

KASPERSKY LAB

Kaspersky[®] Anti-Virus 6.0 for
Windows Servers

GUÍA DEL USUARIO

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Guía del usuario

© Kaspersky Lab

<http://www.kaspersky.com>

Fecha de revisión: Julio, 2007

Índice

CAPÍTULO 1. AMENAZAS A LA SEGURIDAD DEL EQUIPO	9
1.1. Fuentes de amenazas.....	9
1.2. Cómo se propagan las amenazas.....	10
1.3. Tipos de amenazas.....	12
CAPÍTULO 2. KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS.....	15
2.1. Novedades de Kaspersky Anti-Virus 6.0 for Windows Servers	15
2.2. Elementos de defensa de Kaspersky Anti-Virus for Windows Servers.....	16
2.2.1. Antivirus de archivos.....	17
2.2.2. Tareas de análisis antivirus	17
2.2.3. Herramientas del programa	18
2.3. Requisitos hardware y software del sistema	19
2.4. Paquetes software.....	20
2.5. Servicios para usuarios registrados.....	21
CAPÍTULO 3. INSTALACIÓN DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	22
3.1. Proceso de instalación con el Asistente de instalación.....	23
3.2. Asistente de configuración	27
3.2.1. Utilizar objetos guardados con la versión 5.0.....	27
3.2.2. Activación del programa	27
3.2.2.1. Selección de un método de activación del programa	28
3.2.2.2. Introducción del código de activación	29
3.2.2.3. Obtención de un archivo llave	29
3.2.2.4. Selección de un archivo llave de licencia.....	29
3.2.2.5. Fin de la activación del programa	30
3.2.3. Configuración de la actualización	30
3.2.4. Planificación de un análisis antivirus.....	31
3.2.5. Restricciones de acceso al programa.....	31
3.2.6. Fin del Asistente de configuración	32
3.3. Instalación del programa desde la línea de comandos	32
3.4. Procedimiento de instalación del Objeto de directiva de grupo.....	33

3.4.1. Instalación del programa	33
3.4.2. Actualización del programa	34
3.4.3. Desinstalación del programa.....	35
3.5. Actualización de la versión 5.0 a la versión 6.0.....	35
CAPÍTULO 4. INTERFAZ DEL PROGRAMA.....	36
4.1. Icono de la barra del sistema	36
4.2. Menú contextual	37
4.3. Ventana principal del programa.....	38
4.4. Ventana de configuración del programa	40
CAPÍTULO 5. PRIMEROS PASOS	42
5.1. ¿Cuál es el estado de protección de mi equipo?.....	42
5.1.1. Indicadores de protección	42
5.1.2. Estado de Kaspersky Anti-Virus for Windows Servers	46
5.1.3. Estadísticas de funcionamiento del programa	47
5.2. Cómo analizar el equipo en busca de virus	48
5.3. Cómo analizar zonas críticas del equipo.....	48
5.4. Cómo analizar un archivo, carpeta o disco en busca de virus	49
5.5. Cómo actualizar el programa.....	50
5.6. Qué hacer si la protección no funciona	51
CAPÍTULO 6. SISTEMA DE ADMINISTRACIÓN DE LA PROTECCIÓN	52
6.1. Detener y reanudar la protección en su equipo	52
6.1.1. Suspensión de la protección	53
6.1.2. Desactivación de la protección	54
6.1.3. Suspensión / Detención de la protección	55
6.1.4. Reanudación de la protección de su equipo	55
6.1.5. Salir del programa	56
6.2. Tipos de programas malintencionados supervisados.....	56
6.3. Creación de una zona de confianza	57
6.3.1. Reglas de exclusión	59
6.3.2. Aplicaciones de confianza.....	62
6.4. Ejecución de tareas con otro perfil.....	64
6.5. Configuración de tareas planificadas y notificaciones	66
6.6. Opciones de energía	68
6.7. Configuración de servidor multiprocesador.....	69

CAPÍTULO 7. PROTECCIÓN ANTIVIRUS DEL SISTEMA DE ARCHIVOS DEL SERVIDOR	70
7.1. Selección de un nivel de seguridad para archivos.....	71
7.2. Configuración del componente Antivirus de archivos.....	73
7.2.1. Definición de los tipos de los objetos que se analizarán.....	73
7.2.2. Cobertura de protección.....	76
7.2.3. Configuración avanzada.....	78
7.2.4. Restauración de los parámetros predeterminados del componente Antivirus de archivos.....	81
7.2.5. Selección de acciones sobre objetos.....	81
7.2.6. Creación de una plantilla de notificación.....	83
7.3. Desinfección pospuesta.....	84
CAPÍTULO 8. ANÁLISIS ANTIVIRUS DE SU EQUIPO	85
8.1. Administración de tareas de análisis antivirus.....	86
8.2. Creación de una lista de objetos que deben analizarse.....	86
8.3. Creación de tareas de análisis antivirus.....	88
8.4. Configuración de tareas de análisis antivirus.....	89
8.4.1. Selección de un nivel de seguridad.....	90
8.4.2. Definición de los tipos de objetos que se analizarán.....	91
8.4.3. Restauración de los parámetros de análisis predeterminados.....	94
8.4.4. Selección de acciones sobre objetos.....	94
8.4.5. Configuración avanzada del análisis antivirus.....	96
8.4.6. Aplicación de una configuración global a todas las tareas.....	98
CAPÍTULO 9. PRUEBAS DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	99
9.1. Prueba con el 'virus' EICAR y sus modificaciones.....	99
9.2. Prueba del componente Antivirus de archivos.....	101
9.3. Prueba de las tareas de análisis antivirus.....	102
CAPÍTULO 10. ACTUALIZACIONES DEL PROGRAMA	104
10.1. Ejecución del componente de actualización.....	105
10.2. Anulación de la actualización anterior.....	106
10.3. Creación de tareas de actualización.....	107
10.4. Configuración de la actualización.....	108
10.4.1. Selección de un origen de actualizaciones.....	108
10.4.2. Selección del método y de los objetos que deben actualizarse.....	111

10.4.3. Configuración de la conexión.....	113
10.4.4. Distribución de actualizaciones.....	115
10.4.5. Acción después de actualizar.....	116
CAPÍTULO 11. OPCIONES AVANZADAS.....	118
11.1. Cuarentena para objetos potencialmente infectados.....	119
11.1.1. Acciones con objetos en cuarentena.....	120
11.1.2. Configuración de la cuarentena.....	122
11.2. Copias de respaldo de objetos peligrosos.....	122
11.2.1. Operaciones con la zona de respaldo.....	123
11.2.2. Configuración de los parámetros de respaldo.....	125
11.3. Informes.....	125
11.3.1. Configuración de los parámetros de informe.....	128
11.3.2. <i>Detectados</i> (ficha).....	129
11.3.3. <i>Eventos</i> (ficha).....	130
11.3.4. <i>Estadísticas</i> (ficha).....	131
11.3.5. <i>Configuración</i> (ficha).....	131
11.3.6. <i>Usuarios vetados</i> (ficha).....	132
11.4. Información general acerca del programa.....	133
11.5. Administración de licencias.....	135
11.6. Soporte técnico.....	137
11.7. Configuración de la interfaz de Kaspersky Anti-Virus for Windows Servers.....	138
11.8. Trabajar con opciones avanzadas.....	140
11.8.1. Notificaciones de eventos de Kaspersky Anti-Virus for Windows Servers.....	141
11.8.1.1. Tipos de eventos y modos de entrega de las notificaciones.....	142
11.8.1.2. Configuración de notificaciones por correo.....	143
11.8.1.3. Configuración de los parámetros del registro de eventos.....	145
11.8.2. Autoprotección y restricción de acceso.....	145
11.8.3. Solución de conflictos con otras aplicaciones.....	147
11.9. Importación y exportación de la configuración de Kaspersky Anti-Virus for Windows Servers.....	147
11.10. Restablecimiento de la configuración predeterminada.....	148
CAPÍTULO 12. ADMINISTRACIÓN DEL PROGRAMA CON KASPERSKY ADMINISTRATION KIT.....	149
12.1. Administración de la aplicación.....	151
12.1.1. Iniciando/deteniendo la aplicación.....	152

12.1.2. Configuración de los parámetros de la aplicación.....	153
12.1.3. Parámetros específicos.....	155
12.2. Administración de tareas.....	156
12.2.1. Inicio y detención de tareas.....	157
12.2.2. Creación de tareas.....	158
12.2.2.1. Creación de tareas locales.....	158
12.2.2.2. Creación de tareas de grupo.....	160
12.2.2.3. Creación de tareas globales.....	161
12.2.3. Configuración de tarea.....	161
12.3. Control de directivas.....	163
12.3.1. Creación de directivas.....	163
12.3.2. Examen y modificación de la configuración de la directiva.....	165
CAPÍTULO 13. OPERACIONES DESDE LA LÍNEA DE COMANDOS.....	167
13.1. Activación de la aplicación.....	169
13.2. Administración del Antivirus de archivos y las tareas.....	169
13.3. Análisis antivirus.....	172
13.4. Actualizaciones del programa.....	176
13.5. Parámetros para deshacer la actualización.....	177
13.6. Exportación de la configuración.....	178
13.7. Importación de la configuración.....	179
13.8. Ejecución del programa.....	180
13.9. Detención del programa.....	180
13.10. Obtención de un archivo de depuración.....	180
13.11. Visualización de la Ayuda.....	181
13.12. Códigos de retorno de la interfaz de la línea de comandos.....	181
CAPÍTULO 14. MODIFICACIÓN, REPARACIÓN Y DESINSTALACIÓN DEL PROGRAMA.....	183
14.1. Modificación, reparación y desinstalación del programa con el Asistente de instalación.....	183
14.2. Desinstalación del programa desde la línea de comandos.....	186
ANEXO A. INFORMACIÓN DE REFERENCIA.....	187
A.1. Lista de archivos analizados por extensión.....	187
A.2. Máscaras aceptadas para exclusión de archivos.....	189
A.3. Posibles máscaras de exclusión en la clasificación de la Enciclopedia del virus.....	191

A.4. Parámetros del archivo <i>setup.ini</i>	191
ANEXO B. KASPERSKY LAB.....	193
B.1. Otros productos Kaspersky Lab	194
B.2. Cómo encontrarnos	205
ANEXO C. CONTRATO DE LICENCIA.....	207

CAPÍTULO 1. AMENAZAS A LA SEGURIDAD DEL EQUIPO

A medida que las tecnologías de la información se desarrollan con rapidez y ocupan todos los aspectos de la vida, también crece el número y el espectro de los crímenes contra la seguridad de los datos.

Los cibercriminales han dado muestras de su interés por las actividades de organizaciones administrativas o comerciales. Con sus intentos de robar o revelar información confidencial, dañan la imagen profesional, interrumpen la actividad comercial y pueden alterar los contenidos de datos de una organización. Estos actos pueden causar daños considerables al capital, tangible o intangible.

Ninguna empresa grande está fuera de riesgo. Los usuarios particulares también pueden ser víctimas de ataques. Con el uso de diversas herramientas, los criminales consiguen apoderarse de sus datos personales (cuenta bancaria, números de tarjetas de crédito, contraseñas), provocan fallos en el sistema o se apoderan completamente del equipo. A continuación, el equipo puede servir como integrante de una red fantasma, es decir una red de equipos infectados utilizados por piratas para atacar servidores, enviar correo no solicitado, robar información confidencial y propagar nuevos virus y troyanos.

En el mundo de hoy, todo el mundo sabe que la información tiene un valor y debe ser protegida. Al mismo tiempo, la información debe estar disponible para un determinado grupo de usuarios que la necesitan (empleados, clientes y socios de negocio, por ejemplo). De ahí proviene la necesidad de crear un sistema de seguridad integral, que tenga en cuenta todas las posibles fuentes de amenazas, sean humanas o fabricadas por otras personas, o desastres naturales, y utilizar un abanico completo de medidas defensivas en todos los niveles: físico, administrativo y software.

1.1. Fuentes de amenazas

Una persona o grupo de personas, incluso algún fenómeno independiente de la actividad humana, puede amenazar a la seguridad de la información. De acuerdo con esto, todas las fuentes de amenazas pueden dividirse en tres grupos:

- **El factor humano.** Este grupo de amenazas incluye las acciones de personas que disponen (o no) de acceso autorizado a la información. Las amenazas de este grupo se subdividen en:

- *Externas*, que incluyen a los cibercriminales, los piratas ("hacker" en inglés), las estafas por Internet, los colaboradores sin escrúpulos y las organizaciones criminales.
- *Internas*, incluyendo las actuaciones del personal de la empresa. Las acciones de este grupo pueden ser deliberadas o accidentales.
- **El factor tecnológico.** Este grupo de amenazas se relaciona con problemas de orden técnico, por ejemplo, equipos que se vuelven obsoletos, software y hardware de mala calidad a la hora de procesar información. Todo ello conduce a fallos en los equipos y, a menudo, a pérdidas de datos.
- **Los desastres naturales.** Este grupo de amenazas incluye cualquier número de eventos de origen natural o independientes de la actividad humana.

Es necesario tener en cuenta estas tres fuentes de amenazas al desarrollar un sistema de protección de la seguridad. Esta Guía del usuario tan sólo cubre aquéllas que están directamente relacionadas con la especialidad de Kaspersky Lab, es decir, las amenazas externas que dependen de factores humanos.

1.2. Cómo se propagan las amenazas

A medida que se desarrollan las tecnologías informáticas y las herramientas de comunicaciones, los piratas disponen de posibilidades mayores para la propagación de amenazas. Examinemos esto con más detalle:

Internet

Internet es excepcional porque no es propiedad de nadie y nada sabe de fronteras geográficas. En gran medida, ha favorecido el desarrollo de innumerables recursos Web y el intercambio de información. Hoy día, cualquiera tiene acceso a información en Internet o puede crear su propia página Web.

Sin embargo, las impresionantes características de la red mundial ofrecen a los piratas la posibilidad de cometer crímenes, e Internet hace más difícil detectarlos y castigarlos.

Los piratas colocan virus y otros programas malintencionados en sitios Internet, presentándolos como software gratuito. Del mismo modo, las secuencias de comandos que se ejecutan automáticamente cuando abre una página Web, pueden ejecutar acciones peligrosas en su PC,

modificando incluso el Registro del sistema, robando datos personales o instalando algún software malintencionado.

Mediante el uso de tecnologías de red, los piratas pueden asaltar servidores corporativos. Estos ataques pueden causar fallos en el funcionamiento de su equipo o facilitar a piratas un acceso completo al sistema y, por consiguiente, a la información que tenga almacenada. También llegan a utilizarlo como parte de una red fantasma.

Intranet

La intranet se denomina red interna, especialmente diseñada para administrar información dentro de una misma organización o un red doméstica. Una intranet es un espacio unificado de almacenamiento, intercambio y acceso a información para todos los equipos de la red. Esto significa que si un equipo de la red está infectado, los demás corren un grave riesgo de infección. Para evitar este tipo de situaciones, es necesario proteger tanto el perímetro de la red como cada equipo individual.

