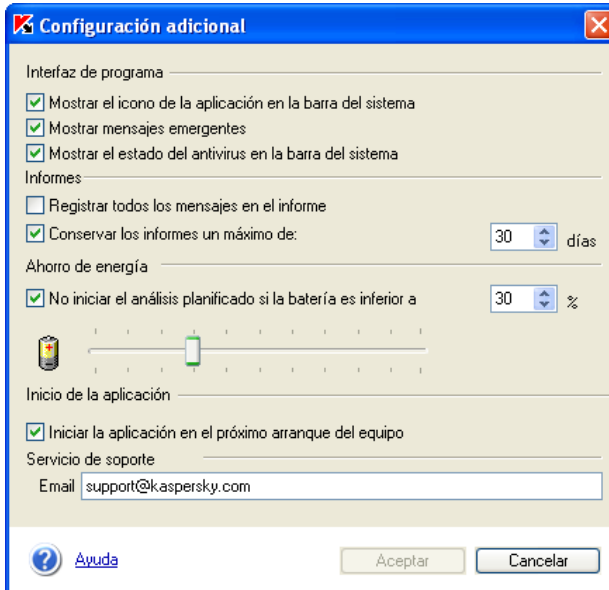


Figura 44. Funciones adicionales de Kaspersky Anti-Virus

CAPÍTULO 6. CONTROL DE LA APLICACIÓN CON KASPERSKY ADMINISTRATION KIT

6.1. Control de directivas

Esta sección describe la creación y administración de directivas para Kaspersky Anti-Virus. Encontrará información detallada acerca del control de directivas en el manual del administrador de Kaspersky Administration Kit 5.0.

6.1.1. Creación de una directiva



Para crear una nueva directiva, proceda de la forma siguiente:

1. En la carpeta **Grupos** del explorador de consola, seleccione un grupo de equipos para asignarlos a la nueva directiva.
2. Seleccione la carpeta **Directivas** dentro del grupo seleccionado, abra el menú contextual, y haga clic en **Nuevo→Directiva...** para iniciar un Asistente para crear una nueva directiva.

La aplicación para la creación de una nueva directiva se organiza como un Asistente de Windows que le guía a través de todo el proceso. Para cambiar entre los cuadros de diálogo del asistente, haga clic en **Anterior** y **Siguiente**. Para terminar el trabajo con el asistente, haga clic en **Terminar**. Para cancelar el asistente en cualquier etapa, haga clic en **Cancelar**.

Paso 1. Información general de la directiva

Los primeros cuadros de diálogo del asistente son de introducción, debe indicar el nombre de la directiva en el campo **Nombre** y seleccionar **Kaspersky Anti-Virus 5.0 for Windows Workstations** en la lista **Elija la aplicación para la que define una directiva**.



Tan sólo es posible crear una directiva de grupo por aplicación. Si una directiva de grupo de nivel superior ya existe, las directivas de niveles inferiores tan sólo pueden alterar los parámetros señalados como modificables en el nivel superior.

Paso 2. Definición del nivel de protección antivirus

En este nivel, necesita seleccionar el nivel de protección antivirus de la nueva directiva (ver detalles en la sección 4.2 pág. 31). La aplicación ofrece tres niveles de configuración predeterminados de la protección antivirus:

Paso 3. Seleccione el origen de la actualización

En esta etapa (ver Figura 45), se le pedirá que configure los parámetros de actualización de la base antivirus y de los módulos de aplicación. Deberá especificar el origen de las actualizaciones y definir la configuración de red en la ventana abierta con **Configuración LAN**. La configuración es idéntica a la configuración local. Encontrará información detallada acerca de esto en la sección 5.1.3 pág. 35.

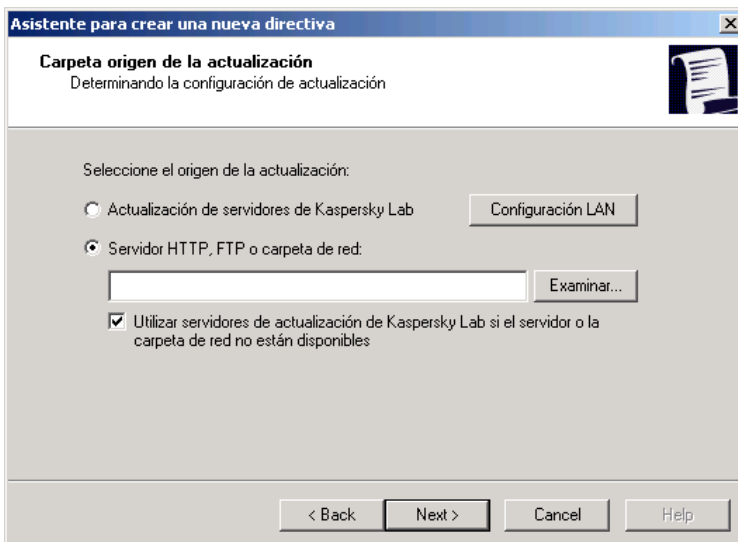


Figura 45. Selección del origen de actualización

Paso 4. Configuración de los parámetros de actualización

En este cuadro de diálogo (ver Figura 46), seleccione la configuración del servicio de actualización de la base antivirus y de los módulos de aplicación. La configuración del proceso de actualización es la misma que para la configuración local. Encontrará información detallada acerca de esto en la sección 5.1.3 pág. 35.

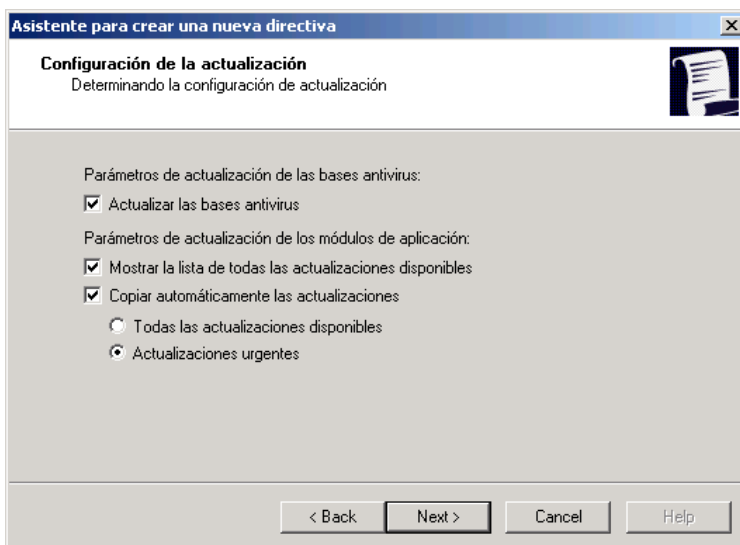


Figura 46. Selección de la configuración del servicio de actualizaciones

Paso 5. Fin de la creación de la directiva

La ventana final del asistente le informa de que una nueva directiva ha sido creada con éxito.

Después de cerrar el asistente, la directiva de esta aplicación se agrega a la carpeta de **Directivas** del grupo correspondiente y se muestra en el panel de resultados.

Para aplicar una directiva, modifique su configuración e imponga restricciones a la modificación de los parámetros de tarea y aplicación. La nueva directiva se aplica a los equipos clientes hasta la primera sincronización de éstos con el servidor.

Una directiva se aplica de la forma siguiente: las tareas residentes existentes (por ejemplo, la protección en tiempo real) en ejecución dentro de un equipo

cliente, continúan con la nueva configuración de directiva. Las tareas periódicas actualmente en ejecución, como el análisis a petición o las actualizaciones, continúan con la antigua configuración. En este caso, los cambios se aplicarán la próxima vez que se reinicie la aplicación.

Puede copiar y desplazar directivas de un grupo a otro, y administrarlas con los comandos estándar del menú contextual (**Copiar/Pegar**, **Cortar/Pegar** y **Eliminar**), o con los mismos comandos del menú **Acción**. Para mover una directiva, arrastre su icono con el puntero hasta otro lugar.

6.1.2. Examen y modificación de la configuración de la directiva

Mientras realiza modificaciones, puede personalizar la configuración de directiva, impedir modificaciones en sus parámetros dentro de grupos anidados, y bloquear los parámetros de aplicación y tareas para que otros usuarios no puedan modificarlos.



Para bloquear la modificación de los parámetros de directiva por parte de los usuarios, señale esta directiva con el icono de "bloqueo": . Los parámetros que es posible modificar están señalados como .



Para ver o modificar la configuración actual de la directiva:

1. En la carpeta **Grupos** del explorador de consola, seleccione un grupo de equipos para el que desea modificar la configuración de directiva.
2. Seleccione la carpeta **Directivas** dentro de este grupo. Todas las directivas disponibles para este grupo son mostradas en el panel de resultados.
3. En la lista de directivas, seleccione una directiva para **Kaspersky Anti-Virus 5.0 for Windows Workstations** (el nombre de la aplicación aparece en la columna **Programa**).
4. Abra el menú contextual de la directiva seleccionada y haga clic en **Propiedades**. Se abrirá una ventana con las propiedades de directiva para la aplicación **Kaspersky Anti-Virus 5.0 for Windows Workstations** y con varias fichas. |

Las fichas **General**, **Forzado** y **Control de eventos** son fichas estándar de Kaspersky Administration Kit (consulte el Manual del administrador de Kaspersky Administration Kit para obtener detalles).

Las fichas restantes muestran parámetros específicos de Kaspersky Anti-Virus 5.0 for Windows Workstations. Describimos a continuación estas fichas con mayor detalle.

6.1.2.1. Información de la aplicación

La ficha **General** (ver Figura 47) muestra información general acerca de la directiva:

- Nombre de directiva;
- La aplicación de esta directiva se asigna a (**Kaspersky Anti-Virus 5.0 for Windows Workstations**);
- Versión de aplicación;
- Fecha y hora de creación;
- Fecha y hora de la última modificación.

En esta ficha, puede modificar el nombre de la directiva.

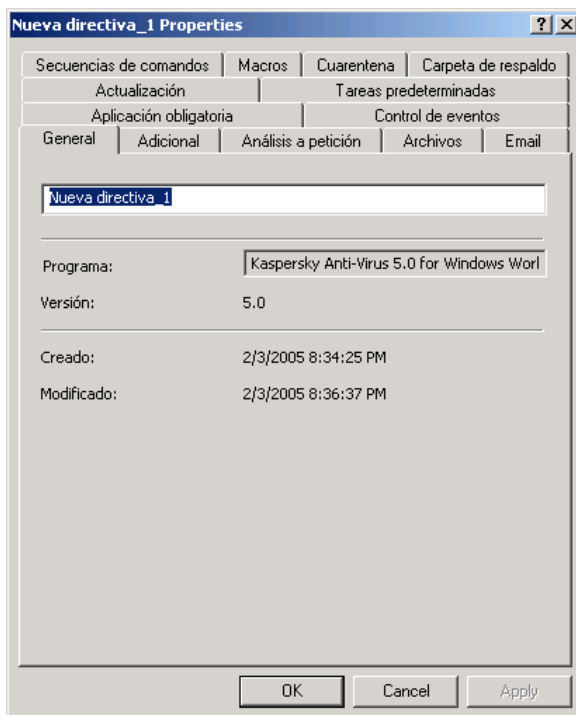


Figura 47. La ficha **General**

6.1.2.2. **Análisis a petición**

Utilice la ficha **Análisis a petición** (ver Figura 48) para configurar la directiva para el análisis a petición.

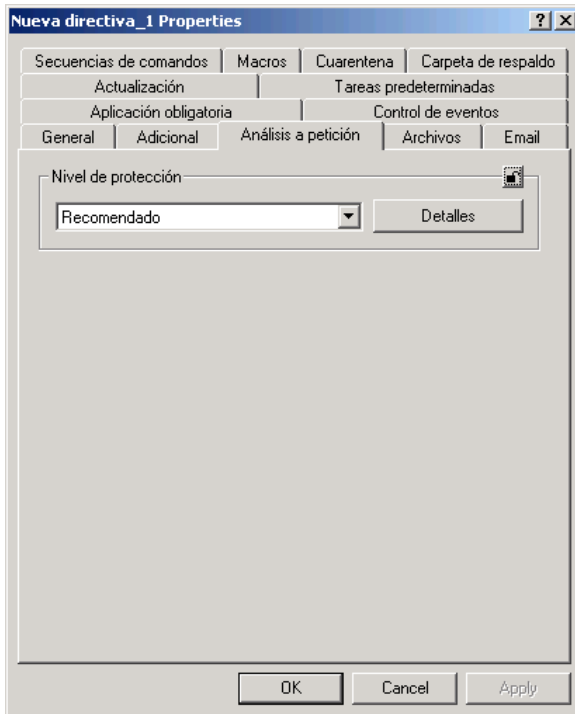


Figura 48. La ficha **Análisis a petición**

La lista **Nivel de protección** permite seleccionar uno de los tres niveles de protección predeterminados de protección antivirus (ver sección 4.2, p.33):

Haga clic en **Adicional** para abrir una ventana donde revisar la configuración correspondiente al nivel seleccionado, o para utilizarla como modelo de su propia configuración. Esto cambiará el nivel de nivel de protección a **Personalizado**.