Correo

Porque prácticamente cada equipo dispone de clientes de correo instalados y porque existen programas malintencionados que aprovechan el contenido de la libreta de direcciones, se dan las condiciones necesarias para la propagación de programas malintencionados. El usuario de un equipo infectado, sin ni siquiera saber que esto ocurre, puede enviar mensajes infectados a sus amigos y compañeros de trabajo y éstos a su vez, vuelven a enviar más mensajes infectados. Por ejemplo, resulta común que un archivo infectado no sea detectado cuando distribuye información comercial dentro del sistema de correo interno de una organización. Cuando esto ocurre, ya no son unas pocas personas las que resultan infectadas. Pueden ser centenares o miles de empleados, que todos juntos suman decenas de miles de suscriptores.

Medios de almacenamiento extraíbles

Los medios extraíbles (disquetes, CD-ROM y unidades USB de memoria flash) son ampliamente utilizados para almacenar y transmitir información.

Cuando abre un archivo que contiene código malintencionado en un soporte de almacenamiento extraíble, puede dañar los datos almacenados en local en su equipo y propagar el virus hacia otras unidades de disco de su equipo, o hacia otros equipos de la red.

1.3. Tipos de amenazas

Existe hoy día un gran número de amenazas que pueden afectar la seguridad del equipo. Esta sección presenta la amenazas bloqueadas por Kaspersky Anti-Virus for Windows Servers.

Gusanos

Esta categoría de programas malintencionados se propagan a sí mismo aprovechando las vulnerabilidades de los sistemas operativos. Esta categoría se nombró así por la forma en que los gusanos "reptan" de un equipo a otro, usando las redes y el correo. Esta característica permite a los gusanos propagarse realmente rápido.

Los gusanos penetran en el equipo, buscan direcciones de red de otros equipos y envían otras tantas copias de sí mismos, una por dirección. Además, los gusanos utilizan a menudo los datos de las libretas de direcciones del cliente de correo. Algunos de estos programas malintencionados crean en ocasiones archivos de trabajo en los discos de sistema, pero pueden ejecutarse sin consumir ningún recurso del sistema, excepto la RAM.

Virus

Los virus son programas que infectan otros programas, inyectan su propio código en ellos para tomar el control de los archivos infectados cuando son abiertos. Esta definición sencilla explica la acción básica que produce la *infección* por un virus.

Troyanos

Los caballos de Troya (los "troyanos") son programas que actúan en equipos sin autorización, eliminan información en discos, cuelgan el sistema, roban datos confidenciales, etc. Esta clase de programa malintencionado no es un virus en el sentido tradicional, ya que no infecta otros equipos o datos. Los troyanos no penetran por efracción en los equipos sino que son propagados por piratas, escondidos dentro de software corriente. Los daños que pueden causar pueden llegar a superar considerablemente los causados por ataques de virus tradicionales.

Recientemente, los gusanos se han convertido en el tipo más extendido de software malintencionado, seguidos de virus y troyanos. Algunos programas malintencionados toman sus características de dos o incluso las tres categorías.

Software publicitario o adware

El software publicitario viene incluido dentro de programas, sin el conocimiento del usuario, y está diseñado para mostrar publicidad. En

general, el software publicitario se incluye dentro de programas distribuidos gratuitamente. Las publicidades aparecen en la interfaz del programa. Estos programas también suelen recopilar datos personales acerca del usuario y mandarlo al desarrollador; modifican los parámetros del navegador (páginas de inicio y de búsqueda, niveles de seguridad, etc.) y generan tráfico fuera del control del usuario. Todo esto puede conducir a una pérdida de seguridad y ser causa directa de pérdidas económicas.

Software espía o spyware

Este software recoge información acerca de un usuario u organización sin su conocimiento. El software espía a menudo consigue escapar completamente a la detección. En general, el objetivo del software espía es:

- rastrear las acciones de un usuario en el equipo;
- recopilar información sobre el contenido del disco; en estos casos, suele explorar numerosos directorios y el Registro del sistema para compilar la lista de software instalado en el equipo;
- recoger información sobre la calidad de la conexión, el ancho de banda, la velocidad del módem, etc.

Software de riesgo

Un software potencialmente peligroso que no tiene por sí mismo un comportamiento dañino, puede ser utilizado como componente auxiliar de un código malintencionado, porque contiene fallos y errores. En algunas situaciones, la presencia de estos programas en un equipo puede poner sus datos en peligro. Este tipo de programas incluye, por ejemplo, las herramientas de administración remota, los mapeadores de teclado, clientes IRC, servidores FTP y las herramientas de uso genérico para interrumpir o disimular procesos.

Otro tipo de programa malintencionado que se asemeja a este tipo de software publicitario, espía o de riesgo es aquél que se presenta como un complemento de su navegador Internet para reencaminar el tráfico.

Bromas

Este tipo de software no supone ningún riesgo directo pero presenta mensajes indicando que estos daños sí se han producido o pueden producirse bajo algunas condiciones. Estos programas a menudo advierten al usuario de peligros que no existen, como el anuncio del reformato del disco (aunque no se produzca en realidad ningún formato) o de la detección de virus en archivos no infectados.

Procesos ocultos o rootkits

Son herramientas utilizadas para disimular actividades dañinas. Disimulan la presencia de programas malintencionados para evitar ser detectados por programas antivirus. Los procesos ocultos modifican el sistema operativo y las funciones básicas de un equipo para ocultar su propia presencia y las acciones del pirata en los equipos infectados.

Otros programas peligrosos

Son programas creados para generar ataques DoS en servidores remotos o para penetrar en otros equipos así como programas que intervienen en el entorno de desarrollo de programas malintencionados. Este tipo de programas incluye herramientas de efracción, compiladores de virus, buscadores de vulnerabilidades, programas de recuperación de contraseñas y otros tipos de programas para atacar recursos en la red o penetrar en un sistema.

Advertencia.

En lo que sigue, utilizamos la palabra "virus" para referirnos a cualquier programa malintencionado o peligroso. Sólo aportamos precisiones sobre el tipo de programa dañino cuando es necesario.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Kaspersky Anti-Virus 6.0 for Windows Servers es una nueva generación de productos de seguridad para los datos.

2.1. Novedades de Kaspersky Anti-Virus 6.0 for Windows Servers

Presentamos a continuación las nuevas características de Kaspersky Anti-Virus for Windows Servers:

Nuevas características de protección

- La tecnología de protección de archivos del programa ha sido modificada: ahora puede reducir la carga de su procesador y del subsistema de discos, y aumentar la velocidad de los análisis de archivos con las tecnologías iChecker e iSwift. Al operar de este modo, la aplicación no analizará dos veces los archivos.
- El proceso de análisis se ejecuta ahora en segundo plano, lo que permite al administrador seguir trabajando con el equipo. Si se produce una petición simultánea de recursos, el análisis antivirus se detiene hasta que termine la operación del usuario y continúa de nuevo en el punto donde se detuvo.
- Las zonas críticas del servidor, donde una infección podría tener consecuencias graves, son asignadas a tareas separadas. Puede configurar esta tarea para que se ejecute automáticamente cada vez que inicia el sistema.
- La función de notificación al usuario (ver 11.8.1 pág. 141) ha sido ampliada para algunos eventos que se producen durante el funcionamiento del programa. Puede elegir el método de notificación de cada uno de estos eventos: correos, sonidos, mensajes emergentes.
- Las nuevas características incluyen la tecnología de autoprotección de la aplicación, la protección contra el acceso remoto no autorizado a los servicios del programa, la protección de los archivos de la aplicación

contra el acceso o modificación no autorizados así como la protección con contraseña de la configuración del programa.

Nuevas características de la interfaz de aplicación

- La nueva interfaz de Kaspersky Anti-Virus for Windows Servers simplifica y facilita el uso de las funciones del programa. Asimismo, para modificar la apariencia del programa puede crear y utilizar sus propias imágenes y combinaciones de color.
- El programa le proporciona regularmente consejos mientras lo utiliza: Kaspersky Anti-Virus for Windows Servers muestra mensajes de información acerca del nivel de protección, describe sus operaciones con comentarios y consejos e incluye una sección de Ayuda completa.

Nuevas características de actualización del programa

- Esta versión de la aplicación introduce un nuevo procedimiento de actualización mejorado: Kaspersky Anti-Virus comprueba automáticamente si están disponibles nuevos paquetes de actualización. Si encuentra nuevas actualizaciones, las descarga e instala en el equipo.
- Las descargas son incrementales, ignorando los archivos que ya han sido descargados. Esto permite reducir el tráfico de descarga para actualizaciones a la décima parte.
- Las actualizaciones son descargadas desde el origen más eficiente.
- El programa cuenta con una característica que permite deshacer las actualizaciones y restaurar la última versión funcional de las firmas si, por ejemplo, las firmas de amenazas son dañadas o se produce un error al copiarlas.
- Se incluye una nueva característica que permite distribuir las actualizaciones a una carpeta local donde otros equipos de la red pueden recuperarlas, para reducir el tráfico Internet.

2.2. Elementos de defensa de Kaspersky Anti-Virus for Windows Servers

El sistema de protección de Kaspersky Anti-Virus for Windows Servers incluye:

- El Antivirus de archivos (ver 2.2.1 pág. 17), que supervisa el sistema de archivos del equipo en modo de tiempo real.

- Tareas de análisis antivirus (ver 2.2.2 en la página 17) que se hace cargo del análisis antivirus de la memoria y del sistema de archivos del equipo, tanto como de archivos, carpetas, discos o zonas individuales.
- Características de soporte (ver 2.2.3 en la página 18) que ofrecen información de soporte para trabajar con el programa y ampliar sus posibilidades.

2.2.1. Antivirus de archivos

El servidor está protegido en tiempo real por el componente **Antivirus de archivos**.

Un sistema de archivos puede contener virus y otros programas peligrosos. Los programas malintencionados pueden mantenerse dentro del sistema de archivos durante años después de haber sido introducidos algún día mediante una unidad extraíble o Internet, sin manifestarse de ningún modo. Pero basta con abrir el archivo infectado para activar el virus instantáneamente.

El componente Antivirus de archivos supervisa el sistema de archivos del equipo. Analiza todos los archivos que pueden ser abiertos, ejecutados o guardados en el servidor así como todas las unidades de disco conectadas. Kaspersky Anti-Virus intercepta cada intento de acceso a un archivo y analiza dicho archivo en busca de virus conocidos. Sólo es posible seguir usando el archivo si no está infectado o si el tratamiento del componente Antivirus de archivos tuvo éxito. Si no es posible reparar un archivo por cualquier razón, se eliminará y una copia del archivo se guardará en el Respaldo (ver 11.2 pág. 122), o se moverá a Cuarentena (ver 11.1 en la página 119).

2.2.2. Tareas de análisis antivirus

Además de supervisar constantemente con el componente Antivirus de archivos todas las vías de penetración de los programas malintencionados, es extremadamente importante analizar con regularidad su equipo. Esto es necesario para controlar los riesgos de propagación de programas malintencionados que no fueron descubiertos por el componente Antivirus de archivos, por ejemplo, porque el nivel de seguridad estaba definido a un nivel demasiado bajo.

Kaspersky Anti-Virus for Windows Servers configura de forma predeterminada las tareas de análisis antivirus siguientes:

Zonas críticas

Análisis antivirus de todas las zonas críticas del equipo. Esto incluye la memoria del sistema, los programas de inicio, los sectores de arranque

en disco y los directorios del sistema *Microsoft Windows*. El objetivo de la tarea es detectar con rapidez los virus activos sin tener que realizar un análisis completo del equipo.

Mi PC

Busca virus en su equipo mediante un análisis completo de todos los discos, de la memoria y de los archivos.

Objetos de inicio

Analiza todos los programas de inicio automático que se cargan al arrancar el sistema, así como la memoria y los sectores de arranque de los discos duros.

También tiene la opción de crear otras tareas de análisis antivirus y definir su planificación.

2.2.3. Herramientas del programa

Kaspersky Anti-Virus for Windows Servers incluye un cierto número de herramientas de soporte, diseñadas para ofrecer protección en tiempo real, aumentar las posibilidades del programa y ayudarle mientras lo utiliza.

Actualizar

Para estar siempre listo para eliminar un virus o cualquier otro programa peligroso, Kaspersky Anti-Virus for Windows Servers necesita estar actualizado. El componente *Actualizar* está precisamente diseñado para ello. Es responsable de la actualización de las bases de aplicación y de los módulos de programa de Kaspersky Anti-Virus for Windows Servers.

La característica Distribuir actualizaciones le permite guardar las firmas de amenazas, la base de datos de ataques de red y los módulos de aplicación descargados desde los servidores de actualización de Kaspersky Lab, para permitir que otros equipos puedan utilizarlas sin consumir ancho de banda.

Archivos de datos

El componente Antivirus de archivos, todos los análisis y actualizaciones del programa crean informes de ejecución. Los informes contienen información sobre las operaciones completadas y el resultado de las mismas. La característica de *Informes* le mantendrá siempre informado del funcionamiento de cualquier componente de Kaspersky Anti-Virus for Windows Servers. En caso de problema, puede enviar los informes a Kaspersky Lab para que nuestros especialistas puedan estudiar la situación con el mayor detalle y ayudarle lo más rápidamente posible.

Kaspersky Anti-Virus for Windows Servers mueve todos los archivos sospechosos de ser peligrosos a un almacén especial de *Cuarentena*, donde se conservan cifrados para evitar que puedan infectar el equipo. Puede analizar estos objetos, restaurarlos a sus ubicaciones de origen, eliminarlos o mover manualmente archivos a cuarentena. Todos los archivos que quedan desinfectados después de terminar el análisis antivirus son automáticamente restaurados a sus ubicaciones de origen.

La *zona de respaldo* conserva copias de los archivos desinfectados y eliminados por Kaspersky Anti-Virus. Estas copias se crean por si es necesario restaurar los archivos o tener información acerca de su infección. Las copias de respaldo de los archivos también se almacenan en formato cifrado para evitar posteriores infecciones.

Puede restaurar un archivo a su ubicación original a partir de la copia de respaldo y eliminar ésta.

Soporte

Todos los usuarios registrados de Kaspersky Anti-Virus pueden beneficiarse de nuestro servicio de soporte técnico. Para saber dónde exactamente puede obtener soporte técnico, utilice la característica de *Soporte*.

Estos vínculos le permiten consultar el foro de usuarios de Kaspersky Lab así como una lista de preguntas frecuentes, que pueden ayudarle a resolver su problema. También puede completar un formulario en línea, para enviar al Soporte técnico un informe de error o una pregunta sobre el funcionamiento de la aplicación.

También podrá tener acceso al Soporte técnico en línea y, por supuesto, estamos siempre dispuestos a ayudarle con Kaspersky Anti-Virus por teléfono.

2.3. Requisitos hardware y software del sistema

Para ejecutar correctamente Kaspersky Anti-Virus, su equipo debe cumplir los siguientes requisitos mínimos:

Requisitos generales:

- 50 Mb de espacio libre en el disco duro
- CD-ROM (para instalar Kaspersky Anti-Virus for Windows Servers desde el CD de instalación)

- Microsoft Internet Explorer 5.5 o superior (para actualizar las firmas de amenazas y los módulos de aplicación por Internet)
- Microsoft Windows Installer 2.0

Sistema operativo:

- Microsoft Windows 2000 Server/Advanced Server con Service Pack 4 o superior, y todas las actualizaciones disponibles.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, todos los Service Packs, todas las actualizaciones disponibles.
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Paquetes software

Puede adquirir la versión en paquete de Kaspersky Anti-Virus for Windows Servers en nuestros distribuidores o descargarla desde tiendas Internet, incluso en la sección **eStore** de www.kaspersky.com.

Si adquiere la caja del programa, la distribución incluye:

- Un sobre sellado con un CD de instalación que contiene los archivos de programa.
- Una llave de licencia, en el paquete de instalación o en un disquete especial, o un código de activación de la aplicación en el estuche del CD.
- Una Guía del usuario
- El contrato de licencia de usuario final (CLUF)

Antes de abrir el sobre con el disco de instalación, lea atentamente todo el contrato.

Si adquiere Kaspersky Anti-Virus for Windows Servers en una tienda en línea, habrá copiado el producto desde el sitio Internet de Kaspersky Lab (**Downloads** → **Product Downloads**: Descargas de productos). Puede descargar la Guía del usuario en la sección **Downloads** → **Documentation** (Descargas de documentación).

Le enviaremos una llave de licencia o un código de activación por correo un vez recibido el pago.

El contrato de licencia de usuario final es un contrato legal entre Usted y Kaspersky Lab que describe los términos y condiciones de uso del producto que acaba de adquirir.

Lea el contrato atentamente.

Si no está de acuerdo con los términos y condiciones del CLUF, puede devolver la caja del producto al distribuidor donde lo compró y recuperar el dinero abonado. En este caso, el sobre con el disco de instalación debe seguir cerrado.

Si rompe el sello del disco de instalación, significa que acepta todos los términos del CLUF.

2.5. Servicios para usuarios registrados

Kaspersky Lab proporciona a sus usuarios registrados un abanico de servicios que les permite sacar todo el partido de Kaspersky Anti-Virus for Windows Servers.

Después de activar el programa, se convierte en usuario registrado, con acceso a los servicios siguientes por el tiempo de licencia:

- Nuevas versiones del programas sin coste alguno;
- Consultas acerca de la instalación, configuración y funcionamiento del programa, por teléfono y correo electrónico
- Notificaciones acerca de nuevas versiones de productos Kaspersky Lab y virus nuevos (sólo para usuarios inscritos a la lista de noticias de Kaspersky Lab)

Kaspersky Lab no ofrece soporte técnico acerca del uso y funcionamiento del sistema operativo ni para otros productos que los suyos.

CAPÍTULO 3. INSTALACIÓN DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Existen varios métodos de instalación de Kaspersky Anti-Virus 6.0 for Windows Servers:

- Instalación local: instala la aplicación en un equipo único. Es necesario tener acceso directo a dicho equipo para ejecutar y completar la instalación. Es posible realizar una instalación local de los dos modos siguientes:
 - instalación interactiva con el Asistente de instalación de la aplicación (ver 3.1 pág. 23); este modo de instalación requiere la interacción con el usuario;
 - instalación desatendida, que se ejecuta desde la línea de comandos, sin necesidad de interactuar con el usuario (ver 3.3 pág. 32).
- Instalación remota: instala de forma remota la aplicación en equipos de la red, desde la estación de trabajo del administrador, y utiliza:
 - la suite Kaspersky Administración Kit (ver la Guía de implementación de Kaspersky Administración Kit);
 - directivas de dominios y grupos Microsoft Windows Server 2000/2003 (ver 3.4 pág. 33).

Le recomendamos cerrar todas las aplicaciones en ejecución antes de instalar Kaspersky Anti-Virus (incluso en caso de instalación remota).

Si Kaspersky Anti-Virus 5.0 ya está instalado, se eliminará y actualizará a Kaspersky Anti-Virus 6.0 durante la ejecución del programa de instalación (ver 3.5 pág. 35 para más detalles). Las actualizaciones a las últimas revisiones (de versiones anteriores) se realizan de forma transparente dentro de Kaspersky Anti-Virus 6.0.

3.1. Proceso de instalación con el Asistente de instalación

Para instalar Kaspersky Anti-Virus for Windows Servers en su equipo, ejecute el archivo instalador de Microsoft Windows desde el CD de instalación.

Nota:

El proceso de instalación de la aplicación a partir de un paquete de instalación descargado de Internet es similar al de la instalación desde el CD de instalación.

Un Asistente de instalación abre el programa. Cada ventana contiene un conjunto de botones para desplazarse por el proceso de instalación. Esta es una breve descripción de sus funciones:

- **Siguiente:** acepta una acción y se desplaza al paso siguiente de la instalación.
- **Anterior:** regresa al paso previo del proceso de instalación.
- **Cancelar:** cancela la instalación del producto.
- **Terminar:** pone fin al proceso de instalación del programa.

Presentamos a continuación los pasos del proceso de instalación.

Paso 1. Comprobación de los requisitos de sistema para instalar Kaspersky Anti-Virus for Windows Servers

Antes de instalar el programa en su equipo, el programa de instalación comprueba el sistema operativo y los Service Packs necesarios para instalar Kaspersky Anti-Virus for Windows Servers. También busca en su equipo otros programas necesarios y comprueba que sus derechos de usuario le permiten instalar el software.

Si alguno de estos requisitos no se cumple, el programa presentará un mensaje con la información del error. Le recomendamos instalar cualquier Service Packs mediante **Windows Update**, así como cualquier otro programa necesario antes de instalar Kaspersky Anti-Virus for Windows Servers.

Paso 2. Pantalla de bienvenida del instalador

Si su equipo cumple todos los requisitos, en cuanto ejecuta el archivo de instalación una ventana le informa del inicio de la instalación de Kaspersky Anti-Virus for Windows Servers.

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

Paso 3. Lectura del contrato de licencia de usuario final

La siguiente ventana contiene el Contrato de licencia de usuario final entre Usted y Kaspersky Lab. Léalo con atención y si está de acuerdo con todos los términos y condiciones del contrato, seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**. El proceso de instalación continuará.

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

Paso 4. Selección de una carpeta de instalación

El paso siguiente de la instalación de Kaspersky Anti-Virus for Windows Servers sirve para indicar donde se instalará el programa dentro de su equipo. La ruta predeterminada es:

- **<Unidad>\Archivos de programa\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers:** para sistemas de 32 bits
- **<Unidad>\Archivos de programa\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers:** para sistemas de 64 bits

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

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

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

Paso 5. Utilización de parámetros de instalación guardados

En esta etapa, debe especificar si desea utilizar los parámetros o las firmas de amenazas que fueron guardados cuando eliminó una versión anterior de Kaspersky Anti-Virus 6.0 en su equipo.

Veamos con más detalle cómo funcionan las opciones mencionadas.

Si instaló una versión o compilación anterior de Kaspersky Anti-Virus for Windows Servers en su equipo y conservó las firmas de amenazas al desinstalarla, puede aprovecharla para la versión actual. Para ello, active

Firmas de amenazas. Las firmas de amenazas incluidas con el programa de instalación no serán copiadas al servidor.

Para utilizar los parámetros de protección configurados y guardados de una versión anterior, active la casilla **Configuración de la protección.**

Paso 6. Selección del tipo de instalación

En este paso, debe seleccionar qué partes del programa desea instalar en su equipo. Tiene tres opciones:

Completa. Si selecciona esta opción, se instalarán todos los componentes de Kaspersky Anti-Virus for Windows Servers.

Personalizado. Esta opción le permite seleccionar los componentes de programa que desea instalar. Para más información, vea Paso 7.

Para seleccionar el tipo de instalación, haga clic en el botón correspondiente.

Paso 7. Selección de los componentes de programa para instalar

Este paso sólo aparece si seleccionó el tipo de instalación **Personalizado**.

Si seleccionó la instalación personalizada, deberá activar los componentes de Kaspersky Anti-Virus for Windows Servers que desea instalar. De forma predeterminada, la instalación del componente Antivirus de archivos y del conector del Agente de administración para administración remota con Kaspersky Administration Kit, están seleccionados.

Para activar los componentes que desea instalar, haga clic en el icono junto al nombre de componente y seleccione **Se instalará en la unidad de disco duro local** en el menú abierto. Encontrará más información acerca de la protección proporcionada por un componente y el espacio en disco necesario para la instalación en la parte inferior de la ventana de instalación del programa.

Si no desea instalar un componente, seleccione **La característica completa se instalará en el disco duro local** desde el menú contextual.

Después de seleccionar los componentes que desea instalar, haga clic en **Siguiente**. Para restablecer la lista de programas predeterminados, haga clic en **Restablecer**.

Paso 8. Búsqueda de otros programas antivirus

En este paso, el programa de instalación busca otros productos antivirus instalados en su equipo, incluyendo productos de Kaspersky Lab, que podrían

plantear problemas de compatibilidad con Kaspersky Anti-Virus for Windows Servers.

El programa de instalación presenta en pantalla la lista de estos programas. El programa le pregunta si desea desinstalarlos antes de continuar con la instalación.

Puede optar por la desinstalación manual o automática bajo la lista de aplicaciones antivirus detectadas (sólo los productos de Kaspersky Lab serán eliminados automáticamente).

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

Paso 9. Fin de la instalación del programa

En este paso, el programa le invita a concluir la instalación del programa en su equipo.

No recomendamos desactivar la casilla **Activar la autoprotección antes de instalar** cuando instala Kaspersky Anti-Virus 6.0 por primera vez. Al activar los módulos de protección, podrá anular correctamente la instalación del programa en caso de producirse errores durante la operación. Si está reinstalando el programa, le recomendamos desactivar esta casilla.

Si instala la aplicación de forma remota mediante **Escritorio remoto de Microsoft Windows**, le recomendamos activar la casilla **Activar la autoprotección antes de instalar**. En otro caso, el proceso de instalación podría no completarse o hacerlo incorrectamente.

Si desea agregar automáticamente las exclusiones recomendadas por Microsoft para servidores, active la casilla **Excluir áreas recomendadas por Microsoft del análisis antivirus**.

Para agregar la variable de entorno %Path% al entorno de avp.com después de la instalación, active la casilla **Agregar la ruta de avp.com a la variable de entorno %PATH%**.

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

Advertencia:

Quando instala los componentes de Kaspersky Anti-Virus que interceptan el tráfico de red, las conexiones de red actuales se interrumpen. La mayoría se restablecen al cabo de poco tiempo.

Paso 10. Fin del proceso de instalación

La ventana **Completar Instalación** contiene información para terminar el proceso de instalación de Kaspersky Anti-Virus.

Para iniciar el Asistente de configuración, haga clic en **Siguiente** (ver 3.2 pág. 27).

Si la instalación se terminó con éxito puede que un mensaje en pantalla le indique que debe reiniciar su equipo.

3.2. Asistente de configuración

La ventana principal de Kaspersky Anti-Virus 6.0 for Windows Servers se inicia al final de la instalación del programa. Le permite definir una primera configuración de los parámetros del programa en función de las características y utilización de su equipo.

La interfaz del Asistente de instalación está diseñada como la de cualquier Asistente de Microsoft Windows y consta de varios pasos: puede desplazarse por ellos con los botones **Anterior** y **Siguiente**, o salir con **Terminar**. El botón **Cancelar** interrumpe el Asistente en cualquier punto.

Si para interrumpir el Asistente, cierra la ventana del Asistente, la aplicación no se ejecutará. Cada vez que inicie la aplicación, el Asistente de instalación volverá a mostrarse hasta que termine el procedimiento con éxito.

3.2.1. Utilizar objetos guardados con la versión 5.0

Esta ventana del Asistente se muestra cuando instala la aplicación por encima de Kaspersky Anti-Virus 5.0. El programa le invita a seleccionar los datos de la versión 5.0 que desea importar en la versión 6.0. Se incluyen los archivos de cuarentena o respaldo o los parámetros de protección.

Para utilizar esta información en la versión 6.0, active las casillas necesarias.

3.2.2. Activación del programa

Antes de activar el programa, asegúrese de que la configuración de hora y fecha del equipo corresponde con la actual.

El programa se activa con la instalación de una llave de licencia utilizada por Kaspersky Anti-Virus para comprobar el contrato de licencia y determinar su fecha de caducidad.

La llave de licencia contiene la información del sistema necesaria para el funcionamiento de todas las características del programa así como otros datos:

- información de soporte (quién ofrece asistencia y dónde obtenerla);
- nombre, número y fecha de caducidad de su licencia.

3.2.2.1. Selección de un método de activación del programa

Dependiendo de si ya dispone de una llave de licencia para Kaspersky Anti-Virus o necesita obtener una desde el servidor de Kaspersky Lab, dispone de varias opciones para activar el programa:

- **Activar con código de activación.** Seleccione esta opción de activación si ha adquirido la versión completa del programa y recibió un código de activación. Este código de activación le facilita un archivo llave que le da acceso a todas las funciones de la aplicación durante el plazo previsto por el contrato de licencia.
- **Activar la versión de prueba.** Seleccione esta opción de activación si desea instalar la versión de evaluación del programa antes de decidirse por adquirir la versión comercial. Recibirá una llave gratuita válida por el tiempo especificado en el contrato de licencia de evaluación.
- **Utilizar una llave de licencia existente.** Active el programa con el archivo llave de licencia de Kaspersky Anti-Virus 6.0.
- **Activar más tarde.** Al elegir esta opción, se pasa por alto la etapa de activación. Kaspersky Anti-Virus for Windows Servers quedará instalado en su equipo y tendrá acceso a todas las características del programa, salvo las actualizaciones (sólo puede actualizar las bases de aplicación una vez después de instalar el programa).

Las dos primeras opciones de activación utilizan un servidor Web de Kaspersky Lab, lo que requiere una conexión Internet. Antes de activar el programa, compruebe sus parámetros de red (ver 10.4.3 en la pág. 113) en la ventana abierta con **Configuración LAN** (si es necesario). Para información más avanzada acerca de la configuración de los parámetros de red, póngase en contacto con el administrador del sistema o con su proveedor de servicios Internet.

Si no dispone de conexión Internet cuando instala el programa, puede activar la aplicación más tarde (ver 11.5 pág. 135) desde la interfaz o utilizar el acceso Internet de otro equipo para registrarse en el sitio Web del Soporte técnico de Kaspersky Lab y obtener una llave con su código de activación.

3.2.2.2. Introducción del código de activación

Para activar el programa, introduzca el código de activación. Si compró el programa por Internet, recibirá el código de activación por correo electrónico. Si compró la versión en paquete del programa, el código de activación del programa se encuentra en el sobre del CD de instalación.

El código de activación es una secuencia de cuatro grupos de cinco letras o números cada uno, separados por guiones, sin espacios. Por ejemplo, 11AA1-11AAA-1AA11-1A111. Observe que el código utiliza el juego de caracteres latino.

Indique su información de contacto en la parte inferior de la ventana: nombre completo, dirección de correo electrónico, país y ciudad de residencia. Esta información puede ser necesaria para identificar a un usuario si, por ejemplo, un archivo llave se pierde o ha sido robado. Si esto ocurre, sus datos de contacto le permitirán obtener una nueva llave de licencia.

3.2.2.3. Obtención de un archivo llave

El Asistente de configuración se conecta a los servidores de Kaspersky Lab y envía sus datos de registro (el código de activación y su información personal), que son examinados en el servidor.

Si el código de activación supera la comprobación, el Asistente recupera un archivo llave de licencia. Si instala la versión de evaluación del programa, el Asistente de configuración recuperará una llave de prueba sin código de activación.

El archivo recibido se instalará automáticamente para poder utilizar el programa y se abrirá la ventana de activación terminada, con información detallada sobre la llave utilizada.

Si el código de activación no pasa la inspección, aparecerá un mensaje correspondiente en pantalla. Si esto se produce, póngase en contacto con el distribuidor donde adquirió el programa para más información.