La ventana de configuración adicional contiene las fichas **Cobertura de análisis**, **Accion** y **Adicional**.

Utilice la ficha **Cobertura de análisis** (ver Figura 49) para definir el tipo y la lista de objetos excluidos del análisis (para obtener detalles vea la sección 5.3 pág. 56).

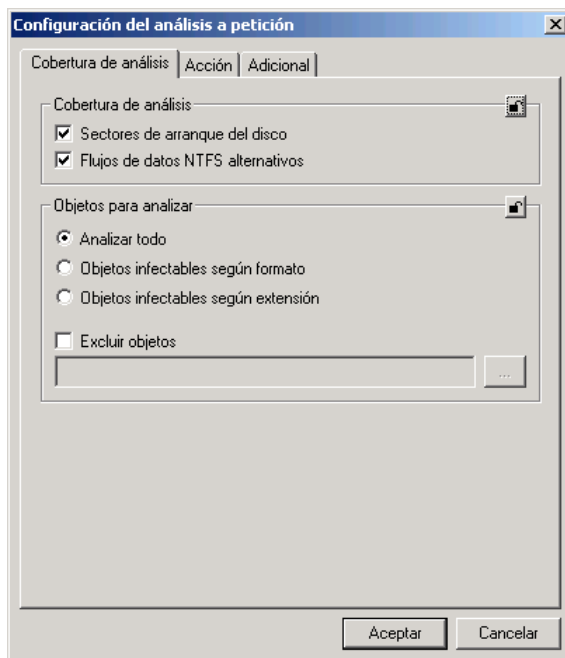


Figura 49. La ficha **Cobertura de análisis**

En la zona **Acciones** (ver Figura 50), seleccione alguna de las siguientes acciones, para aplicarlas a los objetos **infectados** o **sospechosos**, dependiendo del nivel de protección seleccionado (ver sección 5.3 pág. 56 para obtener detalles acerca de los tipos de acción realizados por la aplicación en el modo de análisis a petición).

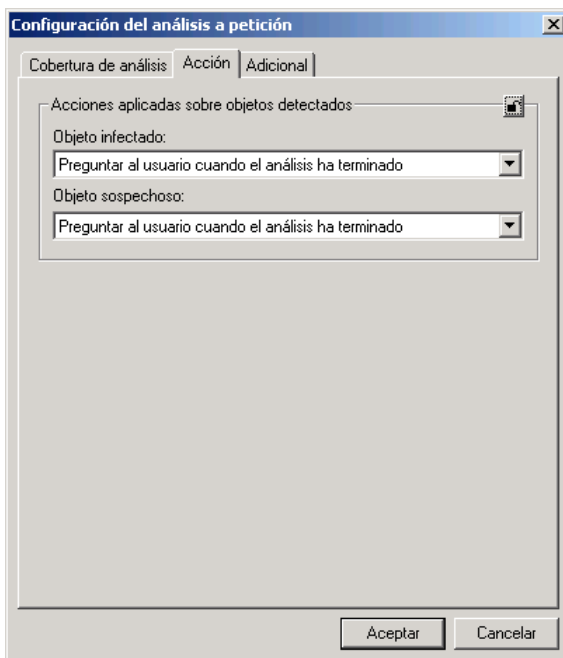
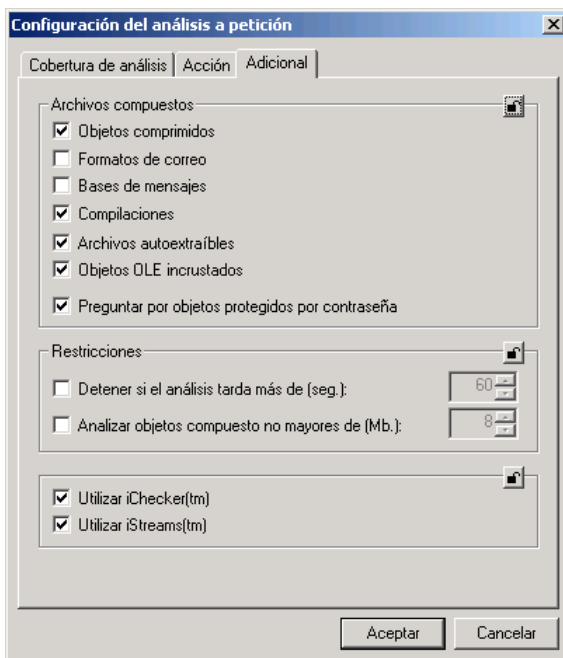


Figura 50. La ficha **Accion**

En la ficha **Adicional** (ver Figura 51) puede activar o desactivar el análisis de varios tipos de archivos compuestos y la pregunta de una contraseña de compilaciones cifradas, así como activar restricciones sobre el proceso de análisis (para más detalles, vea la sección 5.3 pág. 56).

Figura 51. La ficha **Adicional**

6.1.2.3. Protección constante del sistema de archivos

La ficha **Archivos** (ver Figura 52) permite personalizar la configuración de la directiva para la protección permanente de los objetos del sistema de archivos. Las opciones del nivel de protección y la ventana de configuración adicional son las mismas que para la ficha **Análisis a petición**.

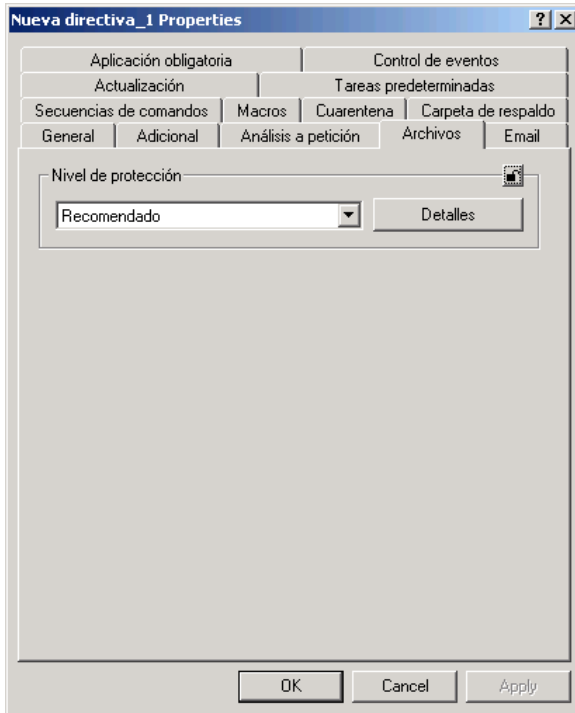


Figura 52. La ficha **Archivos**

Utilice la ficha **Cobertura de análisis** (ver Figura 53) para definir los objetos que serán analizados o excluidos del análisis en tiempo real. Esta configuración es idéntica a la configuración local descrita en la sección 5.2.1 pág. 43.

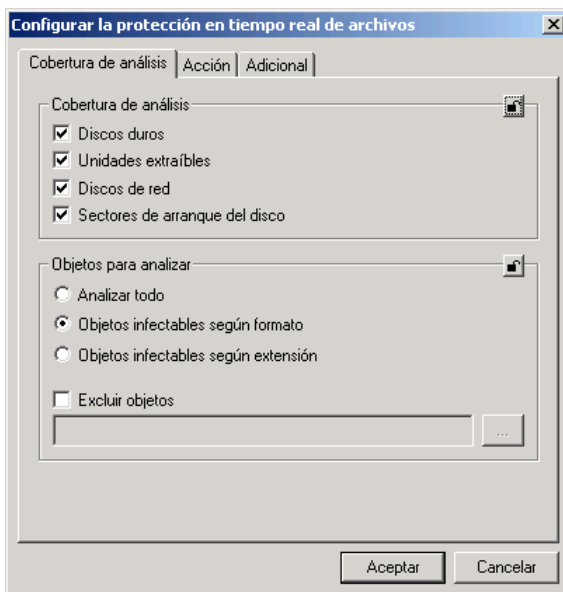


Figura 53. La ficha **Cobertura de análisis**

En la zona **Acción** (ver Figura 54), seleccione alguna acción aplicada a los objetos **infectados** o **sospechosos**, dependiendo del nivel de protección seleccionado (ver sección 5.2.1 pág. 43 para obtener detalles acerca de los tipos de acción realizados por la aplicación en el modo de análisis a petición).

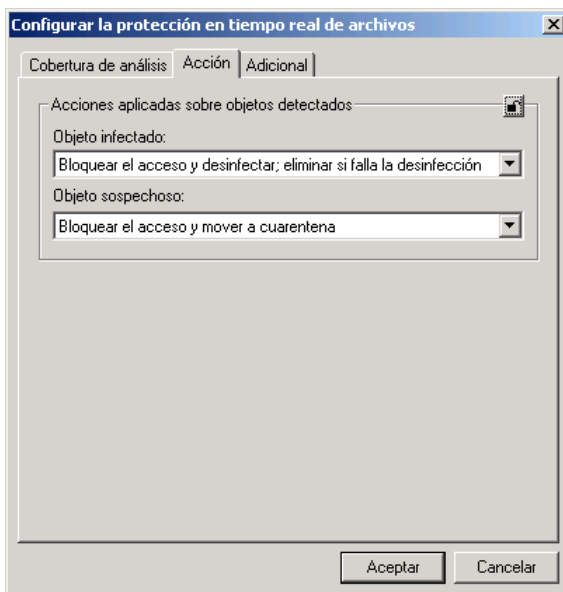
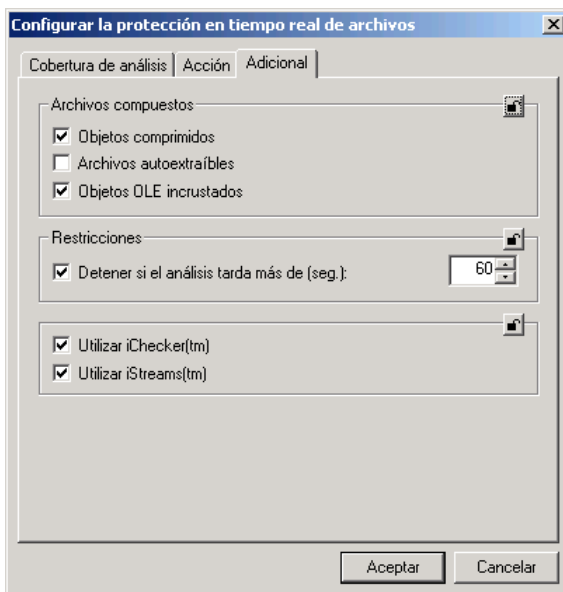


Figura 54. La ficha **Acción**

En la ficha **Adicional** (ver Figura 55), puede activar o desactivar el análisis de diferentes tipos de archivos complejos, así como limitar la duración del análisis, y activar o desactivar las tecnologías iChecker e iStreams (ver sección 5.2.1 en la página 43 para obtener detalles).

Figura 55. La ficha **Adicional**

6.1.2.4. Análisis del correo

En la ficha **E-mail** (ver Figura 56), puede configurar la directiva de análisis de mensajes entrantes y salientes.

Las opciones del nivel de protección y la ventana de configuración adicional son las mismas que para la ficha **Análisis a petición**.