3.2.2.4. Selección de un archivo llave de licencia

Si dispone de un archivo llave de licencia para Kaspersky Anti-Virus for Windows Servers, el Asistente le preguntará si desea instalarlo. En ese caso, utilice el botón **Examinar** y seleccione el archivo llave de licencia (con extensión.key) en la ventana de selección de archivos.

Después de instalar con éxito la llave, aparecerá la información de licencia en la parte inferior de la ventana: nombre del titular del software registrado, número de

licencia, tipo de licencia (completa, prueba-beta, evaluación, etc.), así como la fecha de caducidad de la llave.

3.2.2.5. Fin de la activación del programa

El Asistente de configuración le informará de que el programa ha sido activado con éxito. También muestra la información de la llave de licencia instalada: nombre del titular del software registrado, número de licencia, tipo de licencia (completa, prueba-beta, evaluación, etc.), así como la fecha de caducidad de la llave.

3.2.3. Configuración de la actualización

La calidad de la protección de su equipo depende directamente de la actualización regular de las bases de aplicación y de los módulos de programa. En esta ventana, el Asistente de configuración le pide que seleccione el modo de actualización del programa y que configure la planificación.

- **Automático.** Kaspersky Anti-Virus comprueba en los orígenes de actualizaciones la presencia de actualizaciones a intervalos especificados. Los análisis pueden ser configurados para realizarse con mayor frecuencia durante epidemias de virus, y con menor frecuencia el resto del tiempo. Si encuentra nuevas actualizaciones, las descarga e instala en el equipo. Es la configuración predeterminada.
- **Cada 2 hora(s).** Las actualizaciones se ejecutarán automáticamente de acuerdo con la planificación definida. Para configurar las propiedades de planificación, haga clic en **Cambiar**.
- **Manual.** Al elegir esta opción, tendrá que ejecutar las actualizaciones del programa manualmente.

Observe que las bases de aplicación y los módulos de programa incluidos con el software pueden estar ya desfasadas cuando instala el programa. Por ello, le recomendamos descargar las últimas actualizaciones del programa. Para ello, haga clic en **Actualizar ahora**. A continuación Kaspersky Anti-Virus for Windows Servers descargará las actualizaciones necesarias desde los puntos de actualización y las instalará en su equipo.

Si desea configurar las actualizaciones (configurar las propiedades de red, seleccionar el recurso desde donde se descargan las actualizaciones, definir la cuenta de ejecución de la tarea o activar la opción de distribución de las actualizaciones), haga clic en **Configuración**.

3.2.4. Planificación de un análisis antivirus

El análisis de zonas seleccionadas en su equipo en busca de objetos malintencionados es una de las claves para proteger equipo.

Quando instala Kaspersky Anti-Virus for Windows Servers, se crean tres tareas predeterminadas de análisis antivirus. En esta ventana, el Asistente de instalación le invita a configurar una tarea de análisis:

Objetos de inicio

De forma predeterminada, Kaspersky Anti-Virus analiza automáticamente los objetos de inicio cuando arranca. Puede configurar los parámetros de planificación en otra ventana, haga clic en **Cambiar**.

Zonas críticas

Para poder analizar automáticamente las zonas críticas de su equipo (memoria del sistema, objetos de inicio, sectores de arranque, carpetas del sistema Microsoft Windows), active la casilla apropiada. Para configurar las propiedades de planificación, haga clic en **Cambiar**.

La configuración predeterminada para este análisis automático está desactivada.

Mi PC

Para ejecutar un análisis antivirus completo de su equipo automáticamente, active la casilla correspondiente. Para configurar las propiedades de planificación, haga clic en **Cambiar**.

De forma predeterminada, la ejecución planificada de esta tarea está desactivada. Sin embargo, le recomendamos ejecutar un análisis antivirus completo del servidor inmediatamente después de instalar el programa.

3.2.5. Restricciones de acceso al programa

Kaspersky Anti-Virus le da opción para proteger el programa con contraseña, dado que muchas personas pueden utilizar el mismo equipo y muchos programas malintencionados podrían intentar desactivar la protección. El uso de una contraseña permite proteger el programa contra intentos no autorizados de desactivación o modificación de sus parámetros.

Para activar la protección con contraseña, active la casilla **Activar la protección con contraseña** y complete los campos **Contraseña** y **Confirmar contraseña**.

Debajo, especifique el área que desea proteger con contraseña:

- Todas las operaciones (excepto notificaciones de eventos peligrosos).**
Pedir la contraseña si el usuario intenta cualquier acción en el programa salvo en respuesta a notificaciones de detección de objetos peligrosos.
- Operaciones seleccionadas:**
 - Guardar la configuración del programa:** solicita una contraseña cuando un usuario intenta guardar los cambios en la configuración del programa.
 - Salir del programa:** solicita una contraseña si un usuario intenta cerrar el programa.
 - Parada/Pausa de componentes de protección o de tareas de análisis antivirus:** solicita una contraseña si un usuario intenta suspender o desactivar completamente cualquier componente de protección o tarea de análisis antivirus.

3.2.6. Fin del Asistente de configuración

La última ventana del Asistente presenta un mensaje informándole que el programa ha sido instalado y configurado con éxito. Para iniciar la aplicación inmediatamente, active la casilla **Iniciar el producto**.

Si algo va mal durante la instalación, por ejemplo un problema de incompatibilidad con otra aplicación antivirus, se le invita a reiniciar su equipo.

3.3. Instalación del programa desde la línea de comandos

Para instalar Kaspersky Anti-Virus 6.0 for Windows Servers, escriba lo siguiente en la línea de comandos:

```
msiexec /i <nombre_paquete>
```

Se abre el Asistente de instalación (ver 3.1 pág. 23). Después de instalar el programa, debe reiniciar el equipo.

Para realizar una instalación desatendida de la aplicación (sin ejecutar el Asistente de instalación), escriba:

```
msiexec /i <nombre_paquete> /qn
```

Esta opción requiere reiniciar su equipo manualmente después de terminar la instalación. Para reiniciar automáticamente desde la línea de comandos, escriba:

```
msiexec /i <nombre_paquete> ALLOWREBOOT=1 /qn
```

Observe que se producirá un reinicio automático en modo desatendido (parámetro /qn).

Para instalar la aplicación con una contraseña de desinstalación, escriba:

```
msiexec /i <nombre_paquete> KLUNINSTPASSWD=*****, en  
caso de instalación interactiva;
```

```
msiexec /i <nombre_paquete> KLUNINSTPASSWD=*****  
/qn, en caso de instalación desatendida sin reinicio del sistema;
```

```
msiexec /i <nombre_paquete> KLUNINSTPASSWD=*****  
ALLOWREBOOT=1 /qn, en caso de instalación desatendida con  
reinicio del sistema;
```

Si instala Kaspersky Anti-Virus en modo desatendido, el archivo *setup.ini* le da acceso a parámetros de instalación generales de la aplicación (ver A.4 pág. 191), el archivo de configuración *install.cfg* (ver 13.7 pág. 179), y el archivo llave de licencia. Observe que estos archivos deben ubicarse en la misma carpeta que el paquete de instalación de Kaspersky Anti-Virus.

3.4. Procedimiento de instalación del Objeto de directiva de grupo

Esta característica es compatible con equipos que ejecutan Microsoft Windows 2000 o superior.

El **Editor de objetos de directiva de grupo** le permite instalar, actualizar y desinstalar Kaspersky Anti-Virus en estaciones de trabajo de su organización dentro del mismo dominio, sin necesidad de utilizar Kaspersky Administración Kit.

3.4.1. Instalación del programa

Para instalar Kaspersky Anti-Virus:

1. Cree una carpeta compartida en el equipo que actúa como controlador de dominio y copie a ella el paquete de instalación (*.msi*) de Kaspersky Anti-Virus.

También puede copiar el archivo *setup.ini*, que contiene los parámetros de instalación generales de la aplicación (ver A.4 pág. 191), el archivo

de configuración *install.cfg* (ver 13.7 pág. 179), y el archivo llave de licencia.

2. Abra el **Editor de objetos de directiva de grupo** con MMC (para obtener más información acerca de los Objetos de directiva de grupo, consulte la Ayuda de Microsoft Windows Server).
3. Cree un nuevo paquete. Para ello, en el árbol de consola, seleccione **Objeto de directiva de grupo/ Configuración del equipo/Configuración de software/ Instalación de software** y haga clic en el comando **Nuevo/ Paquete** en el menú contextual.

En la ventana abierta, especifique la ruta de la carpeta compartida con el programa instalador Anti-Virus (ver 1). Elija **Asignar** en el cuadro de diálogo **Seleccionar el método de despliegue** y haga clic en **Aceptar**.

La directiva de grupo entrará en acción en cada estación de trabajo, la próxima vez que el equipo se registre en el dominio. A continuación, Kaspersky Anti-Virus se instalará en todos estos equipos.

3.4.2. Actualización del programa

Para actualizar Kaspersky Anti-Virus:

1. Copie el paquete de instalación que contiene la actualización de Kaspersky Anti-Virus en formato *.msi* a la carpeta compartida.
2. Abra el **Editor de objetos de directiva de grupo** y cree un nuevo paquete siguiendo los pasos anteriores.
3. Seleccione el nuevo paquete y seleccione **Propiedades** en el menú contextual. En la ventana de propiedades del paquete, abra la ficha **Actualizaciones** y especifique el paquete que contiene el instalador de la versión anterior de Kaspersky Anti-Virus. Para instalar la actualización de Kaspersky Anti-Virus y conservar los parámetros de protección, seleccione una variante de actualización de la versión anterior.

La directiva de grupo entrará en acción en cada estación de trabajo, la próxima vez que el equipo se registre en el dominio.

Observe que no es posible actualizar Kaspersky Anti-Virus en equipos con Microsoft Windows 2000 Server, utilizando el Editor de objetos de directiva de grupo.

3.4.3. Desinstalación del programa

Para desinstalar Kaspersky Anti-Virus:

1. Abra el **Editor de objetos de directiva de grupo**.
2. Para ello, en el árbol de consola, seleccione **Objeto de directiva de grupo/ Configuración del equipo/ Configuración de software/ Instalación de software**.

Seleccione el paquete Kaspersky Anti-Virus en la lista. Abra el menú contextual y seleccione el comando **Todas las tareas/ Quitar**.

En el cuadro de diálogo **Eliminar programa**, seleccione **Desinstalar inmediatamente el software de usuarios y equipos** para desinstalar Kaspersky Anti-Virus en el próximo reinicio del equipo.

3.5. Actualización de la versión 5.0 a la versión 6.0

Si el Vigilante de Office de Kaspersky Anti-Virus 5.0 for Windows File Servers está instalado en su servidor, puede actualizarlo a Kaspersky Anti-Virus 6.0 for Windows Servers.

Después de iniciar el programa de instalación de Kaspersky Anti-Virus 6.0, tendrá la opción de desinstalar primero la versión 5.0 ya instalada del producto. Cuando la desinstalación del programa termine, deberá reiniciar su equipo para que comience la instalación de la versión 6.0.

Advertencia:

Si instala Kaspersky Anti-Virus 6.0 for Windows Servers por encima de una versión anterior, desde una carpeta de red protegida con contraseña, apunte lo siguiente. Después de desinstalar la versión 5.0 de la aplicación y reiniciar su equipo, el programa de instalación no le autorizará el acceso a la carpeta de red del paquete de instalación. Por tanto, el programa de instalación quedará interrumpido. Para instalar el programa correctamente, ejecute el instalador únicamente desde una carpeta local.

CAPÍTULO 4. INTERFAZ DEL PROGRAMA



Kaspersky Anti-Virus for Windows Servers dispone de una interfaz clara y amigable. Este capítulo describe sus características básicas.

- Icono de la barra del sistema (ver 4.1 pág. 36)
- Menú contextual (ver 4.2 pág. 37)
- Ventana principal (ver 4.3 pág. 38)
- Ventana de configuración del programa (ver 4.4 pág. 40)




4.1. Icono de la barra del sistema

Justo después de instalar Kaspersky Anti-Virus for Windows Servers, su icono aparecerá en la barra del sistema.

Este icono es una especie de indicador de las operaciones de Kaspersky Anti-Virus for Windows Servers. Refleja el estado de protección y muestra un número de funciones básicas realizadas por el programa.

Si el icono se encuentra activo  (color), significa que su equipo está protegido. Si el icono se encuentra inactivo  (blanco y negro), significa que la protección en tiempo real está desactivada.

El icono de Kaspersky Anti-Virus for Windows Servers cambia de acuerdo con la operación realizada:

	Análisis en curso de un archivo abierto, guardado o ejecutado directamente o por otro programa.
	la actualización de firmas y módulos para Kaspersky Anti-Virus está en curso.
	Ocurrió un error en alguno de los componentes de Kaspersky Anti-Virus.

El icono también facilita el acceso a las funciones básicas de la interfaz del programa: el menú contextual (ver 4.2 pág. 37) y la ventana principal (ver 4.3 pág. 38).

Para abrir el menú contextual, haga clic con el botón derecho en el icono del programa.

Para abrir la ventana principal de Kaspersky Anti-Virus for Windows Servers en la sección **Protección** (la pantalla predeterminada cuando abre el programa), haga doble clic en el icono del programa. Si sólo hace clic, la ventana principal se muestra con la última sección abierta la última vez que cerró el programa.

4.2. Menú contextual

Puede ejecutar tareas de protección básicas desde el menú contextual (ver Figura 1).



Figura 1. Menú contextual

El menú de Kaspersky Anti-Virus for Windows Servers ofrece los elementos siguientes:

Analizar Mi PC: realiza un análisis completo del equipo. Se analizan los archivos de todas las unidades, incluso en los medios extraíbles.

Análisis antivirus: selecciona objetos y ejecuta su análisis antivirus. De forma predeterminada, la lista contiene un cierto número de entradas, como la carpeta Inicio, las bases de correo, todas las unidades del equipo, etc. Puede agregar y seleccionar archivos de la lista y ejecutar el análisis antivirus.

Actualizar: descarga actualizaciones de los módulos de programa y firmas de amenazas y los instala en su equipo.

Activar: activa el programa. Debe activar su versión de Kaspersky Internet Security para darse de alta como usuario registrado y beneficiarse de todas las funciones de la aplicación y servicios del Soporte técnico. Esta opción de menú sólo está disponible si el programa no está activado.

Configuración: muestra y configura los parámetros de Kaspersky Anti-Virus for Windows Servers.

Abrir Kaspersky Anti-Virus – abre la ventana principal del programa (ver 4.3 pág. 38).

Suspender / Reanudar la protección: desactiva temporalmente o activa el componente Antivirus de archivos. (ver 2.2.1 pág. 17). Esta opción no afecta a las actualizaciones del programa ni las tareas de análisis antivirus.

Salir: cierra Kaspersky Anti-Virus for Windows Servers (al seleccionar esta opción, la aplicación se descarga de la RAM del equipo).

Si una tarea de búsqueda de virus está en ejecución, su nombre aparece en el menú contextual con una barra de progreso porcentual. Si selecciona la tarea, podrá abrir la ventana de informe para conocer sus resultados.

4.3. Ventana principal del programa

La ventana principal de Kaspersky Anti-Virus for Windows Servers (ver Figura 2) puede dividirse en dos partes funcionales:

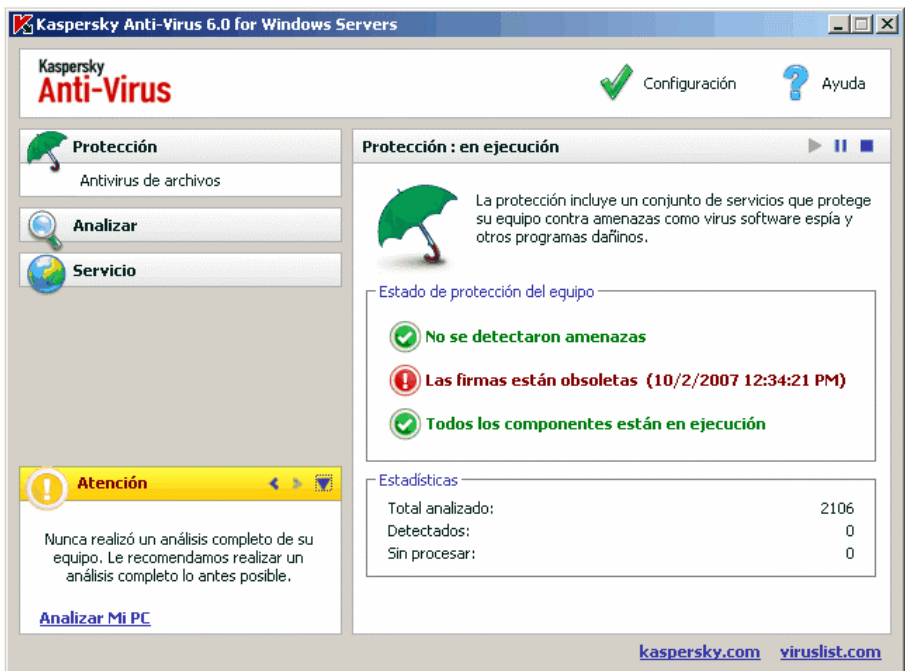
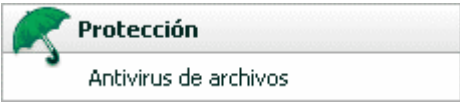
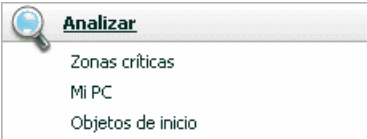


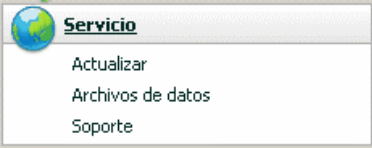
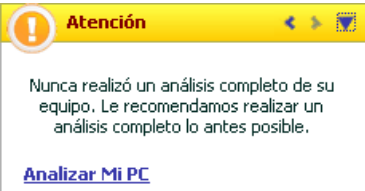
Figura 2. Ventana principal de Kaspersky Anti-Virus for Windows Servers

- la parte izquierda de la ventana, el panel de exploración, le conduce de forma rápida y sencilla a todos los componentes, tareas de análisis antivirus o actualización, y herramientas de soporte del programa;
- En la parte derecha de la ventana, el panel de información, contiene información sobre el componente de protección seleccionado en la parte izquierda y muestra los parámetros de cada uno, con herramientas para realizar análisis antivirus, trabajar con archivos en cuarentena y de respaldo, administrar llaves de licencia, etc.

Cuando selecciona una entrada en la parte izquierda de la ventana, la parte derecha muestra la información correspondiente a su selección.

Examinaremos ahora los elementos del panel de exploración de la ventana principal con más detalle.

Sección de la ventana principal	Descripción
<p>Esta ventana está principalmente destinada a informarle acerca del estado de protección de su equipo. La sección Protección está prevista precisamente para ello.</p> 	<p>Aquí podrá encontrar información general acerca del funcionamiento de Kaspersky Anti-Virus for Windows Servers, para comprobar que todos los componentes se ejecutan correctamente y examinar las estadísticas generales.</p>
<p>Para analizar su equipo en busca de archivos o programas malintencionados, utilice la sección Analizar en la ventana principal.</p> 	<p>Esta sección contiene una lista de objetos en los que puede buscar virus.</p> <p>Las tareas más comunes e importantes se incluyen en la sección. Se incluyen tareas de análisis antivirus para zonas críticas, programas de inicio así como un análisis del equipo completo.</p>

<p>La sección Servicio incluye características avanzadas de Kaspersky Anti-Virus for Windows Servers.</p> 	<p>También puede actualizar el programa, mostrar informes de rendimiento de cualquiera de los componentes de Kaspersky Anti-Virus, trabajar con los objetos en cuarentena y en la zona de respaldo, revisar la información de soporte técnico, crear un disco de emergencia y administrar llaves de licencia.</p>
<p>La sección de comentarios y consejos le acompaña mientras utiliza el programa.</p> 	<p>Esta sección siempre ofrece la lectura de consejos o de mejoras del nivel de protección del servidor. Encontrará también comentarios acerca del rendimiento actual del programa y sus parámetros.</p>

Cada elemento del panel de exploración se complementa con un menú contextual especializado. Así, el menú contiene entradas para el componente Antivirus de archivos, herramientas de ayuda para su rápida configuración y administración, así como para los informes. Existe un menú avanzado para tareas de análisis antivirus y de actualización que le permite crear su propia tarea, a partir de otra seleccionada.

Para modificar la apariencia del programa puede crear y utilizar sus propias imágenes y combinaciones de color.

4.4. Ventana de configuración del programa

Puede abrir la ventana de configuración de Kaspersky Anti-Virus for Windows Servers desde la ventana principal (ver 4.3 pág. 38). Para ello, haga clic en Configuración en la parte superior.

La ventana de configuración (ver Figura 3) tiene una presentación similar a la ventana principal de la aplicación.

- La parte izquierda de la ventana le da acceso rápido y directo a los parámetros del componente Antivirus de archivos, a las tareas de búsqueda antivirus, de actualización y a las herramientas del programa;
- La parte derecha de la ventana contiene la lista detallada de los parámetros del elemento seleccionado en la izquierda de la ventana.

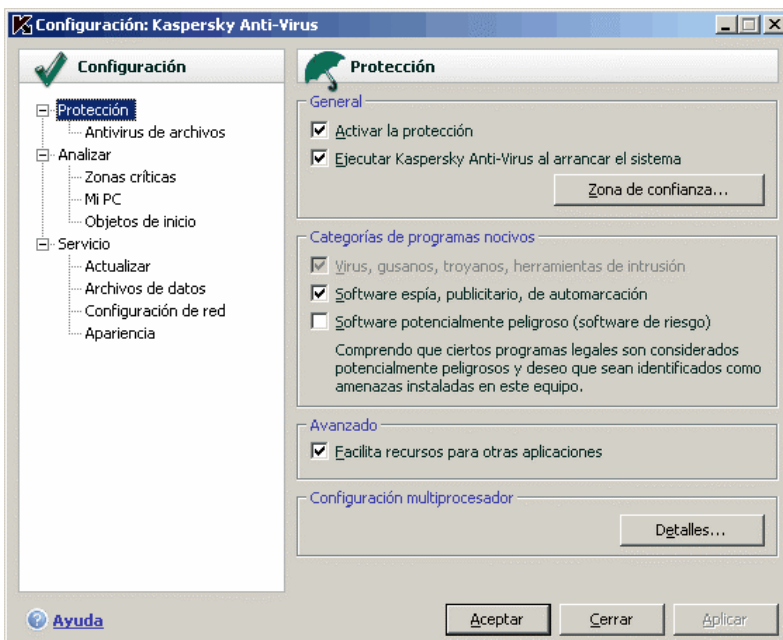


Figura 3. Ventana de configuración de Kaspersky Anti-Virus for Windows Servers

Cuando selecciona cualquier sección, componente o tarea en la parte izquierda de la ventana de configuración, la parte derecha presenta los parámetros básicos asociados. Para configurar parámetros avanzados, puede abrir una segunda y tercera ventana de configuración. Encontrará una descripción detallada de los parámetros del programa en las secciones correspondientes.

CAPÍTULO 5. PRIMEROS PASOS

Uno de los principales objetivos de los expertos de Kaspersky Lab al diseñar Kaspersky Anti-Virus for Windows Servers fue ofrecer una configuración óptima de todas las opciones del programa.

Para facilitarle sus primeros pasos, hemos reunido todas las etapas de configuración preliminar en un mismo Asistente de configuración (ver 3.2 pág. 26) que se inicia tan pronto como se instala el programa. Siguiendo las instrucciones del Asistente, podrá activar el programa, configurar los parámetros de actualización y ejecución del análisis antivirus y proteger con contraseña el acceso al programa.

Después de instalar e iniciar el programa, le recomendamos realizar los pasos siguientes:

- Compruebe el estado actual de la protección (ver 5.1 pág. 42) para asegurarse de que Kaspersky Anti-Virus for Windows Servers se ejecuta en el nivel apropiado.
- Actualice el programa (ver 5.5 pág. 50) si el Asistente de configuración no lo hizo automáticamente después de instalar el programa.
- Analice el equipo (ver 5.2 pág. 48) en busca de virus.

5.1. ¿Cuál es el estado de protección de mi equipo?

Encontrará información resumida acerca de la protección de su equipo en la ventana principal de la aplicación, en la entrada **Protección**. El *estado actual de la protección* del equipo y *las estadísticas de rendimiento general* del programa se muestran ahí.


El **estado de protección** muestra el estado actual de protección de su equipo con indicadores especiales (ver 5.1.1 pág. 42). La sección Estadísticas (ver 5.1.2 pág. 46) analiza la sesión actual del programa.

5.1.1. Indicadores de protección

El **estado de la protección** viene determinado por tres indicadores (ver Figura 4), que reflejan el grado de protección de su equipo en un momento dado, a la

vez que muestran los problemas en la configuración y en la actividad del programa.

Cada indicador tiene tres posibles presentaciones:

-  – *la situación es normal*; el indicador muestra que el estado de protección del equipo es adecuado, que no hay problemas en la configuración o la actividad del programa.

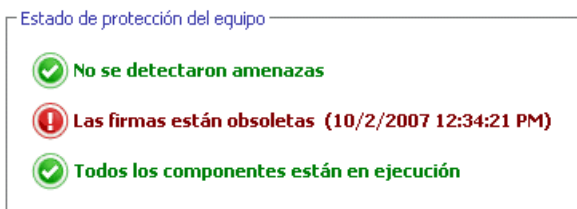






Figura 4. Indicadores que reflejan el estado de protección del equipo

-  – *existen una o varias alteraciones* en el funcionamiento de Kaspersky Anti-Virus for Windows Servers, comparado con el nivel recomendado, que podría afectar a la seguridad de sus datos. Preste atención a las acciones recomendadas por los expertos de Kaspersky Lab, indicadas por vínculos.
-  – *el estado de seguridad del equipo es crítico*. Siga de cerca las recomendaciones para mejorar la protección de su equipo. Las acciones recomendadas se facilitan con vínculos.



Examinaremos con más detalle ahora los indicadores de protección y las situaciones que cada uno describe.


El primer indicador sirve para reflejar la presencia de archivos y programas malintencionados en su equipo. Los tres valores del indicador tienen el significado siguiente:

	<p><i>No se detectaron amenazas</i></p> <p>Kaspersky Anti-Virus for Windows Servers no ha detectado ningún archivo o programa peligroso en su equipo.</p>
	<p><i>Todas las amenazas han sido neutralizadas</i></p> <p>Kaspersky Anti-Virus for Windows Servers ha neutralizado todos los archivos y programas infectados con virus y eliminado los que no pudo neutralizar.</p>




	<p><i>Se detectaron amenazas</i></p> <p>Su equipo corre el riesgo de infección. Kaspersky Anti-Virus for Windows Servers ha detectado programas malintencionados (virus, troyanos, gusanos, etc.) que deben ser neutralizados. Para ello, utilice el vínculo Neutralizar todo. Haga clic en el vínculo Detalles para obtener información más detallada acerca de los objetos malintencionados.</p>
---	---

El segundo indicador muestra el grado de eficacia de la protección de su equipo. El indicador toma uno de los valores siguientes:

	<p><i>Fecha de firmas: (fecha, hora)</i></p> <p>Tanto la aplicación y las firmas de amenazas utilizadas por Kaspersky Anti-Virus for Windows Servers son las versiones más recientes.</p>
	<p><i>Las firmas han caducado</i></p> <p>Los módulos de programa y las bases de aplicación de Kaspersky Anti-Virus for Windows Servers no han sido actualizadas desde varios días. Corre el riesgo de infectar su equipo con nuevos programas malintencionados aparecidos desde la última actualización del programa. Le recomendamos actualizar Kaspersky Anti-Virus for Windows Servers. Para ello, utilice el vínculo Actualizar.</p>
	<p><i>Las firmas de amenazas están total o parcialmente dañadas</i></p> <p>Las firmas de amenazas están parcialmente dañadas. En este caso, se recomienda ejecutar de nuevo el programa de actualizaciones. Si el mismo mensaje de error vuelve a aparecer, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab.</p>
	<p><i>Reinicie el equipo</i></p> <p>Debe reiniciar el sistema para que el programa se ejecute correctamente. Guarde y cierre todos los archivos con los que está trabajando y utilice el vínculo Reiniciar el equipo.</p>
	<p><i>Las actualizaciones del programa están desactivadas</i></p> <p>El servicio de actualización de firmas de amenazas y módulos de programas está desactivado. Para preservar la protección en tiempo real, le recomendamos autorizar las actualizaciones.</p>

	<p><i>Las firmas están obsoletas</i></p> <p>Kaspersky Anti-Virus for Windows Servers no ha sido actualizado desde hace tiempo. Está poniendo sus datos seriamente en peligro. Actualice el programa tan pronto como sea posible. Para ello, utilice el vínculo <u>Actualizar</u>.</p>
	<p><i>Las firmas de amenazas están dañadas</i></p> <p>Los archivos de firmas de amenazas están completamente dañados. En este caso, se recomienda ejecutar de nuevo el programa de actualizaciones. Si el mismo mensaje de error vuelve a aparecer, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab.</p>

El tercer indicador muestra la actividad actual del programa. El indicador toma uno de los valores siguientes:

	<p><i>Todos los componentes están en ejecución</i></p> <p>Kaspersky Anti-Virus for Windows Servers protege su equipo contra todas las vías de penetración de programas malintencionados.</p>
	<p><i>La protección antivirus no está instalada</i></p> <p>Cuando instaló Kaspersky Anti-Virus for Windows Servers, no se instaló ninguno de los componentes de supervisión. Esto significa que sólo puede buscar virus. Para una seguridad máxima, conviene instalar los componentes de protección en su equipo.</p>
	<p><i>Todos los componentes están en pausa</i></p> <p>El componentes de protección está en pausa. Para restaurar los componentes, seleccione Reanudar la protección en el menú contextual: para ello, haga clic en el icono de la barra del sistema.</p>
	<p><i>Todos los componentes están desactivados</i></p> <p>La protección está completamente desactivada. El componente de protección no está en ejecución. Para restaurar los componentes, seleccione Reanudar la protección en el menú contextual: para ello, haga clic en el icono de la barra del sistema.</p>
	<p><i>Algunos componentes han tenido fallos</i></p> <p>El componente de Kaspersky Anti-Virus ha encontrado errores internos. Si esto ocurre, le recomendamos activar el componente o reiniciar el</p>

	equipo ya que es posible que los controladores de componentes tengan que ser registrados en el sistema después de su actualización.
--	---

5.1.2. Estado de Kaspersky Anti-Virus for Windows Servers



Para saber cómo Kaspersky Anti-Virus for Windows Servers protege su sistema de archivos, o ver el progreso de la tarea de análisis antivirus o de actualización de las firmas de amenazas, abra la sección correspondiente de la ventana principal del programa.