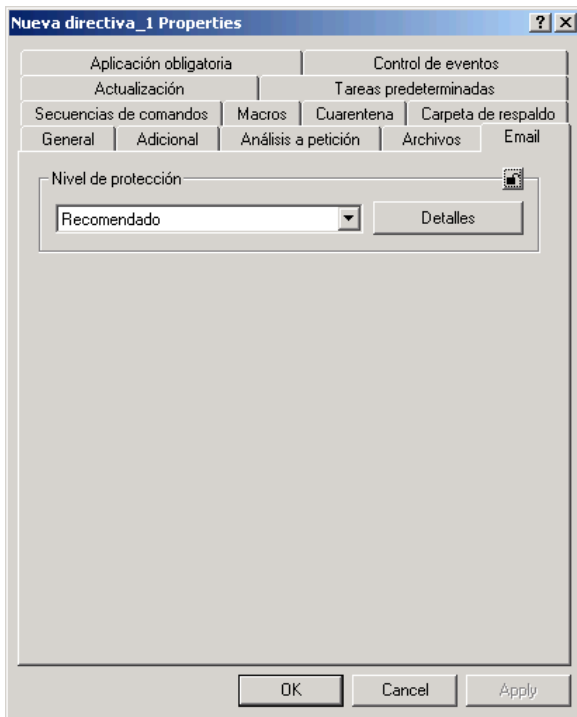


Figura 56. La ficha **Email**

En la sección **Cobertura de análisis** (ver Figura 57), seleccione los objetos analizados y especifique los tipos de mensajes excluidos. Esta configuración es idéntica a la configuración local. Encontrará información detallada acerca de esto en la sección 5.2.2 pág. 48.

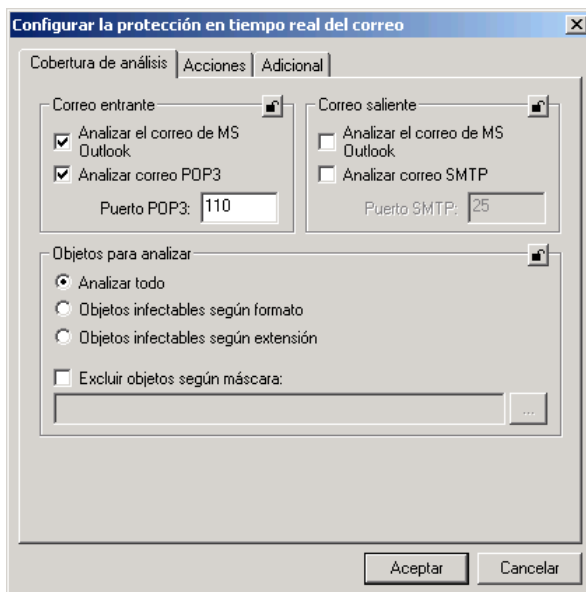


Figura 57. La ficha **Cobertura de análisis**

En la zona **Acción** (ver Figura 58), seleccione alguna de las siguientes acciones, para aplicarlas a los objetos **infectados** o **sospechosos**, dependiendo del nivel de protección seleccionado (ver sección 5.2.2 pág. 48 para obtener detalles acerca de los tipos de acción realizados por la aplicación en el modo de análisis del correo electrónico).

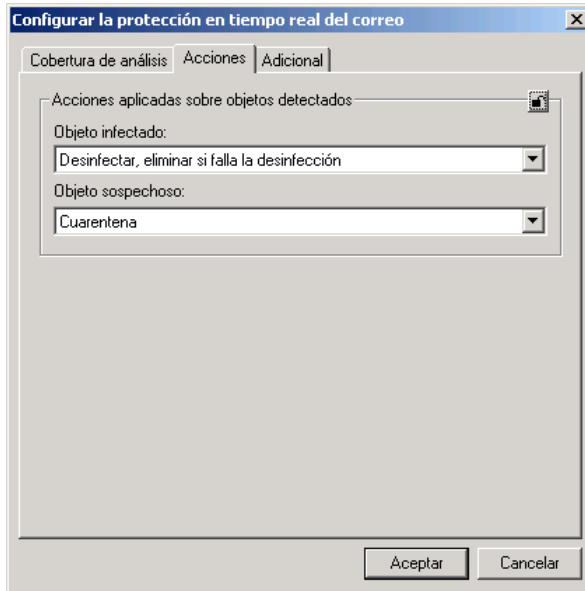
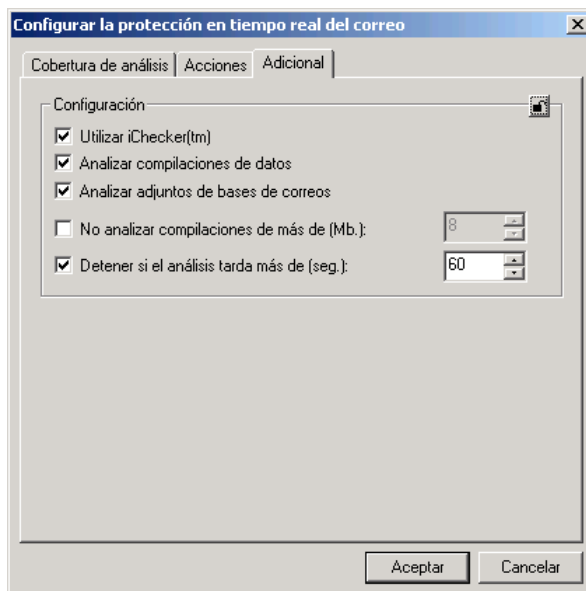


Figura 58. La ficha Acciones

En la ficha **Adicional** (ver Figura 59), puede activar o desactivar el uso de la tecnología iChecker™ y especificar algunas restricciones para el análisis de correo (ver sección 5.2.2 en la página 48 para obtener detalles).

Figura 59. La ficha **Adicional**

6.1.2.5. **Análisis de secuencias de comandos**

Puede configurar la directiva de análisis en tiempo real de las secuencias de comandos VBScript y JavaScript potencialmente peligrosas desde la ficha **Secuencias de comandos** (Figura 60).

Las opciones del nivel de protección y la ventana de configuración adicional son las mismas que para la ficha **Análisis a petición**.

En la ventana de configuración adicional, la acción *Bloquear la ejecución* está especificada para todos los niveles de protección. La elección de una acción diferente cambia el nivel a **Personalizado**.

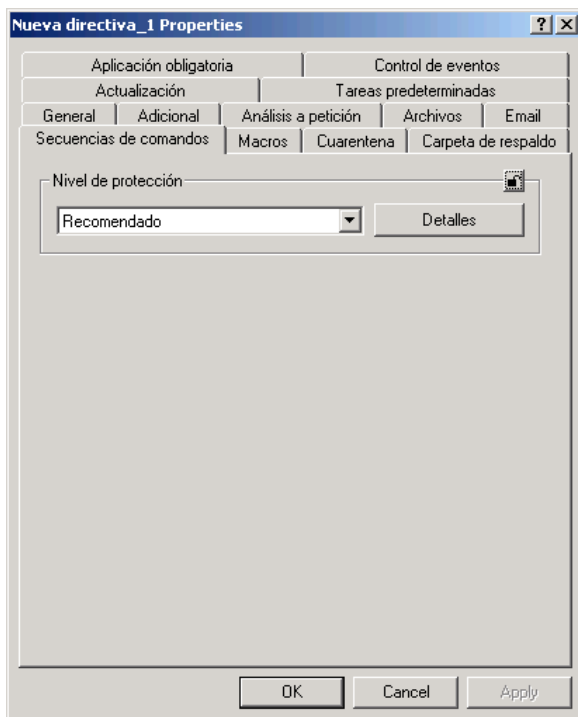
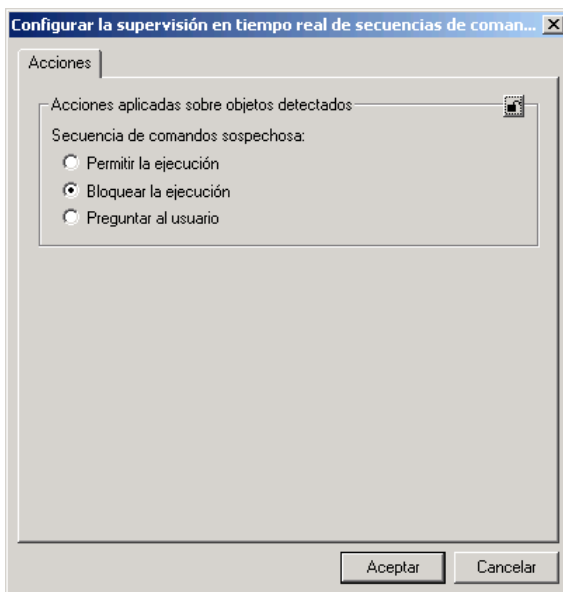


Figura 60. La ficha **Secuencias de comandos**

Figura 61. La ficha **Acciones**

6.1.2.6. Análisis de macros

La ficha **Macros** (ver Figura 62) permite modificar la configuración de directiva para el análisis de macros VBA empleadas por aplicaciones ofimáticas.

Las opciones del nivel de protección y la ventana de configuración adicional son las mismas que para la ficha **Análisis a petición**.

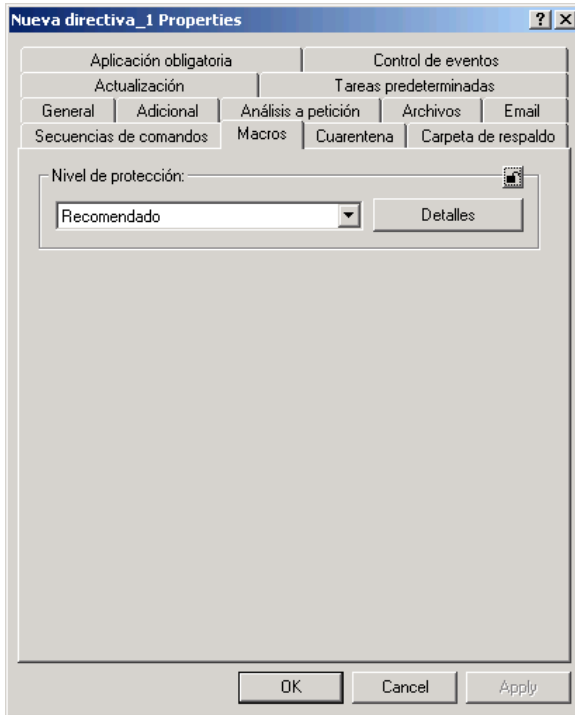


Figura 62. La ficha **Macros**

Haga clic en el vínculo **Detalles** para abrir un cuadro de diálogo (ver Figura 63) con la lista de los principales tipos de macros supervisados por Kaspersky Anti-Virus.

Existen cinco tipos de macros enumerados en las fichas correspondientes:

- **Módulos:** Macros que operan con módulos de proyectos:
 - Copiando módulos (OrganizerCopy);
 - Borrando módulos (OrganizerDelete);
 - Renombrando módulos (OrganizerRename);
 - Agregando módulo;
 - Eliminando módulo;
 - Importación de módulos;
 - Exportación de módulos.

- **Cadenas:** Macros que modifican el código de las macros:
 - Creando procedimiento;
 - Agregando cadenas de macro de un archivo al módulo;
 - Agregando cadenas a la macro;
 - Insertando cadenas a la macro;
 - Reemplazando cadenas en macro;
 - Eliminando cadenas de la macro.
- **Archivos:** operaciones con archivos:
 - Eliminando archivos;
 - Cambiando los atributos de archivo;
 - Creando carpetas;
 - Eliminando carpetas;
 - Abriendo archivo en escritura.
- **ActiveX:** operaciones con objetos ActiveX:
 - Creación de objetos ActiveX;
 - Creación de un objeto ActiveX en un equipo remoto;
 - Acceso a un objeto ActiveX.
- **Otras:** otras macros, incluyendo:
 - Desactivando el mensaje Guardar la plantilla normal;
 - Copiando hojas de Excel;
 - Desactivando la protección antivirus;
 - Ejecución del comando MacroCopy;
 - Ejecución de comandos del Shell;
 - Llamando a funciones del API;
 - Simulación de tecla.