Por ejemplo, para ver el estado actual del componente Antivirus de archivos, seleccione **Antivirus de archivos** en la parte izquierda de la ventana principal del programa. La parte derecha de la ventana mostrará información completa sobre la actividad del componente.

En el caso del componente Antivirus de archivos, la parte derecha contiene la **barra de estado**, el cuadro **Estado** y el cuadro **Estadísticas**.

Para el componente Antivirus de archivos, la *barra de estado* se muestra como sigue:



- *Antivirus de archivos: en ejecución* – la protección de archivos está activa dentro del nivel seleccionado (ver 7.1 pág. 71).
- *Antivirus de archivos: suspendido*: el componente Antivirus de archivos ha sido desactivado durante un cierto tiempo determinado. El componente reanudará las operaciones automáticamente después de concluir el tiempo asignado, o después de reiniciar el programa. También puede reanudar la protección de archivos manualmente, con el botón  ubicado en la barra de estado.
- *Antivirus de archivos: desactivado*: el componente ha sido detenido por el usuario. Puede reanudar la protección de archivos manualmente, con el botón  ubicado en la barra de estado.
- *Antivirus de archivos: disfunción*: la protección de archivos no está disponible por alguna razón.
- *Antivirus de archivos: desactivado (error)*: el componente encontró un error.

Si un componente presenta un error, intente reiniciarlo. Si el reinicio produce un error, revise el informe del componente, donde puede aparecer la razón del fallo. Si no puede corregir el problema, guarde el

informe del componente con **Acciones** → **Guardar como** y póngase en contacto con el Soporte técnico de Kaspersky Lab.

Los parámetros de funcionamiento de un componente se indican en la sección **Estado**:

- *Antivirus de archivos*: estado actual del componente (en ejecución, desactivado, suspendido, etc.).
- *Nivel de seguridad*: conjunto de parámetros de funcionamiento del componente, de acuerdo con los cuales el programa protege los archivos. De forma predeterminada, el nivel de seguridad **Recomendado** está seleccionado y analiza tan sólo los objetos del sistema de archivos expuestos a infección. Por ejemplo, los archivos ejecutables (.exe).
- La *acción* tomada cuando se detecta un objeto peligroso

No existe cuadro de **Estado** para las tareas de análisis antivirus de actualización. El nivel de seguridad, la acción aplicada a los programas peligrosos en el caso de tareas de análisis antivirus y el modo de ejecución de las actualizaciones aparecen en el recuadro **Configuración**.

El recuadro **Estadísticas** contiene información sobre el funcionamiento de los componentes de protección, las actualizaciones o las tareas de análisis antivirus.

5.1.3. Estadísticas de funcionamiento del programa

Las **estadísticas del programa** se encuentran en el cuadro **Estadística** de la sección **Protección** en la ventana principal del programa (ver Figura 5), y muestran información general sobre la protección del equipo, registrada desde el momento en que instaló Kaspersky Anti-Virus for Windows Servers.



Estadísticas	
Archivos analizados:	168
Detectados:	0
Último analizado:	0

Figura 5. El cuadro de estadísticas generales del programa

Haga clic en cualquier punto dentro de la zona para ver un informe con información detallada. Las fichas muestran:

- Información sobre objetos encontrados (ver 11.3.2 pág. 129) y el estado atribuido a éstos
- Informe de eventos (ver 11.3.3 pág. 130)

- Estadísticas generales de análisis (ver 11.3.4 pág. 131) de su equipo
- Parámetros de rendimiento del programa (ver 11.3.5 pág. 131)

5.2. Cómo analizar el equipo en busca de virus

Después de la instalación, el programa le informará sistemáticamente (con una nota especial en la parte inferior izquierda de la ventana del programa) de que su equipo no ha sido analizado todavía, recomendándole hacerlo inmediatamente.

Kaspersky Anti-Virus incluye una tarea predeterminada de análisis antivirus. Se encuentra en la ventana principal del programa en la sección **Analizar**.

Después de seleccionar la tarea **Mi PC**, obtendrá las estadísticas del último análisis del equipo y los parámetros de tarea: qué nivel de protección se seleccionó y qué acciones van a tomarse para objetos peligrosos.

Para analizar su equipo contra programas malintencionados,

1. Abra la ventana principal del programa y seleccione la tarea **Mi PC** en la entrada **Analizar**.
2. Haga clic en el botón **Analizar**.

A continuación se ejecutará el análisis del servidor, con los detalles presentados en una ventana especial. Cuando hace clic en **Cerrar**, la ventana de progreso de la instalación queda oculta pero el análisis no se detiene.

5.3. Cómo analizar zonas críticas del equipo

Es extremadamente importante asegurar las zonas críticas de su equipo para garantizar su buen funcionamiento. Existe una tarea de análisis antivirus especial para estas zonas, que se encuentra en la ventana principal del programa, en la sección **Analizar**.

Después de seleccionar la tarea **Zonas críticas**, podrá consultar las estadísticas del último análisis del equipo y los parámetros de tarea: las estadísticas del último análisis de estas zonas; parámetros de tarea; nivel de protección seleccionado y acciones que se tomarán en caso de amenazas a la seguridad. También puede seleccionar las zonas críticas que desea analizar e iniciar inmediatamente un análisis antivirus de dichas zonas.

Para analizar las zonas críticas de su equipo contra programas malintencionados,

1. Abra la ventana principal del programa y seleccione la tarea **Zonas críticas** en la entrada **Analizar**.
2. Haga clic en el botón **Analizar**.

Al hacerlo, se ejecutará un análisis de las zonas seleccionadas, y los detalles aparecerán presentados en una ventana especial. Cuando hace clic en **Cerrar**, la ventana de progreso de la instalación queda oculta pero el análisis no se detiene.

5.4. Cómo analizar un archivo, carpeta o disco en busca de virus

En algunos casos es necesario analizar objetos individuales en busca de virus, pero no el equipo completo: por ejemplo, en el caso de discos duros. Puede seleccionar el objeto para analizar con las herramientas estándar de Microsoft Windows Server (por ejemplo, en la ventana del **Explorador** o en el **Escritorio**, etc.).

Para analizar un objeto,

Sitúe el cursor sobre el nombre del objeto seleccionado, abra el menú contextual de Microsoft Windows Server con un clic derecho y elija **Buscar virus** (ver Figura 6).

A continuación se ejecutará un análisis del objeto seleccionado, con los detalles presentados en una ventana especial. Cuando hace clic en **Cerrar**, la ventana de progreso de la instalación queda oculta pero el análisis no se detiene.

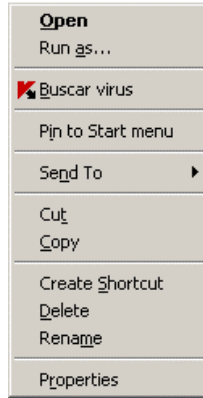


Figura 6. Análisis antivirus de un objeto seleccionado con el menú contextual estándar de Microsoft Windows Server

5.5. Cómo actualizar el programa

Kaspersky Lab actualiza las bases de aplicación y los módulos de programa de Kaspersky Anti-Virus for Windows Servers a partir de servidores de actualización especializados.

Los servidores de actualización de Kaspersky Lab son sitios Internet de Kaspersky Lab donde se almacenan las actualizaciones del programa.

Advertencia:

Necesita una conexión Internet para actualizar Kaspersky Anti-Virus for Windows Servers.

De forma predeterminada, Kaspersky Anti-Virus for Windows Servers busca automáticamente las actualizaciones en los servidores de Kaspersky Lab. Si el servidor contiene actualizaciones recientes, Kaspersky Anti-Virus las descarga e instala en segundo plano.

Para actualizar Kaspersky Anti-Virus for Windows Servers manualmente,

seleccione la entrada **Actualizar** en la entrada **Servicio** de la ventana principal del programa y haga clic en **Actualizar ahora** en la parte derecha de la ventana.

A continuación, Kaspersky Anti-Virus for Windows Servers ejecutará el proceso de actualización y mostrará sus detalles en una ventana especial.

5.6. Qué hacer si la protección no funciona

Si se producen problemas o errores del componente Antivirus de archivos, compruebe su estado. Si el estado del componente es *no está en ejecución* o *error de operación*, intente reiniciar la aplicación.

Si no es posible resolver el problema después de reiniciar el programa, le recomendamos corregir los posibles errores con la herramienta de restauración (**Inicio** → **Programas** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Modificar, Reparar o Eliminar**).

Si el procedimiento de restauración no da resultado, póngase en contacto con el Soporte técnico de Kaspersky Lab. Puede ser necesario guardar a un archivo un informe de la actividad del componente o de toda la aplicación, para enviarlo al Soporte técnico donde puedan estudiarlo.

Para guardar el informe a un archivo:

1. Seleccione Antivirus de archivos en la entrada **Protección** de la ventana principal del programa y haga clic en cualquier punto del cuadro **Estadísticas**.
2. Haga clic en **Guardar como** y en la ventana abierta, especifique el nombre del archivo donde va guardar el informe de actividad del componente.

Para guardar un informe de arranque o del estado de los componentes de Kaspersky Anti-Virus de una sola vez (Antivirus de archivos, tareas de análisis antivirus, características de soporte):

1. Seleccione la entrada **Protección** en la ventana principal del programa y haga clic en cualquier punto del cuadro **Estadísticas**.

o

Haga clic en Todos los informes en la ventana de informe de cualquier componente. A continuación, la ficha **Informes** mostrará los informes de todos los componentes del programa.

2. Haga clic en **Guardar como** y en la ventana abierta, especifique el nombre del archivo donde va guardar el informe de actividad del componente.

CAPÍTULO 6. SISTEMA DE ADMINISTRACIÓN DE LA PROTECCIÓN

Kaspersky Anti-Virus for Windows Servers permite administrar la protección con múltiples tareas.

- Activar, desactivar y suspender (ver 6.1 pág. 52) el programa.
- Definir los tipos de programas peligrosos (ver 6.2 pág. 56) contra los que Kaspersky Anti-Virus for Windows Servers protegerá su equipo.
- Crear una lista de exclusiones (ver 6.3 pág. 57) para la protección.
- Crear sus propias tareas de análisis antivirus (ver 6.4 pág. 64).
- Planificar un análisis antivirus (ver 6.5 en la pág. 66).
- Configurar los parámetros de rendimiento (ver 6.6 pág. 68) para la protección del equipo.

6.1. Detener y reanudar la protección en su equipo

De forma predeterminada, Kaspersky Anti-Virus se ejecuta al arrancar el sistema y lo protege todo el tiempo que lo utiliza. Las palabras *Kaspersky Anti-Virus 6.0* en el ángulo superior derecho de la pantalla le permiten comprobarlo. Antivirus de archivos (ver 2.2.1 pág. 17) está en ejecución.

Puede desactivar la protección de Kaspersky Anti-Virus for Windows Servers.

Advertencia:

Kaspersky Lab recomienda fuertemente no desactivar la protección, porque podría causar la infección de su equipo y la pérdida de datos.

Observe que en este caso, la protección se describe en el contexto del componente Antivirus de archivos. La desactivación o suspensión no afecta al rendimiento de las tareas de análisis antivirus y las actualizaciones del programa.

6.1.1. Suspensión de la protección

La suspensión de la protección permite desactivar temporalmente el componente Antivirus de archivos.

Para suspender el funcionamiento de Kaspersky Anti-Virus for Windows Servers:

1. Elija **Suspender la protección** en el menú contextual del programa. (ver 4.2 en la página 37).
2. En la ventana **Suspender la protección** abierta (ver Figura 7), seleccione cuándo desea reanudar la protección:
 - **En <intervalo de tiempo>**: la protección se activará después de transcurrido el tiempo indicado. Utilice el menú desplegable para seleccionar el tiempo.
 - **En el próximo inicio del programa**: la protección se activará si abre el programa desde el menú Inicio o después de reiniciar el equipo (en el supuesto de que el programa esté configurado para iniciarse automáticamente al arrancar el equipo (ver 6.1.5 pág. 56).
 - **Sólo a petición del usuario**: la protección quedará desactivada hasta que la vuelva a iniciarla. Para activar la protección, seleccione **Reanudar la protección** desde el menú contextual del programa.

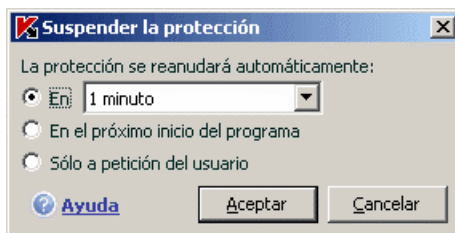



Figura 7. Ventana Suspender la protección

Sugerencia:

También puede interrumpir la protección de su equipo con uno de los métodos siguientes:

- Haga clic en **||** en la entrada Protección.
- Seleccione Salir en el menú contextual. En este caso, el programa será descargado de la memoria del equipo.

Si suspende la protección, el componente Antivirus de archivos se detendrá. Esto queda indicado por:

- El nombre deshabilitado (en gris) del componente Antivirus de archivos en la entrada **Protección** de la ventana principal.
- El icono deshabilitado (en gris) de la barra del sistema.
- El tercer indicador de protección (ver 5.1.1 en la página 42) en su equipo, que indica  **Todos los componentes están en pausa.**

6.1.2. Desactivación de la protección


La desactivación de la protección significa parar completamente el componente Antivirus de archivos. Las tareas de análisis antivirus y de actualización siguen funcionando en este modo.

Si la protección está completamente desactivada, sólo será posible activarla a petición del administrador. El componente Antivirus de archivos no se iniciará automáticamente después de rearrancar el sistema o reiniciar el programa. Recuerde que si Kaspersky Anti-Virus for Windows Servers causa un conflicto con otros programas instalados en su equipo, puede suspender el componente Antivirus de archivos o crear una lista de exclusión (ver 6.3 pág. 57).

Para desactivar toda la protección:

1. Abra la ventana de configuración de Kaspersky Anti-Virus y seleccione la entrada **Protección**.
2. Desactive la casilla **Activar la protección**.


Después de desactivar la protección, el componente Antivirus de archivos se detendrá. Esto queda indicado por:


1. El nombre deshabilitado (en gris) del componente Antivirus de archivos en la entrada **Protección** de la ventana principal.
2. El icono deshabilitado (en gris) de la barra del sistema.
3. El tercer indicador de protección (ver 5.1.1 en la página 42) en su equipo, que indica  **Todos los componentes están desactivados.**

6.1.3. Suspensión / Detención de la protección

Existen varios modos de detener el componente Antivirus de archivos, un análisis antivirus o una actualización. Antes de hacerlo, les recomendamos fuertemente reflexionar sobre las razones de esta detención. Es posible que pueda solucionar el problema de otro modo, por ejemplo, cambiando el nivel de seguridad. Si, por ejemplo, trabaja con una base de datos de la que sabe que no contiene virus, inclúyala simplemente a la lista de exclusiones (ver 6.3 pág. 57).


Para suspender el componente Antivirus de archivos, los análisis antivirus, y las tareas de actualización:


Seleccione el componente o tarea en la parte izquierda de la ventana principal y haga clic en  en la barra de estado.

El estado del componente o tarea cambia a **suspendido**. El componente o tarea quedará suspendido hasta que lo reanude con .

Cuando suspende el funcionamiento del componente o de una tarea, las estadísticas asociadas a la sesión actual de Kaspersky Anti-Virus, se guardan y seguirán utilizándose después de reanudar o actualizar el componente.

Para interrumpir el componente o tareas de protección:

Haga clic en  en la barra de estado. También puede detener el componente desde la ventana de configuración del programa al desactivar la casilla **Activar <nombre de componente>** en la sección **General**.

El estado del componente o tarea cambiará a *detenido (desactivado)*. El componente o tarea quedará detenido hasta que lo reactive con . En el caso de las tareas de análisis antivirus y actualización, podrá elegir las opciones siguientes: continuar la tarea interrumpida o volver a iniciarla desde el principio.

Cuando detiene el componente, se borran todas las estadísticas de operaciones anteriores, que son reemplazadas cuando se inicia de nuevo el componente.


6.1.4. Reanudación de la protección de su equipo

Después de haber suspendido o detenido la protección de su equipo, puede volver a habilitarla con alguno de los métodos siguientes:

- Desde el menú contextual.

Para ello, seleccione **Reanudar la protección**.

- Desde la ventana principal del programa.

Para ello, haga clic en  en la barra de estado de la sección **Protección** en la ventana principal.

El estado de protección cambia inmediatamente a *en ejecución*. El icono del programa en la barra del sistema queda habilitado (en color). El tercer indicador

de protección (ver 5.1.1 en la página 42) del equipo también le confirma que **Todos los componentes están activados**.



6.1.5. Salir del programa

Si tiene que cerrar Kaspersky Anti-Virus for Windows Servers, seleccione **Salir** desde el menú contextual del programa (ver 4.2 en la página 37). A continuación el programa se cerrará, dejando su equipo sin protección.

Tras cerrar el programa, puede activar de nuevo la protección del equipo abriendo Kaspersky Anti-Virus for Windows Servers (**Inicio** → **Programas** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Kaspersky Anti-Virus 6.0 for Windows Servers**).

La protección también puede reanudarse automáticamente al reiniciar el sistema operativo. Para habilitar esta característica, seleccione la sección **Protección** en la ventana de configuración del programa y active la casilla **Iniciar Kaspersky Anti-Virus al arrancar el sistema**.

6.2. Tipos de programas malintencionados supervisados

Kaspersky Anti-Virus for Windows Servers le protege contra varios tipos de programas malintencionados. En cualquier configuración, el programa siempre protege su equipo contra los tipos más peligrosos de programas malintencionados, como virus, troyanos y herramientas de intrusión. Estos programas pueden hacerle un daño significativo a su equipo. Para mejorar la seguridad de su equipo, puede ampliar la lista de amenazas detectadas por el programa al incluir más tipos de programas potencialmente peligrosos.

Para elegir contra qué programas malintencionados Kaspersky Anti-Virus for Windows Servers debe protegerle, seleccione la sección **Protección** en la ventana de configuración del programa (ver 4.4 pág. 40).

El cuadro **Categorías de programas nocivos** contiene tipos de amenazas (ver 1.1 pág. 9):

- Virus, gusanos, troyanos, herramientas de intrusión.** Se agrupan juntos los tipos de programas malintencionados más corrientes y peligrosos. Este sería el nivel mínimo admisible de seguridad. De acuerdo con las recomendaciones de los expertos de Kaspersky Lab, Kaspersky Anti-Virus siempre supervisa esta categoría de programas malintencionados.
- Software espía, publicitario, de automarcación.** Este grupo incluye software potencialmente peligroso que podría causar molestias a un usuario o daños importantes.
- Software potencialmente peligroso (software de riesgo).** Este grupo incluye programas que no son malintencionados ni peligrosos. Pero en ciertas circunstancias pueden utilizarse para dañar su equipo.

Los grupos enumerados cubren todo el espectro de amenazas detectadas por el programa cuando analiza objetos.

Si todos los grupos están seleccionados, Kaspersky Anti-Virus for Windows Servers ofrece el grado más completo de la protección antivirus en su equipo. Si el segundo y tercer grupo están desactivados, el programa sólo le protegerá contra los programas malintencionados más frecuentes. Esto no incluye los programas potencialmente peligrosos y otros que pueda tener instalados en su equipo y dañar sus archivos, robarle su dinero o consumir su tiempo.

Kaspersky Lab no recomienda deshabilitar la supervisión del segundo grupo. Si se produce la situación en la que Kaspersky Anti-Virus clasifica un programa como software de riesgo, pero sabe que no es peligroso, le recomendamos configurar una exclusión (ver 6.3 pág. 57).

6.3. Creación de una zona de confianza

Una *zona de confianza* es una lista de objetos creada por el administrador para que Kaspersky Anti-Virus for Windows Servers no los supervise. En otras palabras, se trata de un conjunto de programas excluidos de la protección.

El administrador crea una zona protegida basada en las propiedades de los archivos utilizados y de los programas instalados en el equipo. La creación de esta lista de exclusiones puede resultar necesaria, por ejemplo, si Kaspersky Anti-Virus for Windows Servers bloquea el acceso a un objeto o programa y está seguro de que dicho archivo o programa es absolutamente seguro.

Puede excluir del análisis archivos de determinados formatos, utilizar una máscara de archivos o excluir una zona (por ejemplo, una carpeta o un

programa), procesos de programa u objetos de acuerdo con la clasificación de la Enciclopedia del virus (el estado que el programa atribuye a los objetos durante un análisis).

Advertencia:

Los objetos excluidos no se toman en cuenta durante los análisis del disco o de la carpeta donde se encuentran. Sin embargo, si selecciona específicamente este objeto, la regla de exclusión no se aplicará.

Para crear una lista de exclusiones,

1. Abra la ventana de configuración de la aplicación y seleccione la entrada **Protección**.
2. Haga clic en **Zona de confianza** en la sección **General**.

Configure reglas de exclusión para objetos y cree una lista de aplicaciones de confianza en la ventana abierta (ver Figura 8).

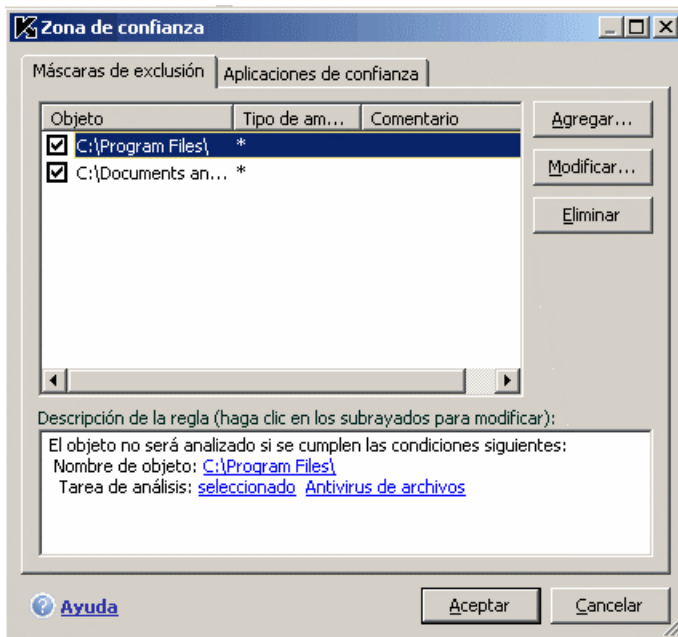


Figura 8. Creación de una zona de confianza

6.3.1. Reglas de exclusión

Las reglas de exclusión son conjuntos de condiciones que Kaspersky Anti-Virus for Windows Servers para saber que no debe analizar un objeto.

Puede excluir del análisis archivos de determinados formatos, utilizar una máscara de archivos o excluir una zona determinada, por ejemplo, una carpeta o un programa, procesos de programa u objetos de acuerdo con su clasificación en la Enciclopedia del virus.

El *Tipo de amenaza* (o veredicto) es el estado que Kaspersky Anti-Virus atribuye a un objeto durante el análisis. Un estado se determina a partir de la clasificación de programas malintencionados y potencialmente peligrosos que figura en la Enciclopedia de virus de Kaspersky Lab.

Un software potencialmente peligroso no tiene por sí mismo un comportamiento dañino, pero puede ser utilizado como componente auxiliar de un código malintencionado, porque contiene fallos y errores. En esta categoría se incluyen, por ejemplo, los programas de administración remota, clientes IRC, servicios FTP, herramientas genéricas para detener u ocultar procesos, interceptores de teclado, macros de contraseñas, software de automarcación, etc. Este tipo de software no se clasifica dentro de los virus. Puede dividirse en varios tipos, por ejemplo, software publicitario, bromas, software de riesgo, etc. (para obtener más información acerca de programas potencialmente peligrosos detectados por Kaspersky Anti-Virus for Windows Servers, consulte la Enciclopedia del virus en la dirección www.viruslist.com). Después del análisis, estos programas pueden acabar bloqueados. Dado que muchos de ellos son ampliamente utilizados por los usuarios, tiene la opción de excluirlos del análisis. Para ello, debe agregar el nombre o la máscara del objeto a la zona de confianza a partir de la clasificación de la Enciclopedia del virus.

Por ejemplo, utiliza con frecuencia un programa de administración remota durante su trabajo. Se trata un sistema de acceso remoto con el que puede trabajar desde un equipo a distancia. Kaspersky Anti-Virus for Windows Servers considera este tipo de actividad propias de aplicaciones potencialmente peligrosas y puede llegar a bloquearlas. Para evitar el bloqueo de la aplicación, debe crear una regla de exclusión que especifique el tipo de amenaza "not-a-virus:RemoteAdmin.Win32.RAdmin.22".

Cuando agrega una exclusión, se crea una regla que el componente Antivirus de archivos y las propias tareas de análisis antivirus utilizarán posteriormente. Puede crear reglas de exclusión en un cuadro de diálogo especial abierto desde la ventana de configuración del componente, a partir de la notificación de detección del objeto y desde la ventana del informe.

*Para agregar exclusiones a la ficha **Máscaras de exclusión**:*

1. Haga clic en **Agregar** en la ficha **Máscaras de exclusión**.

- En la ventana abierta (ver Figura 9), haga clic en el tipo de exclusión en la sección **Propiedades**:

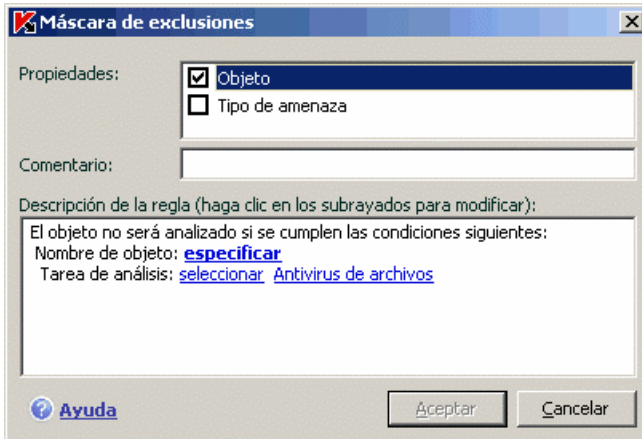


Figura 9. Creación de una regla de exclusión

- Objeto:** excluye de los análisis un determinado objeto, directorio o cualquier archivo incluido una cierta máscara.
- Tipo de amenaza:** excluye del análisis un objeto en función del estado atribuido por su clasificación en la Enciclopedia del virus.

Si activa las dos casillas a la vez, se creará una regla para este objeto, de acuerdo con un determinado estado, en función de la clasificación de la Enciclopedia del virus. En este caso, las reglas siguientes son aplicables:

- Si especifica un archivo concreto en el campo **Objeto** y una descripción en el campo **Tipo de amenaza**, el archivo especificado sólo será excluido si el análisis lo clasifica dentro de la amenaza seleccionada.
 - Si selecciona una zona o carpeta dentro del campo **Objeto** y una descripción (o máscara del tipo de amenaza) en el campo **Tipo de amenaza**, entonces los objetos con esta descripción serán excluidos sólo si se encuentran dentro de dicha zona o carpeta.
- Atribuya valores **a** los tipos de exclusión seleccionados. Para ello, en la sección **Descripción** haga clic en el vínculo especificar junto al tipo de exclusión:
 - En el tipo de **Objeto**, indique su nombre en la ventana abierta (puede ser un archivo, una carpeta particular o una máscara de

archivos (ver A.2 pág. 191). Active **Incluir subcarpetas** para excluir recursivamente los objetos (archivo, máscara de archivos, carpeta) del análisis.

- Escriba el nombre completo de la amenaza que desea excluir de los análisis tal y como aparece en la Enciclopedia del virus o utilice una máscara para definir el **Tipo de amenaza** (ver A.3 en la página 191).

En el caso de algunos tipos de amenazas, puede establecer condiciones avanzadas para aplicar las exclusiones en el campo **Configuración avanzada**.

4. Defina los componentes que Kaspersky Anti-Virus for Windows Servers debe utilizar en esta regla. Si selecciona cualquiera, la regla se aplicará a todos los componentes. Si desea limitar la regla a unos pocos componentes, haga clic en cualquiera, para que cambie a seleccionado. En la ventana abierta, active las casillas de componentes a los que desea aplicar esta regla de exclusión.

Para crear una regla de exclusión a partir de la notificación del programa cuando detecta un objeto peligroso:

1. Utilice el vínculo Agregar a zona de confianza en la ventana de notificación.
2. En la ventana abierta, asegúrese de que todos parámetros de la regla de exclusión cumplen sus necesidades. El programa sugiere el nombre del objeto y el tipo de amenaza automáticamente a partir de los datos de la notificación. Para crear la regla, haga clic en **Aceptar**.

Para crear una regla de exclusión desde la ventana del informe:

1. Seleccione el objeto del informe que desea agregar a las exclusiones.
2. Abra el menú contextual y seleccione **Agregar a zona de confianza** (ver Figura 10).

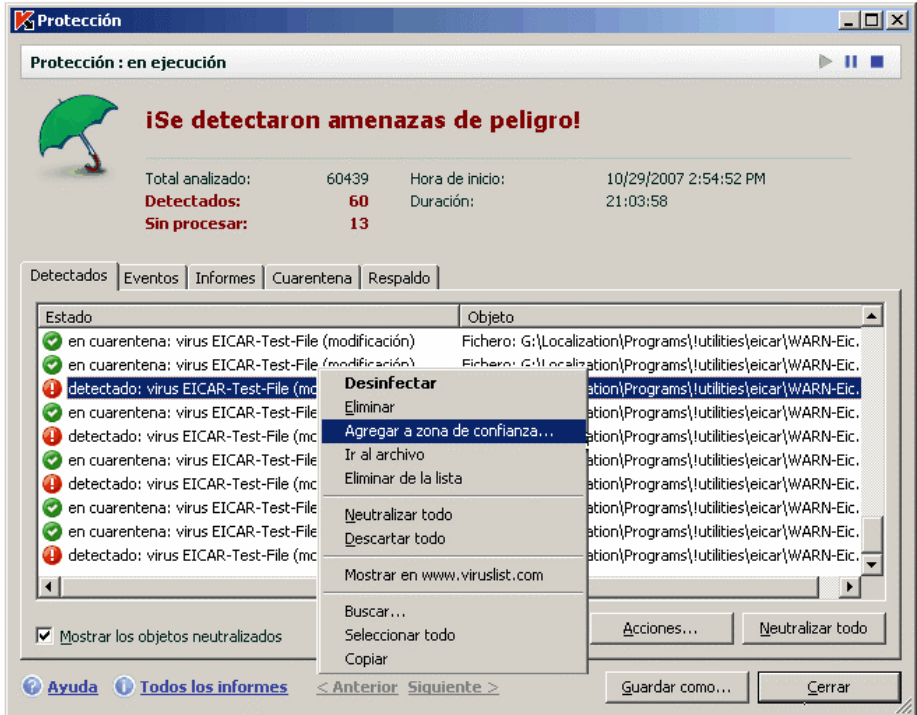


Figura 10. Creación de una regla de exclusión a partir de un informe

6.3.2. Aplicaciones de confianza

Kaspersky Anti-Virus for Windows Servers puede crear una lista de aplicaciones de confianza para las que no es necesario supervisar su actividad con archivos y en la red.