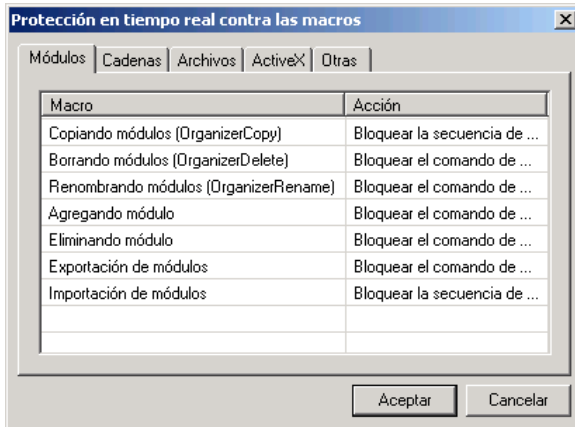


Figura 63. Lista de macros

En la columna **Acción** (ver Figura 63), se muestra la acción aplicada (de acuerdo con el nivel protección seleccionado) por el antivirus a la macro. Las acciones siguientes son posibles:

- *Habilitar los comandos de macro.*
- *Preguntar al usuario.*
- *Bloquear el comando de macro.*
- *Bloquear la secuencia de comandos:* pone fin a la ejecución del conjunto de macros.



Para modificar la acción aplicada por el antivirus a las macros sospechosas que detecta:

haga clic en la acción y seleccione otra acción desde la lista desplegable.

6.1.2.7. Actualización de bases antivirus y módulos de aplicación

En la ficha **Actualización** (ver Figura 64) puede personalizar la configuración de la actualización de la base antivirus y de los módulos de aplicación especificada durante la creación de una nueva directiva.

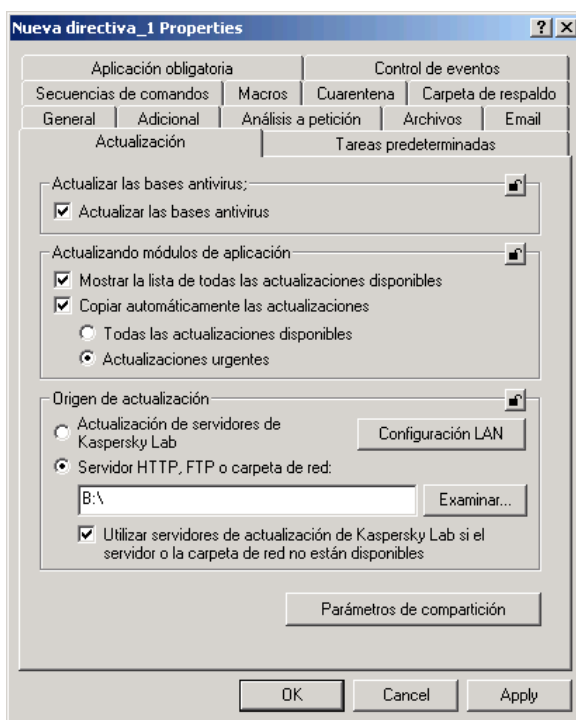


Figura 64. La ficha **Actualización**

La ficha **Actualización** tiene las secciones siguientes: **Actualización las bases antivirus** y **Actualización de módulos de aplicación**: se utiliza para la selección de parámetros para el servicio de actualización de las bases antivirus y de la aplicación (ver Paso 4. pág. 85). **Origen de actualización**: el punto de origen de las actualizaciones y su configuración(ver Etapa 3 en p. 84).

La ventana abierta desde **Copiar configuración** permite al usuario copiar las actualizaciones hacia una carpeta local y configurar los parámetros (ver sección 5.1.3 pág. 35).

6.1.2.8. Operaciones con tareas del sistema

En la ficha **Tareas predeterminadas** (ver figura 66) puede activar o desactivar el inicio de las tareas del sistema en estaciones remotas incluidas dentro del grupo de administración.

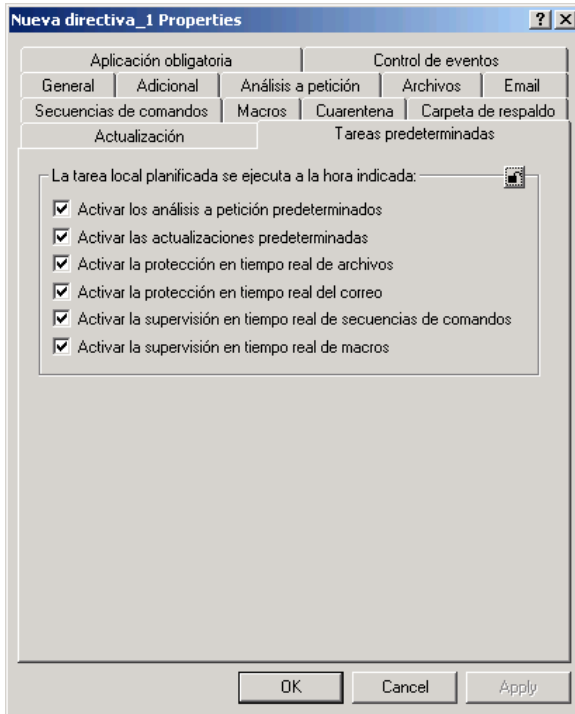
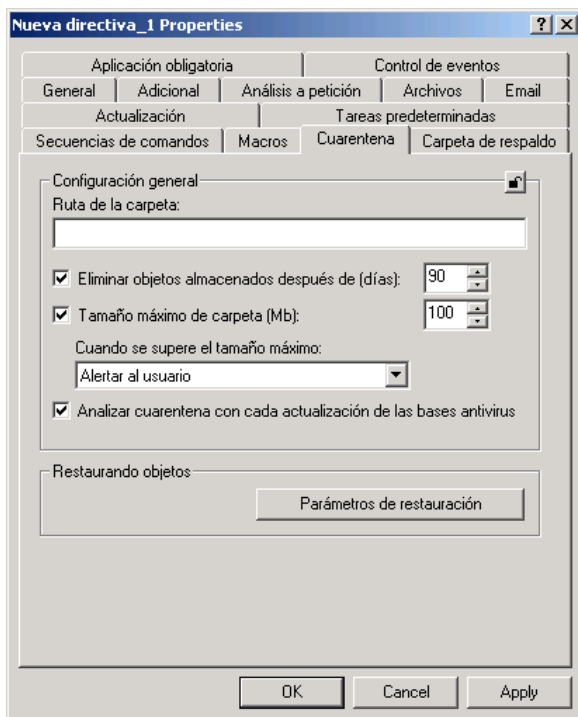


Figura 65. Tareas predeterminadas

6.1.2.9. Configuración de las zonas de Cuarentena y Respaldo

Las fichas **Cuarentena** (ver Figura 66) y **Carpeta de Respaldo** (ver Figura 67) se utilizan para especificar la configuración de directiva de la Cuarentena y la Zona de respaldo.

Estos parámetros son idénticos a los utilizados para controlar la Cuarentena y Respaldo desde una interfaz local (ver sección 5.5.1.1 pág. 72).

Figura 66. La ficha **Cuarentena**

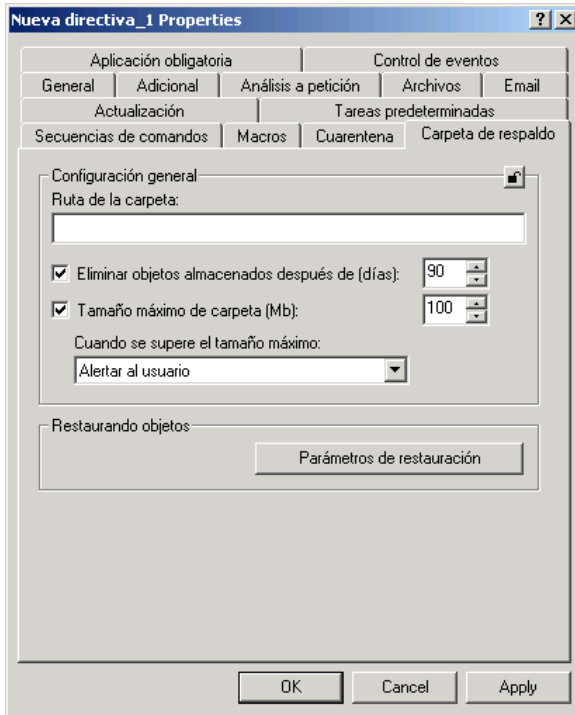


Figura 67. Ficha Carpeta de Respaldo

6.1.2.10. Generación de un informe de actividad de la aplicación

La ficha **Control de eventos** (ver Figura 68) muestra los tipos de eventos que se producen durante el funcionamiento de la aplicación y que son registrados en el informe, así como las ubicaciones del informe y las condiciones de notificación del administrador o de otros usuarios.

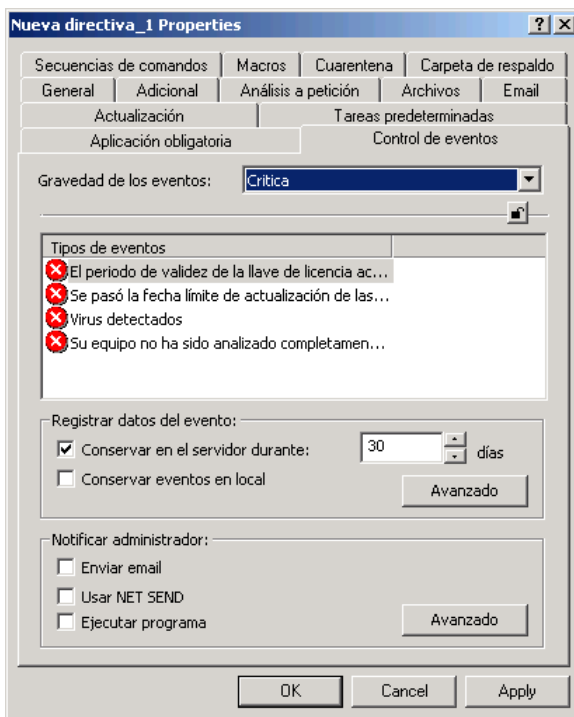


Figura 68. Modificación de una directiva, la ficha **Control de eventos**

Kaspersky Anti-Virus genera un conjunto de eventos que se producen durante el funcionamiento de la aplicación. Cada evento posee su propio indicador de prioridad. Existen cuatro estados de prioridad:

- **Suceso crítico ;**
- **Error;**
- **Advertencia;**
- **Mensaje de información.**

Es posible asignar eventos del mismo tipo a diferentes prioridades, en función de cada situación particular.

Seleccione la prioridad del evento en la lista desplegable **Prioridad de eventos**. En el campo de información inferior se muestran los tipos de eventos para el nivel de prioridad seleccionado.

Listas 2. Eventos

Evento	Prioridad
Ha recibido una actualización de noticias de Kaspersky Lab	Mensaje informativo
Objeto desinfectado	Atención.
Objeto infectado eliminado	Atención.
Nivel de protección en tiempo real modificado	Mensaje informativo
La licencia caducará en breve (dos semanas antes de la fecha límite)	Atención.
Su licencia ha caducado	Evento grave
La licencia no superó la comprobación	Error
Un objeto sospechoso ha sido detectado	Atención.
Error de operación	Atención. Error
Se pasó de la fecha límite de actualización de la base antivirus <ul style="list-style-type: none"> – hace menos de una semana – hace más de una semana 	Atención. Evento grave
Se han detectado virus	Evento grave
Error interno	Error
Su sistema operativo fue reiniciado después de la instalación de la aplicación	Atención.
Archivo protegido por contraseña detectado	Atención.

Evento	Prioridad
El objeto no pudo ser desinfectado	Atención.
Su equipo no ha sido analizado completamente desde hace mucho tiempo: <ul style="list-style-type: none"> – hace menos de una semana – hace más de una semana 	Atención. Evento grave

Puede especificar si desea incluir todos los eventos en el informe así como configurar las notificaciones al administrador en el momento de producirse el evento.

Para una descripción más detallada de la ficha **Control de eventos**, consulte el manual del administrador para "Kaspersky Administration Kit 5.0".

6.1.2.11. Parámetros avanzados

La ficha **Adicional** (ver Figura 69) muestra la configuración del servicio de Kaspersky Anti-Virus 5.0 for Windows Workstation. La mayoría de estos parámetros son los mismos que los avanzados descritos en la sección 5.5.3 pág. 81.

En la ventana que se abre con el botón **Advertencia** (ver Figura 70), puede establecer las condiciones de varias notificaciones:

- Informar al usuario de la presencia de virus:** activa la presentación de mensajes de información al usuario de la detección de un virus.
- Mostrar mensajes emergentes:** desactiva la presentación de mensajes de Kaspersky Anti-Virus.
- Mostrar el icono de la aplicación en la barra del sistema:** desactiva la animación del icono Kaspersky Anti-Virus en el panel del sistema durante el análisis antivirus.

La sección **Advertencia** permite configurar la recepción de avisos sobre el estado de actualización de la base antivirus y el análisis completo del equipo. Existen dos niveles para todas estas tareas: **advertencia** y **evento grave**.

Para cada evento, el campo asociado permite establecer el límite de días pasado el cual el usuario recibirá notificaciones diarias cada vez que se inicie Kaspersky Anti-Virus. Este periodo de tiempo se inicia en la fecha de última ejecución de la tarea correspondiente.

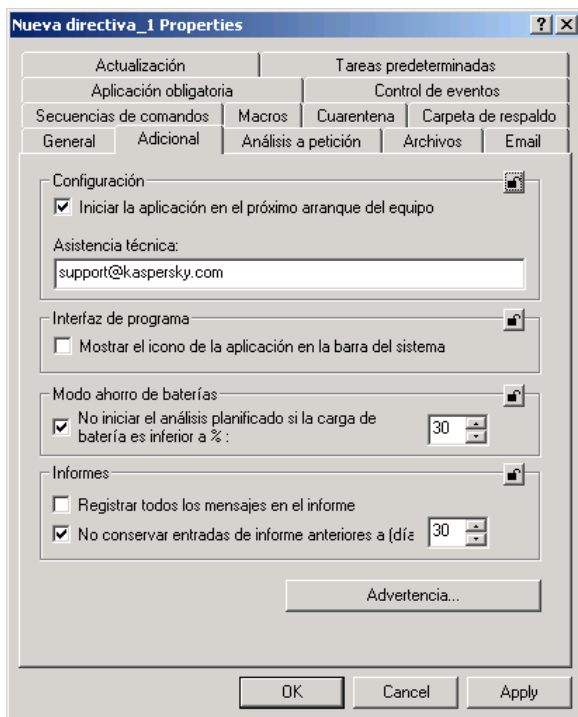


Figura 69. Ficha Adicional

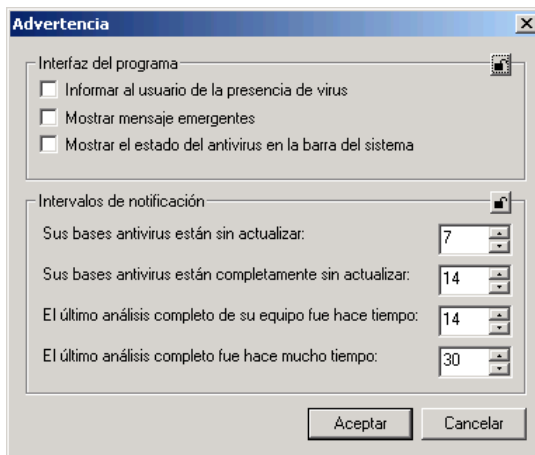


Figura 70. Ficha Advertencia

6.1.2.12. Examen de los resultados del control de directiva

La ficha **Aplicación obligatoria** (ver Figura 71) muestra la información siguiente acerca de la directiva aplicada a los equipos de este grupo:

- El número de equipos a los que se asignó la directiva;
- El número de equipos a los que se aplicó la directiva;
- El número de equipos en los que la directiva está pendiente;
- El número de equipos en los que la directiva falló.

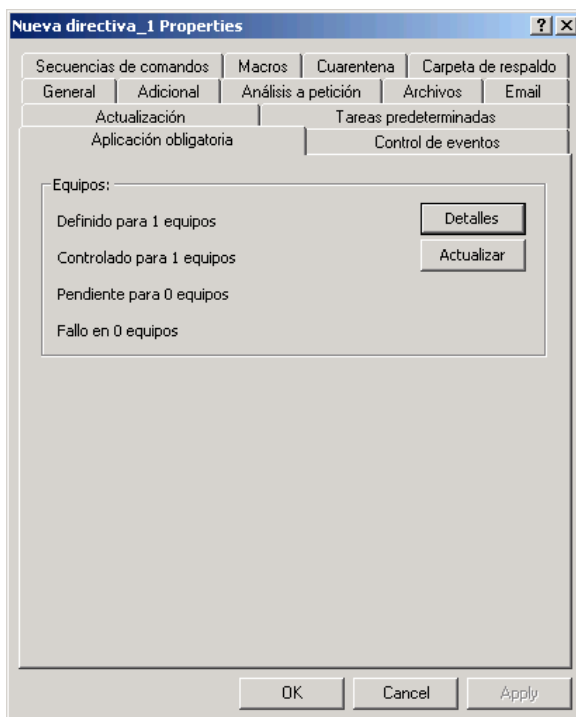


Figura 71. La ficha **Aplicación obligatoria**

Haga clic en **Detalles** para abrir un cuadro de diálogo con detalles acerca de la directiva seleccionada, aplicada a cada equipo cliente. (Para obtener detalles, consulte el manual del administrador de "Kaspersky Administration Kit 5.0".)

6.2. Administración de tareas

Esta sección describe la creación y administración de tareas para Kaspersky Anti-Virus. Encontrará información detallada acerca de la administración de tareas en el manual del administrador de "Kaspersky Administration Kit 5.0".

6.2.1. Creación de tarea

Durante la instalación, se genera una lista de tareas de sistema para cada equipo. La lista (ver Figura 72) incluye tanto las tareas de protección en tiempo real (protección del sistema de archivos, protección del correo, análisis de macros y secuencias de comandos), de análisis a petición (análisis de Mi PC, análisis automático al iniciar la aplicación y análisis de la cuarentena) y de actualización (actualizaciones de bases antivirus, de módulos de aplicación, función de anulación de las actualizaciones de las bases antivirus).

Las tareas de protección en tiempo real son individualizadas y se ejecutan en segundo plano. Se suministra un calendario para las tareas de análisis a petición y de actualización de las bases antivirus.



Puede iniciar las tareas de sistema así como modificar sus parámetros y planificación; no es posible eliminar dichas tareas.

Con Kaspersky Administration Kit, puede crear las tareas siguientes para Kaspersky Anti-Virus:

- Tareas locales asignadas a cada equipo cliente;
- Tareas de grupo asignadas a los grupos de equipos clientes;
- Tareas globales asignadas a un conjunto de equipos clientes tomados de cualquier grupo de una red lógica.

Puede modificar los parámetros de tareas, controlar su ejecución, copiar y eliminar tareas de un grupo a otro, y eliminarlas con el menú contextual (**Copiar/Pegar**, **Cortar/Pegar** y **Eliminar**), o con los mismos comandos del menú **Acción**.

Los parámetros utilizados por un equipo cliente durante la ejecución de las tareas se ajustan a los parámetros de la directiva de grupo, los parámetros específicos de la tarea y los de la aplicación en este equipo cliente.

Todas las tareas son planificadas de modo predeterminado. Es posible deshabilitar temporalmente tareas dentro de la lista de tareas planificadas. En este caso, las tareas permanecen en la lista, pero no son iniciadas.

Puede realizar manualmente operaciones como iniciar, interrumpir, detener o continuar una tarea con los comandos **Inicio/Detener/Pausa/Continuar** del menú contextual o del menú **Acción**.

6.2.1.1. Creación de una tarea local



Para crear una tarea local, proceda de la forma siguiente:

1. En la carpeta **Grupos**, seleccione una carpeta con el nombre del grupo que contiene al equipo cliente requerido.
2. En el panel de resultados seleccione el equipo destinatario de la nueva tarea local, y haga clic en **Propiedades** en el menú contextual o en el menú **Acción**. Se abre el cuadro de diálogo **Propiedades [nombre del equipo]** con las propiedades del equipo cliente (ver Figura 72).
3. Abra la ficha **Tareas** (ver Figura 72). Se muestra una lista completa de tareas planificadas para el equipo cliente.
Para crear una nueva tarea local, haga clic en **Agregar**. Haga clic en **Propiedades** para modificar la configuración de la tarea y en **Eliminar** para eliminar la tarea seleccionada.

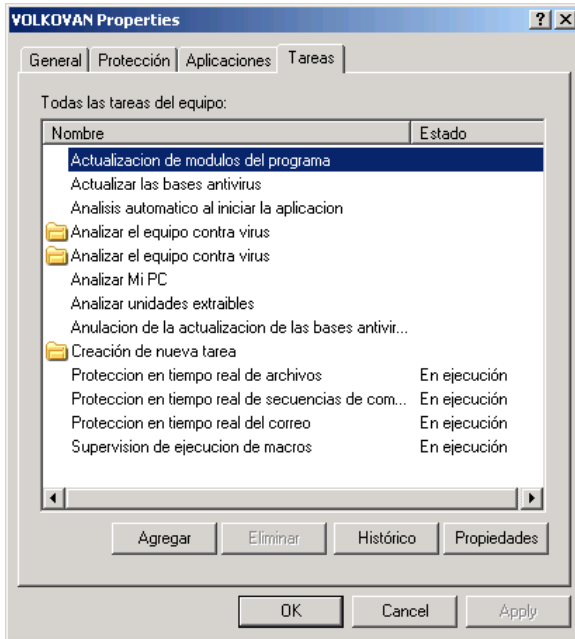


Figura 72. Creación de una tarea local
La ficha **Tareas**

Haga clic en **Agregar** para crear una nueva tarea. La interfaz de la aplicación para la creación de una nueva tarea se organiza como un asistente Windows, que le guía a través de todo el proceso. Para cambiar entre los cuadros de diálogo del asistente, haga clic en **Anterior** y **Siguiente**. Para terminar el trabajo con el asistente, haga clic en **Terminar**. Para terminar el trabajo con el asistente en cualquier etapa, haga clic en **Cancelar**.

Paso 1. Información general de la nueva tarea

El primer cuadro de diálogo del asistente es introductorio: debe escribir el nombre de la tarea en el campo **Nombre**.

Paso 2. Seleccione la aplicación y el tipo de tarea

Seleccione la aplicación **Kaspersky Anti-Virus 5.0 for Windows Workstations** en la lista desplegable **Elija la aplicación para la que define una tarea**. A continuación elija el tipo de tarea en la lista **Elija el tipo de tarea a ejecutar**. Puede crear las tareas siguientes para Kaspersky Anti-Virus for Windows Workstations:

- **Actualización de la base antivirus y los módulos de aplicación:** actualizar las bases antivirus y los componentes de la aplicación.
- **Anulación de la actualización de la base antivirus:** anular las actualizaciones de la base antivirus;
- **Análisis a petición:** analizar objetos a petición;
- **Instalación de llave de licencia:** instalar llaves de licencia;

Paso 3. Configuración de los parámetros de tarea

Dependiendo del tipo de tarea seleccionada, se le ofrecen varias opciones para la configuración de la tarea:

CONFIGURACIÓN DE LA TAREA DE ACTUALIZACIÓN

La configuración de la tarea de actualización de las bases antivirus y de los módulos de aplicación es similar a la que procede para crear una nueva directiva (ver Paso 3. –Paso 4. páginas 84–85). Además, durante la creación de la tarea, puede definir, por ejemplo, los parámetros para compartir actualizaciones recibidas (ver sección 6.1.2.7 pág. 105).

ANULACIÓN DE LAS ACTUALIZACIONES

La tarea de anulación de las actualizaciones de la base antivirus no requiere configuración específica. Después de seleccionar esta tarea, el asistente le mostrará el cuadro de diálogo **Parámetros de planificación de tarea** (ver Paso 4. en la página 118).

CONFIGURACIÓN DE LA TAREA DE ANÁLISIS A PETICIÓN

Seleccione el nivel de protección antivirus de la tarea de análisis a petición. (Vea la sección 4.2 pág. 31)

Haga clic en **Detalles** para abrir una ventana donde revisar la configuración correspondiente al nivel seleccionado, o para utilizarla como modelo de su propia configuración. Esto cambiará el nivel de nivel de protección a **Personalizado**.

En el siguiente cuadro de diálogo (ver Figura 73), especifique los objetos que debe analizar con **Agregar**, **Modificar** y **Eliminar**.

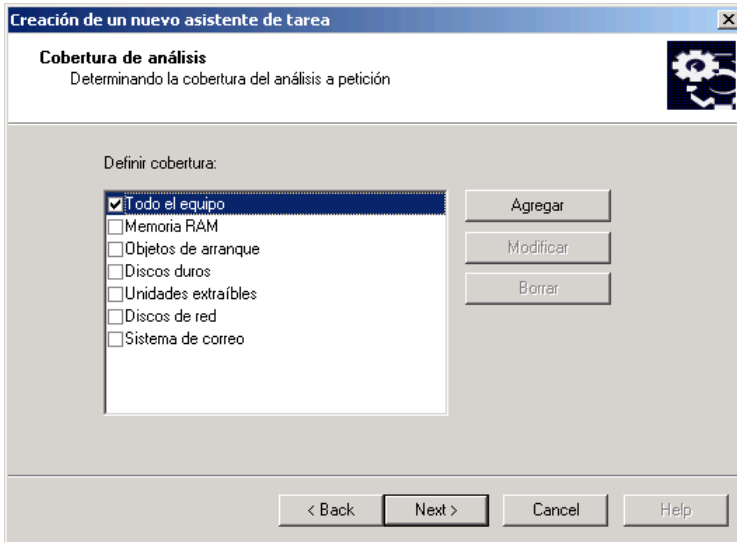


Figura 73. Objetos que se analizarán

TAREA DE INSTALACIÓN DE LLAVE DE LICENCIA

Haga clic en **Examinar** para encontrar la ruta del archivo llave. Para que la nueva llave se convierta en la llave actual, active la casilla **Usar como llave de licencia actual**.

No active esta casilla si la llave se incluye como llave de reserva. Una llave de licencia adicional se convierte en llave actual cuando ésta llega a término.

Paso 4. Planificación de las tareas

Tras configurar el tipo de tarea seleccionado, el asistente abrirá el cuadro de diálogo de **planificación de tarea** (ver Figura 74), que permite planificar la tarea.

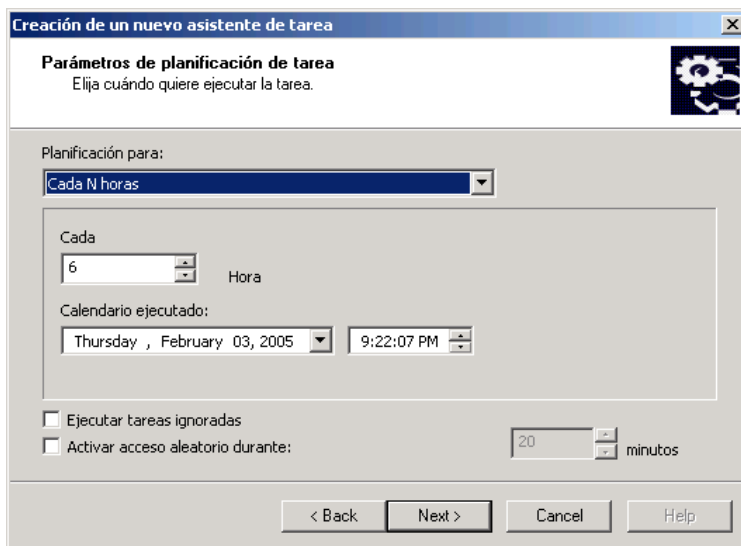


Figura 74. Planificación de una nueva tarea

Seleccione la periodicidad deseada para la tarea en la lista **Agenda de tarea**. Las opciones siguientes estarán disponibles: *Cada N horas*, *cada N días*, *cada N semanas*, *Manualmente*, y *Al iniciar la aplicación*. En función de la selección, los elementos del diálogo cambian:



Las tareas que permiten deshacer actualizaciones e instalar llaves de licencia sólo pueden iniciarse de forma manual.

Puede obtener más detalles acerca de la configuración del inicio de tareas planificadas en el Manual del administrador de Kaspersky Administration Kit.

Paso 5. Fin de creación de la tarea

La última ventana del asistente le informa de que la tarea ha sido creada con éxito.

6.2.1.2. Creación de una tarea de grupo



Para crear una tarea de grupo para Kaspersky Anti-Virus, proceda de la forma siguiente:

1. En el explorador de consola, seleccione un grupo de equipos a los que aplicar la nueva tarea.

2. Seleccione la carpeta **Tareas** dentro del grupo y seleccione **Nuevo/Tarea** en el menú contextual. También puede seleccionar este comando desde el menú **Acción**. Se abre un asistente para la creación de una nueva tarea de grupo, que le guiará a través de todo el proceso de creación. El asistente es parecido al asistente de tareas locales (ver sección 6.2.1.1 en la página 115).

Después de crear la tarea, ésta se agrega a la carpeta **Tareas** del grupo seleccionado y de todos los grupos anidados y se muestra dentro del panel de resultados.

6.2.1.3. Creación de una tarea global



Para crear una tarea global para Kaspersky Anti-Virus, proceda de la forma siguiente:

1. En el explorador de consola, seleccione la entrada **Tareas**, abra el menú contextual y seleccione **Nuevo/Tarea**. También puede seleccionar este comando desde el menú **Acción**.
2. Se abre un asistente para la creación de una nueva tarea global, que le guiará a través de todo el proceso de creación. El asistente es parecido al asistente de tareas locales (ver sección 6.2.1.1 en la página 115 acerca del asistente de tarea local). La única diferencia es que debe además definir la lista de los equipos clientes, dentro de la red lógica, a los que se aplicará la tarea global.
3. Seleccione los equipos dentro de la red lógica a los que desea asignar la nueva tarea. Puede seleccionar equipos en carpetas diferentes o seleccionar la carpeta completa (para obtener más detalles, consulte el manual del administrador de Kaspersky Administration Kit 5.0).



Las tareas globales se aplican tan sólo a un conjunto específico de equipos. Por ejemplo, una tarea de instalación remota asignada a un grupo no se ejecutará en los nuevos equipos que se incluyan en este grupo. Debe crear una nueva tarea o introducir los cambios necesarios a la tarea existente.

Después de crear la tarea, ésta se agrega bajo la entrada **Tareas** del explorador de consola y se muestra dentro del panel de resultados.

6.2.2. Examen y modificación de la configuración de la tarea y supervisión del rendimiento de tarea



Para ver y modificar la configuración de la tarea;

- Para una tarea local, en la carpeta **Grupos**, seleccione una carpeta con el nombre del grupo que contiene al equipo cliente. En el panel de resultados seleccione el equipo y haga clic en **Propiedades** en el menú contextual. Se abre el cuadro de diálogo **Propiedades [nombre del equipo]** de Windows. En el cuadro de diálogo, cambie a la ficha **Tareas** (ver Figura 72). Puede examinar y modificar la configuración de la tarea en la ventana, que se abre cuando hace clic en **Propiedades**.



La ficha **Tareas** muestra una lista completa de tareas asignadas a este equipo local, e incluye tanto las tareas globales como las de grupo. Las tareas globales y de grupo son señaladas por un icono de "carpeta". Nota: puede examinar la configuración de todas las tareas, pero sólo podrá modificar la de las tareas locales.

- Para una tarea de grupo, seleccione el grupo en el explorador de consola y elija la entrada **Tareas** dentro de aquél. El panel de resultados mostrará todas las tareas asignadas a este grupo. Seleccione la tarea deseada y haga clic en **Propiedades** en el menú contextual o en el menú **Acción**.
- Para modificar la configuración de una tarea global, seleccione la entrada **Tareas** en el explorador de consola, seleccione la tarea deseada y haga clic en **Propiedades** en el menú contextual o en el menú **Acción**.

Se abre el cuadro de diálogo **Propiedades: Nombre de tarea** de Windows, con las fichas siguientes: **General**, **Configuración**, **Planificar** y **Advertencia**. El cuadro de diálogo de configuración de la tarea global contiene una ficha **Equipos destino** adicional.

Todas las fichas (con la excepción de la ficha **Configuración**) son fichas estándar de Kaspersky Administration Kit 5.0. Encontrará más información acerca de estas fichas en el Manual del administrador de Kaspersky Administration Kit. La ficha **Configuración** muestra parámetros específicos de Kaspersky Anti-Virus, que dependen del tipo de tarea seleccionada (ver Paso 3. en la página 117).

6.2.3. Inicio y detención de tareas



Tan sólo es posible iniciar tareas en un equipo si la aplicación correspondiente está en ejecución. Si se termina la aplicación, las tareas en ejecución también se interrumpen.

Es posible iniciar y detener todas las tareas tanto de forma automática (de acuerdo con la planificación), como manual, desde las opciones del menú contextual o desde la ventana de configuración de la tarea. También puede pausar una tarea en ejecución y volver a continuarla.



Para iniciar / detener / suspender / continuar manualmente una tarea,

seleccione la tarea deseada, abra el menú contextual y seleccione **Iniciar / Detener/ Suspender/ Continuar** en el menú contextual o en el menú **Acción**.

Otros comandos similares están disponibles desde la ventana de configuración de la tarea en la ficha **General** (ver sección 6.2.2 en la página 121).

6.3. Configuración de los parámetros de la aplicación

Puede modificar parámetros de la aplicación dentro de los equipos clientes que pertenecen al grupo. Puede volver a definir los parámetros definidos como modificables por la directiva de esta aplicación.



Para modificar la configuración de la aplicación:

1. En la carpeta **Grupos**, seleccione una carpeta con el nombre del grupo que contiene al equipo cliente.
2. En el panel de resultados seleccione el equipo en el que va a modificar la configuración de la aplicación, y haga clic en **Propiedades** en el menú contextual o en el menú **Acción**.
3. Tras esto, el cuadro de diálogo estándar **Propiedades <nombre del equipo>** con cuatro fichas, se abre en la ventana principal del programa. Seleccione la ficha **Aplicaciones** (ver Figura 75) con la lista completa de las aplicaciones de Kaspersky Lab instaladas en el equipo cliente.

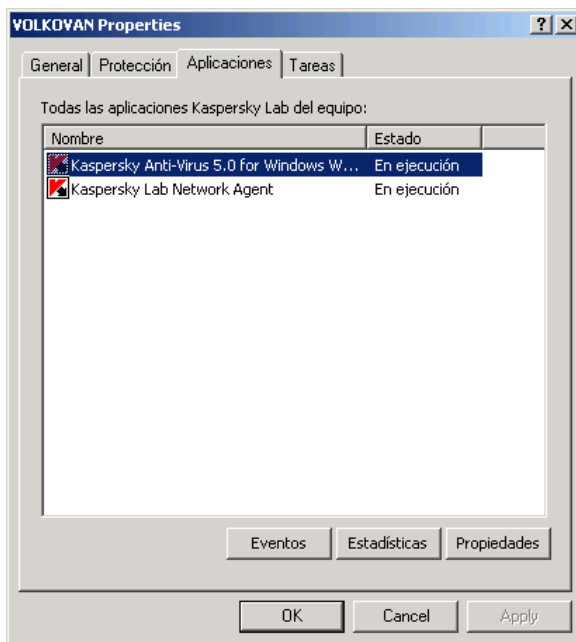


Figura 75. Cuadro de diálogo Propiedades del equipo cliente
Ficha **Aplicaciones**

4. Seleccione **Kaspersky Anti-Virus 5.0 for Windows Workstations**. Bajo la lista, los botones **Eventos**, **Estadísticas** y **Propiedades** permiten:
 - Mostrar una lista de eventos ocurridos en el equipo y registrados en el servidor de administración (para detalles sobre el informe, consulte el manual del administrador de "Kaspersky Administration Kit 5.0").
 - Mostrar estadísticas recientes del rendimiento de la aplicación.
 - Tener acceso a los parámetros de la aplicación. Haga clic en el botón para abrir una ventana con las fichas siguientes: **General**, **Adicional**, **Cuarentena**, **Carpeta de Respaldo**, **Objetos almacenados**, **Licencias** y **Control de eventos**. El detalle de estas ficha se describe a continuación.

6.3.1. Información de la aplicación

En la ficha **General** (ver Figura 76) dispone de información general acerca de la aplicación (Kaspersky Anti-Virus 5.0 for Windows Workstations); cómo iniciar o detener su funcionamiento.

La parte superior de la ventana muestra el título de la aplicación, su versión, la fecha de instalación, su estado (si la aplicación está en ejecución o detenida en un equipo local) así como información acerca del estado de las bases antivirus.

Puede iniciar y detener la aplicación con los botones apropiados.

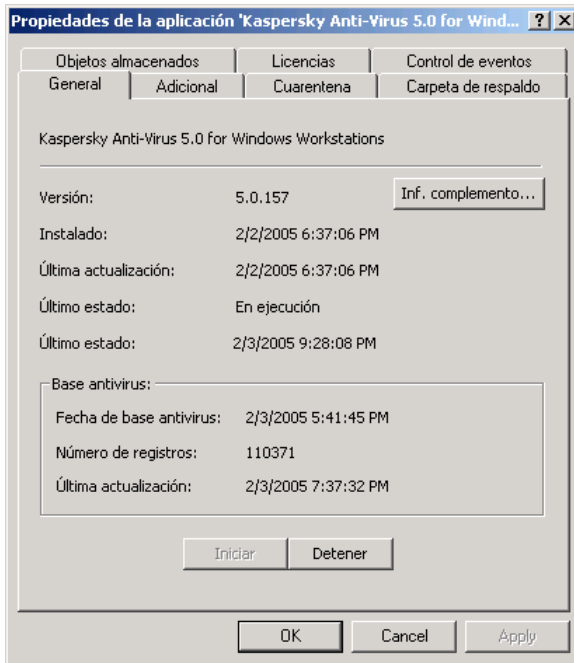


Figura 76. Ventana de configuración de la aplicación, la ficha **General**

6.3.2. Configuración adicional de la aplicación

Las fichas **Adicional**, **Cuarentena** y **Respaldo** permiten configurar Kaspersky Anti-Virus en estaciones de trabajo remotas.

Estas configuraciones son duplicados de la directiva de grupo correspondiente (ver detalles en la sección 6.1.2 pág. 86). La directiva sigue siendo prioritaria para la configuración de la aplicación.



Quando configura la aplicación en un equipo local, sólo puede modificar los parámetros permitidos por la directiva de grupo.

6.3.3. Trabajar con la zonas de cuarentena y respaldo

Kaspersky Anti-Virus almacena objetos sospechosos y copias de respaldo en almacenes especializados.

Cada equipo dispone de sus propios directorios de cuarentena y respaldo.

Puede examinar los objetos en las zonas de cuarentena y respaldo de un equipo desde la ficha **Objetos almacenados** (ver Figura 77).

Para ello, haga clic en la **Lista de objetos** en las secciones **Cuarentena** y **Carpeta de Respaldo** (respectivamente).



Si la aplicación no puede establecer una conexión con el equipo cliente, un cuadro de diálogo permite elegir entre reintentar o cancelar la conexión.

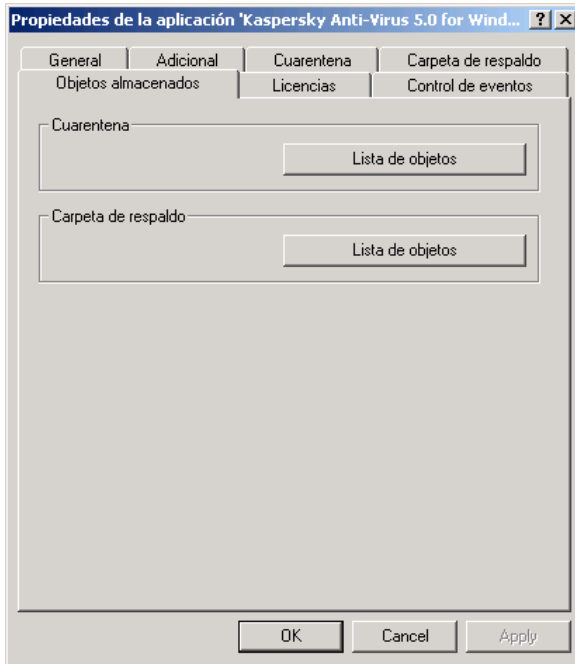







Figura 77. La ficha **Objetos almacenados**

Los cuadros de diálogo con el contenido de ambas zonas son similares (ver Figura 78). En la parte central del cuadro de diálogo, puede ver una lista de archivos en cuarentena o de respaldo. La información siguiente está disponible, para cada objeto: nombre, estado, fecha de inclusión en cuarentena y ruta de origen.

Encima de la lista, una barra de tareas permite administrar objetos en cuarentena o de respaldo. Utilice los botones para:

-  – Restaurar un objeto. Haga clic en este icono para restaurar el objeto seleccionado, y especifique la ubicación de destino.
-  Dentro del control remoto con Kaspersky Administration Kit, los objetos podrán ser restaurados tan sólo en un equipo donde esté instalada la *consola de administración*.
-  – Eliminar el objeto de la carpeta de almacenamiento.
-  – Actualizar el contenido del almacén.
-  – Analizar los objetos de nuevo (sólo para cuarentena).

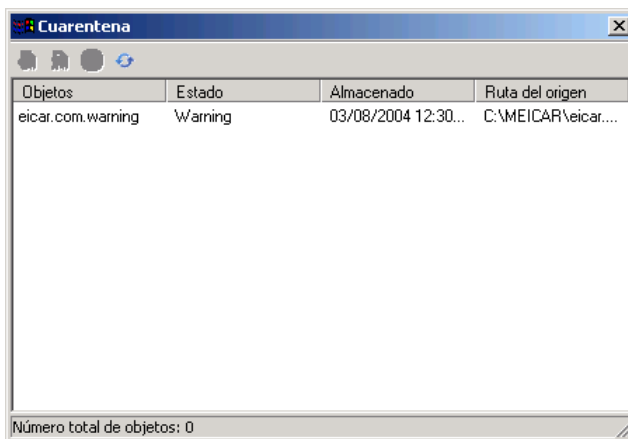


Figura 78. Almacenamiento en cuarentena

6.3.4. *Mostrar información de llaves de licencia*

La ficha **Licencias** (ver Figura 79) es sólo informativa. Muestra información acerca de las llaves de licencia actuales y de reserva que estén instaladas en un equipo específico.

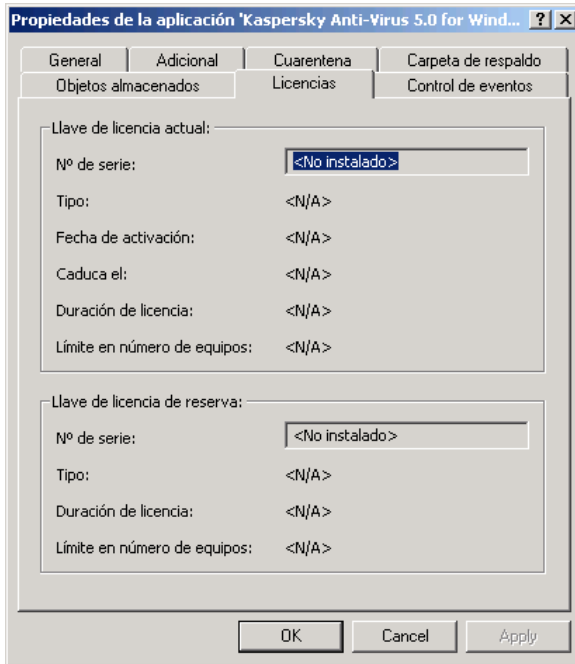


Figura 79. Ficha Licencias

6.3.5. *Parámetros de generación de informes*


La ficha **Control de eventos** da acceso a la configuración del servicio de mensajería, que envía notificaciones acerca del funcionamiento del antivirus desde un equipo remoto.

Esta ficha reproduce la configuración de la ficha correspondiente a la directiva de grupo.

CAPÍTULO 7. PRUEBAS DE FUNCIONAMIENTO DE KASPERSKY ANTI-VIRUS

7.1. Prueba con el "virus" EICAR y sus modificaciones

Tras completar la instalación y hacer ajustes en Kaspersky Anti-Virus, le recomendamos probar la configuración y funcionamiento de la aplicación con un "virus" de prueba o con modificaciones de éste.

El virus ha sido especialmente diseñado por el organismo  (European Institute for Computer Antivirus Research) con el fin de realizar pruebas con productos antivirus.

El "virus" NO ES EN REALIDAD NINGUN VIRUS porque no contiene código que pueda dañar su equipo. Sin embargo, la mayoría de los productos antivirus lo identifican como un virus.



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

Puede descargar el "virus" de prueba desde el sitio oficial del **EICAR** en la dirección: http://www.eicar.org/anti_virus_test_file.htm. Si no dispone de acceso a Internet, puede crear un "virus" de prueba manualmente. Para crear un "virus" de prueba, escriba la cadena siguiente en cualquier editor de texto plano y guarde el archivo con el nombre **EICAR.COM**:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

El archivo descargado desde el sitio de **EICAR** o creado en un editor como explicado, contiene el cuerpo de un "virus" de prueba estándar. La aplicación antivirus lo detectará, lo identificará con el tipo **Infectado** y aplicará la acción definida por el administrador para objetos pertenecientes a dicho tipo.

Para comprobar la respuesta de la aplicación antivirus con objetos de otros tipos, puede modificar el contenido del "virus" de prueba y agregar uno de los prefijos siguientes (ver tabla a continuación).



Puede comprobar el funcionamiento correcto de Kaspersky Anti-Virus sobre el "virus" modificado EICAR tan sólo si la última actualización de su base antivirus es posterior al 24 de octubre de 2004, o si cuenta con actualizaciones acumuladas hasta el 24 de octubre 2003.

Listas 3. Prueba de las modificaciones del "virus"

Prefijo	Tipo de objeto
Sin prefijo, "virus" de prueba estándar	Infectado: Se produce un error de desinfección del objeto; el objeto se elimina.
CORR-	Dañado
SUSP-	Sospechoso (código vírico desconocido)
WARN-	Advertencia (mutación de código de un virus conocido).
ERRO-	Error durante el análisis del objeto
CURE-	Infectado: el objeto es desinfectado; el texto en el cuerpo del "virus" cambia a CURE
DELE-	Infectado: El objeto es eliminado automáticamente

La primera columna de la tabla contiene los prefijos que deben incluirse al principio de línea, dentro del archivo del "virus" de prueba (por ejemplo: DELE-X5O!P%@AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*).

Después de incluir el prefijo al "virus" de prueba, guárdelo por ejemplo con el nombre eicar_dele.com; utilice nombres similares para todas las versiones modificadas del "virus".

La segunda columna contiene los tipos de objetos identificados por la aplicación antivirus, de acuerdo con el prefijo incluido. Las acciones para cada tipo de objetos se definen en la configuración de la aplicación, personalizada por el administrador.

7.2. Pruebas de funcionamiento correcto de Kaspersky Anti-Virus



Para probar la configuración y la capacidad de reacción de Kaspersky Anti-Virus 5.0 for Windows Workstation,

- Cree un directorio y guarde en disco el "virus" de prueba que acaba de crear.
- Cree y configure una tarea personalizada (ver sección 5.4 pág. 65):
 - agregue la carpeta con los virus de prueba a la lista de objetos analizados por la tarea cuando ésta se ejecuta;
 - seleccione el comando *Preguntar al usuario durante el análisis* como acción aplicada por la aplicación cuando detecta objetos infectados o sospechosos.
- En el cuadro de diálogo **Configuración adicional** (ver sección 5.5.3 pág. 81) active la casilla **Registrar todos los mensajes en el informe** para registrar información de los objetos que no pueden ser comprobados debido a un error.
- Ejecute la tarea.

Durante el análisis, en cuanto se descubren objetos sospechosos o infectados, la aplicación muestra un cuadro de diálogo con información acerca de todos los objetos y pide al usuario que seleccione una acción apropiada. Por ejemplo, en presencia de un objeto con el prefijo SUSP-, se mostrará el mensaje siguiente:

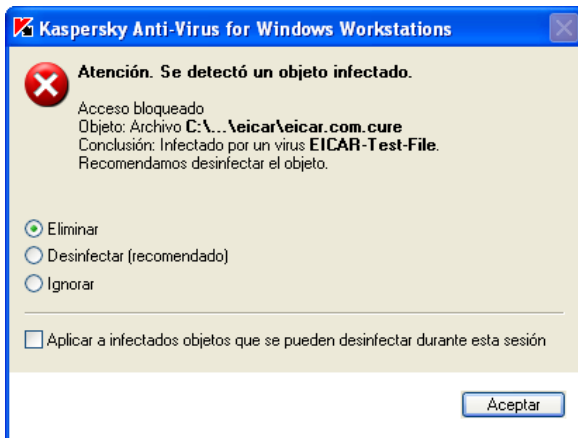


Figura 80 Atención. Se detectó un objeto infectado

Así, puede comprobar la reacción de la aplicación cuando detecta objetos de tipo diferente sólo con seleccionar varias opciones en los cuadros de diálogo mostrados durante el análisis.

Un resumen completo de los resultados del análisis se mostrarán en el informe (ver Figura 81).



Figura 81. Informe de análisis del directorio con virus de prueba

CAPÍTULO 8. CONTROL DE LA LLAVE DE LICENCIA

El funcionamiento de Kaspersky Anti-Virus está predeterminado por la presencia de una *llave de licencia*. La llave se incluye dentro del kit de distribución y le permite utilizar la aplicación a contar de su fecha de compra e instalación.



Kaspersky Anti-Virus NO FUNCIONA sin una llave de licencia.

Kaspersky Anti-Virus no funcionará si la llave de licencia no ha sido instalada, si el periodo de validez ha caducado o si la llave instalada se encuentra en la "lista negra". En estos casos, las funciones generales del antivirus queda deshabilitado hasta que se instale una nueva llave de licencia válida.

Cuando la licencia caduca, el funcionamiento de Kaspersky Anti-Virus sigue siendo el mismo, excepto por que las actualizaciones de la base antivirus y de los componentes de la aplicación ya no son descargadas. Sigue siendo posible analizar su equipo y correo electrónico, así como desinfectar objetos infectados descubiertos, pero tendrá que estar haciéndolo con bases antivirus desfasadas. Por tanto, no podemos garantizar una protección total contra nuevos virus que aparezcan después de caducar su licencia.

Para evitar la infección de su equipo por nuevos virus, recomendamos ampliar su licencia.

Dos semanas antes de caducar la licencia, Kaspersky Anti-Virus presentará notificaciones diarias. Durante dos semanas, podrá ver un mensaje de advertencia cada vez que abre la ventana principal de la aplicación.

El mismo mensaje se muestra también cada vez que abre la ventana principal de Kaspersky Anti-Virus después de caducar la licencia.



Para renovar su licencia, debe adquirir e instalar una nueva llave para Kaspersky Anti-Virus. Para ello:

1. Póngase en contacto con la organización a la que compró el producto para adquirir una nueva llave de licencia para utilizar Kaspersky Anti-Virus;

o:

adquiera la llave de licencia directamente en Kaspersky Lab con un mensaje al Departamento de ventas (sales@kaspersky.com), o complete un formulario de pedido en nuestro sitio Web (www.kaspersky.com). Tras

el pago, recibirá una llave de licencia en la dirección de correo indicada en su formulario de pedido.

2. Instale el archivo llave de licencia. Para más detalles acerca de cómo operar con la llave de licencia desde la interfaz local, vea la sección 8.1 pág. 134; para más detalles acerca del uso de la interfaz de Kaspersky Administration Kit, vea la sección 8.2 pág. 135.



Puede instalar dos llaves: una llave actual, y otra de reserva. La llave actual es utilizada por el paquete software durante sus operaciones corrientes. La aplicación tan sólo puede tener una llave "actual". La llave de reserva es activada en cuanto caduca la llave de licencia actual.

8.1. Trabajar con llaves de licencia desde la interfaz local

Para ampliar su licencia desde la interfaz local de Kaspersky Anti-Virus:

1. Trabajar con llaves de licencia desde la interfaz (para más detalles, ver anterior).
2. Haga clic en [Llaves de licencia](#) en el panel izquierdo de la ficha **Soporte** (Figura 6).
3. En la ventana **Llaves de licencia** (ver Figura 82), haga clic en **Agregar** y seleccione la nueva llave de licencia en el cuadro de diálogo Selección estándar de Windows.

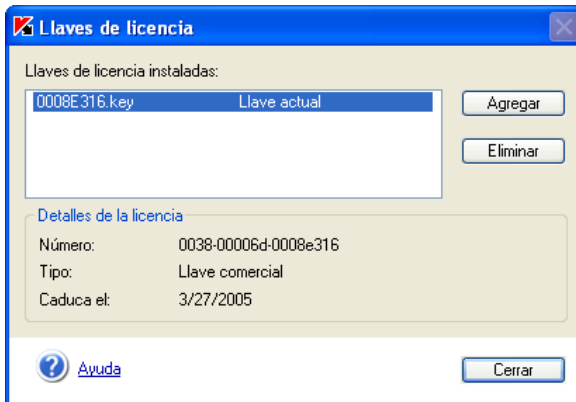


Figura 82. Ventana Control de la llave de licencia

Si agrega un nuevo archivo llave cuando ya dispone de llave actual, la aplicación le ofrece dos opciones de instalación:

- Instale la nueva llave como llave reservada (se recomienda). La nueva llave se agrega a la lista con el indicador "reserva". Cuando la llave actual caduque, la nueva llave adoptará automáticamente el indicador "actual".
- Reemplazar la llave actual por la nueva. La nueva llave se agrega a la lista con el indicador "actual".



Nota: la eliminación de la llave actual vigente causa ¡la eliminación automática de la llave de reserva instalada!

8.2. Trabajar con llaves de licencia desde la interfaz de Kaspersky Administration Kit

Si el paquete es controlado por Kaspersky Administration Kit, es posible ampliar una licencia con uno de los dos métodos siguientes:

- *Agregar licencia de grupo:* ampliación simultánea de la licencia de Kaspersky Anti-Virus para los equipos seleccionados que pertenecen a uno o más grupos (ver detalles en el manual del administrador para "Kaspersky Administration Kit 5.0").
- *Agregar una licencia individual:* amplía la licencia de Kaspersky Anti-Virus para un equipo individual.



Para renovar la licencia de su estación de trabajo, debe adquirir e instalar una nueva llave para Kaspersky Anti-Virus. Para ello:

1. Compre una llave de licencia (ver Capítulo 8 pág. 133).
2. Cree una tarea local para la instalación de la llave de licencia (ver sección 6.2.1.1 pág. 115).

Puede revisar los datos de las llaves de licencia (actuales y de reserva) que estén instaladas en un equipo específico bajo la ficha **Licencias** (ver sección 6.3.4 pág. 127).

CAPÍTULO 9. 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.



¿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 aplicar transformaciones matemáticas a 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 las 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 700 formatos de compilación y compresión de archivos. 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 analizado, 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 quedara bloqueada al finalizar este plazo.



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

Quando 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.
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;
 - 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: *¿Es posible para un intruso sustituir la base antivirus?*

Cada base antivirus utiliza una firma exclusiva que Kaspersky Anti-Virus comprueba en todas sus consultas. 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.



Pregunta: *Utilizo un servidor proxy y el servicio de actualizaciones no funciona en mi equipo. ¿Qué debo hacer?*

Los problemas siguientes pueden inhabilitar las actualizaciones cuando se trabaja con un servidor proxy:

- Configuración de red incorrecta.

Existen dos formas de indicar los parámetros de red cuando se configura el servicio de actualizaciones: utilizar la configuración de Internet Explorer o una configuración personalizada. El servicio de

actualización utiliza a veces incorrectamente la configuración de Internet Explorer. Esto puede ocurrir en los casos siguientes:

- La conexión Internet no está configurada en un equipo;
- La configuración de MS Internet Explorer no está disponible si ninguno de los usuarios se ha conectado;
- el servidor proxy requiere autorización.

En cualquiera de estos casos, especifique directamente los parámetros de red en la configuración del servicio de actualizaciones.

- El servidor proxy utilizado es de un tipo no reconocido por el servicio de actualizaciones de Kaspersky Anti-Virus.

El servicio de actualizaciones no funciona con Kerio WinRoute, porque WinRoute no es totalmente compatible con el protocolo HTTP 1.0. En este caso, se recomienda utilizar otro servidor proxy.

El servicio de actualizaciones tampoco funciona con Microsoft ISA Server a través del protocolo FTP. En este caso, recomendamos recuperar las actualizaciones desde los servidores de Kaspersky Lab a través del protocolo HTTP.

ANEXO A. 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 6) 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 5.5.1.2 pág. 74). 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 5.5.1.2 pág. 74) 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 6). 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 B. 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.

Análisis según extensión: en su análisis, la aplicación examina la extensión del archivo para determinar si se trata de un archivo que puede estar infectado.

Análisis según formato: en su análisis, la aplicación examina el contenido interno del archivo, en concreto el identificador de formato del encabezado de archivo.

Actualización de la base antivirus: Una función de Kaspersky Anti-Virus que garantiza que la protección antivirus de su equipo sigue siendo válida. Los procesos de actualizaciones incluyen la recuperación de una copia de la *base antivirus* desde los *servidores de actualizaciones* de Kaspersky Lab en su equipo, y su integración automática en Kaspersky Anti-Virus Personal.

Administrador de red lógica: persona que controla el funcionamiento del antivirus a través del sistema de control remoto centralizado de Kaspersky Administration Kit.

Administrador de seguridad: persona que controla el funcionamiento de la aplicación. El administrador puede actuar bien en remoto con la *Consola de administración* o con una interfaz local.

Análisis completo: modo de funcionamiento de la aplicación diseñado para analizar el equipo completo en busca de código dañino, tras la petición realizada por el usuario, con la posterior desinfección y eliminación de objetos sospechosos o infectados, si los hay.

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.

Bloqueo de objetos: bloquea el acceso a un objeto desde aplicaciones externas. Un objeto bloqueado no está disponible para lectura, ejecución, modificación ni eliminación.

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.

Control centralizado de la aplicación: forma de control remoto de la aplicación que se realiza desde los servicios de administración ofrecidos por Kaspersky Administration Kit 5.0.

D

Desinfección: Tratamiento que se aplica a los *objetos infectados*. La desinfección se traduce en la recuperación parcial o completa de los datos o resulta en un diagnóstico según el cual no es posible desinfectarlos. Los objetos son desinfectados mediante la base antivirus. Si la desinfección es la primera acción aplicada a un objeto, es decir, la primera después de detectar el objeto sospechoso, la aplicación crea una copia de respaldo del archivo. Si se pierden datos durante la desinfección, puede recuperar este objeto a partir de la copia de respaldo.

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.

Directiva de grupo: conjunto de parámetros de aplicación en vigor dentro de un grupo de administración controlado por Kaspersky Administration Kit 5.0.

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.

iChecker™: tecnología que permite a la aplicación evitar volver a analizar objetos no modificados desde el análisis anterior. La tecnología desarrollada utiliza una base de datos de sumas de control.

iStreams™: tecnología que permite a la aplicación evitar volver a analizar objetos ubicados en unidades con sistema de archivos NTFS y no modificados desde el análisis anterior. La tecnología desarrollada almacena sumas de control en flujos NTFS alternativos.

K

Kaspersky Administration Kit 5.0: aplicación incluida en Kaspersky Business Optimal y en Kaspersky Corporate Suite, diseñada para la administración centralizada de un sistema de protección antivirus en una red corporativa construida sobre aplicaciones Kaspersky Lab.

L

Lista negra: base de datos con información acerca de las llaves utilizadas por usuarios que han violado el Contrato de licencia, así como las llaves generadas pero que quedaron sin vender por cualquier razón. El contenido de la lista negra se actualiza de forma diaria; Kaspersky Anti-Virus no funcionará sin ella.

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 actual: la llave de licencia instalada y actualmente utilizada por Kaspersky Anti-Virus para habilitar sus funciones. Determina el periodo de validez de la licencia y la directiva de licencia correspondiente al producto. Una aplicación tan sólo puede tener una llave "actual".

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 Personal. 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 C. 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.

C.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 Anti-Hacker 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;
- *Clientes de correo*: Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail y Qmail;

¹ En función del tipo de kit de distribución.

- *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 completa 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).

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.

C.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	WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com

ANEXO D. ÍNDICE

Actualización de la Base antivirus,
137

Contrato de licencia, 10

CUARENTENA

ENVIAR UN ARCHIVO PARA SU
EXAMEN EXPERTO, 140

Llave de licencia, 137

Presentación del producto
comprar en línea, 10

Respaldo

trabajar con archivos, 76

Servicio de soporte técnico, 11, 155

ANEXO E. 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).