Por ejemplo, considera que los objetos utilizados por el **Bloc de notas** de Microsoft Windows Server son seguros y no necesitan ser analizados. Para excluir del análisis los objetos utilizados por este proceso, agregue el **Bloc de notas** (Notepad.exe) a la lista de aplicaciones de confianza. Sin embargo, el propio archivo ejecutable y los procesos de las aplicaciones de confianza seguirán siendo analizados como antes. Para excluir completamente la aplicación del análisis, debe utilizar reglas de exclusión (ver 6.3.1 pág. 59).

Además, algunas acciones clasificadas como peligrosas son perfectamente normales dadas las características de un cierto número de programas. Por ejemplo, los programas que interceptan normalmente el texto introducido por el

teclado. Para tener en cuenta estos programas y no supervisarlos, le recomendamos agregarlos a la lista de aplicaciones de confianza.

El uso de exclusiones para aplicaciones de confianza también permite resolver posibles conflictos de compatibilidad entre Kaspersky Anti-Virus for Windows Servers y otras aplicaciones (por ejemplo, el tráfico de red de otro equipo, ya analizado por la aplicación antivirus) y mejorar el rendimiento del equipo.

De forma predeterminada, Kaspersky Anti-Virus for Windows Servers analiza los objetos abiertos, ejecutados o guardados por cualquier proceso de programa.

Puede definir una lista de aplicaciones de confianza desde la ficha especial **Aplicaciones de confianza** (ver Figura 11). De forma predeterminada la lista de aplicaciones de confianza contiene una lista de aplicaciones que no serán supervisadas, de acuerdo con las recomendaciones de Kaspersky Lab, cuando instala Kaspersky Anti-Virus. Si no confía en alguna de las aplicaciones de la lista, desactive su casilla. Puede modificar la lista con los botones **Agregar**, **Modificar** y **Eliminar** asociados.

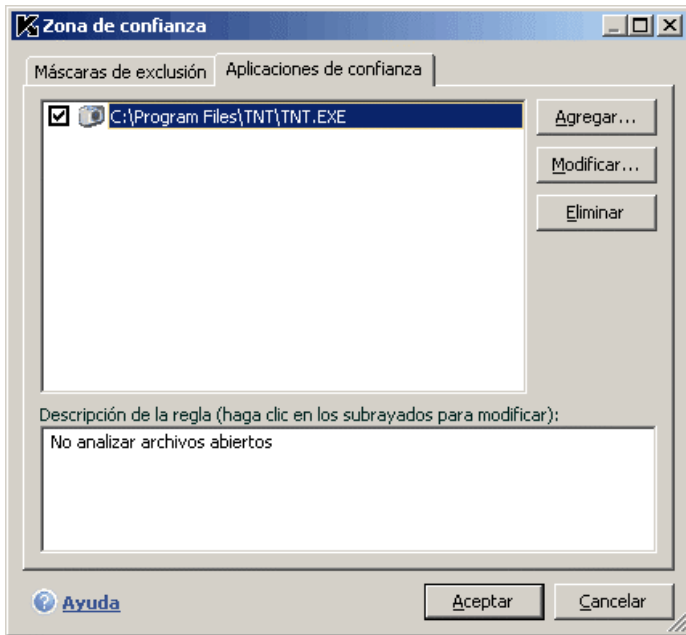


Figura 11. Lista de aplicaciones de confianza

Para agregar un programa a la lista de aplicaciones de confianza:

1. Haga clic en **Agregar** en la parte derecha de la ficha **Aplicaciones de confianza**.

2. En la ventana **Aplicación de confianza** (ver Figura 12) abierta, seleccione la aplicación con **Examinar**. En el menú contextual, haga clic en **Examinar** para abrir una ventana estándar de selección de archivos y determinar la ruta del archivo ejecutable, o haga clic en **Aplicaciones** para ver la lista de aplicaciones actualmente en ejecución y seleccionarlas si es necesario.

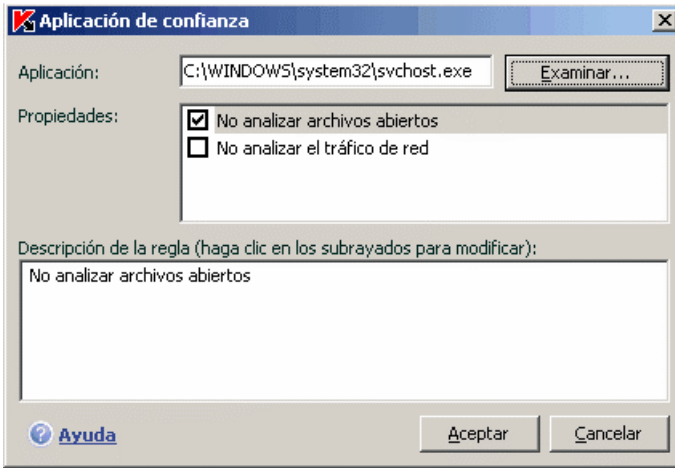


Figura 12. Agregar un programa a la lista de aplicaciones de confianza

Cuando selecciona un programa, Kaspersky Anti-Virus for Windows Servers registra los atributos internos del archivo ejecutable y los utiliza durante los análisis para determinar que el programa es de confianza.

La ruta del archivo se incluye automáticamente cuando selecciona su nombre.

3. A continuación, especifique qué acciones de este proceso son las que Kaspersky Anti-Virus no supervisará:
 - No analizar archivos abiertos:** excluye del análisis todos los archivos procesados por la aplicación de confianza.

6.4. Ejecución de tareas con otro perfil

Kaspersky Anti-Virus 6.0 for Windows Servers permite ejecutar tareas de análisis con un perfil de usuario distinto. Esta característica está desactivada de

forma predeterminada, de modo que las tareas se ejecutan con la cuenta de usuario utilizada para abrir la sesión en el sistema.

Así, por ejemplo, puede necesitar derechos de acceso a algún objeto durante el análisis. Con esta característica, resulta posible configurar tareas para que se ejecuten como un usuario con los privilegios necesarios.

Las actualizaciones de programas puede hacerse desde un origen al que no tiene acceso (por ejemplo, un directorio de actualizaciones en red) o que requiere permisos de usuario autorizado para el servidor proxy. Para usar esta característica, puede ejecutar el componente de actualización con otro perfil que disponga de los derechos adecuados.

Para configurar una tarea de análisis que se inicia bajo un perfil de usuario diferente:

1. Seleccione el nombre de la tarea en la sección **Analizar** (para tareas de análisis antivirus) o **Servicio** (para tareas de actualización) de la ventana principal y utilice el vínculo Configuración para abrir la ventana de configuración de la tarea.
2. Haga clic en **Personalizar** en la ventana de configuración de la tarea y abra la ficha **Avanzado** en la ventana abierta (ver Figura 13).
3. Para habilitar esta característica, active la casilla **Ejecutar esta tarea como**. Escriba los datos de inicio de sesión necesarios para ejecutar la tarea como sigue: nombre de cuenta y contraseña.

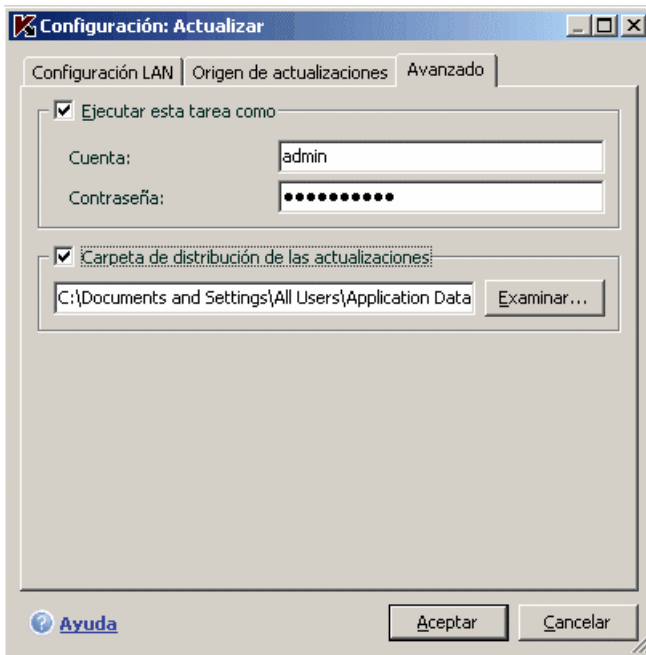


Figura 13. Configuración de una tarea de actualización con otro perfil

6.5. Configuración de tareas planificadas y notificaciones

Los parámetros de planificación son los mismos para las tareas de análisis antivirus, actualizaciones de aplicación y envío de notificaciones de Kaspersky Anti-Virus.

De forma predeterminada, las tareas de análisis antivirus creadas al instalar la aplicación están deshabilitadas. La excepción son los objetos de inicio que se analizan cada vez que se ejecuta Kaspersky Anti-Virus. De forma predeterminada, las actualizaciones se producen automáticamente en cuanto están disponibles en los servidores de actualización de Kaspersky Lab.

En caso de no estar satisfecho con estos parámetros, puede reprogramar la planificación. Seleccione el nombre de la tarea en la sección **Análisis** (para el análisis antivirus) o **Servicio** (para tareas de actualización o distribución de actualizaciones) y abra la ventana de parámetros con un clic en Configuración.

Para que las tareas se inicien de forma planificada, active la casilla de inicio automático en la sección **Modo de ejecución**. Puede modificar las veces en que se inicia la tarea de análisis desde la ventana **Planificación** (ver Figura 14), abierta cuando hace clic en **Cambiar**.

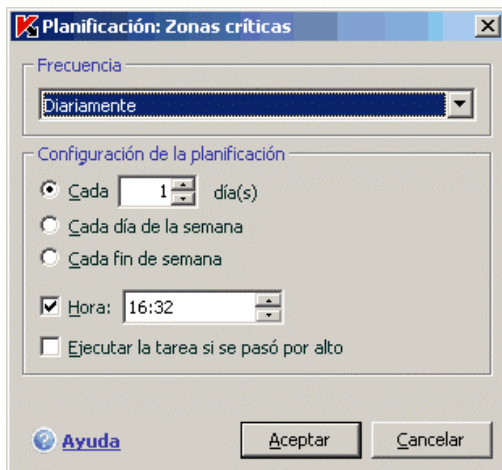


Figura 14. Planificación de una tarea

El primer parámetro que debe definir es la frecuencia de un evento (ejecución de tarea o notificación). Seleccione la opción deseada en la sección **Frecuencia** (ver Figura 14). A continuación, debe especificar los parámetros de la opción seleccionada en la sección Configuración de la planificación. Las opciones siguientes están disponibles:

- **Hora.** Iniciar una tarea o enviar una notificación a la fecha y hora especificadas.
- **Al iniciar la aplicación.** Inicia la tarea o envía una notificación cada vez que se ejecute Kaspersky Anti-Virus. También puede especificar en qué plazo posterior al inicio de la aplicación debe ejecutarse la tarea.
- **Después de cada actualización.** La tarea se ejecuta después de cada actualización de la firma de amenaza (sólo aplicable a tareas de análisis antivirus).
- **Cada N minutos.** El intervalo temporal entre dos análisis o notificaciones será de varios minutos. Especifique el plazo en minutos en los parámetros de planificación. No debe superar los 59 minutos.
- **Cada N horas.** El intervalo temporal entre análisis o notificaciones es de varias horas. Si selecciona esta opción, especifique el intervalo de tiempo en los parámetros de planificación: **Cada N horas** y defina el valor *N*. Por ejemplo, indique **Cada 1 hora** si desea ejecutar la tarea cada hora.

- **Diariamente** La tarea se ejecuta o la notificación se envía en un intervalo de varios días. Especifique el intervalo en los parámetros de planificación:
 - Seleccione **Cada N días** y defina el valor de N, para mantener un intervalo de un varios días. Seleccione **Cada día de la semana** si desea ejecutar un análisis diario, de lunes a viernes.
 - Seleccione **Cada fin de semana** para ejecutar la tarea o enviar la notificación sólo sábados y domingos.Utilice el campo **Hora** para indicar a qué hora del día se ejecutará la tarea de análisis.
- **Semanalmente.** La tarea se ejecuta o la notificación se envía en ciertos días de la semana. Si selecciona esta opción, active las casillas correspondientes a los días de la semana en los que desea ejecutar la tarea. Indique la hora del día en el campo **Hora**.
- **Mensualmente.** La tarea se ejecuta o la notificación se envía una vez al mes a la hora especificada.

Si la tarea de análisis no se puede ejecutar por cualquier razón (un programa de correo no instalado, por ejemplo, o el equipo estaba apagado a dicha hora), puede configurar la tarea para que se inicie automáticamente tan pronto como sea posible. Active **Ejecutar la tarea si se pasó por alto** en la ventana de planificación.

6.6. Opciones de energía

Los análisis antivirus aumentan la carga del procesador central y los subsistemas de disco, por lo que ralentizan los demás programas. De forma predeterminada, en este tipo de situaciones, el programa suspende la ejecución de los análisis antivirus y libera recursos del sistema para las aplicaciones del usuario.

Sin embargo, existe un número de programas que tan pronto como se liberan recursos del procesador pueden ejecutarse en segundo plano. Para que los análisis antivirus no dependan del funcionamiento de este tipo de programas, desactive la casilla **Facilitar recursos para otras aplicaciones** (ver Figura 15).

Observe que este parámetro puede definirse de forma individual para cada tarea de análisis antivirus. Si utiliza esta posibilidad, la configuración específica de una tarea tiene mayor prioridad.

La ventana abierta con **Configuración multiprocesador** permite configurar Kaspersky Anti-Virus para que se ejecute en un servidor multiprocesador (ver 6.7 pág. 69).

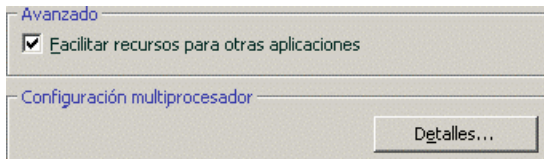


Figura 15. Parámetros de energía

Para configurar los parámetros de energía:

Seleccione la entrada **Protección** en la ventana principal del programa y haga clic en el vínculo Configuración. Configure los parámetros de energía en la sección **Avanzado**.

6.7. Configuración de servidor multiprocesador

Esta ventana permite configurar el rendimiento de un servidor multiprocesador.

Número de instancias del núcleo antivirus: número de copias del núcleo antivirus cargadas cuando se ejecuta Anti-Virus Kaspersky en el servidor. Este número determina el número de procesos antivirus que se ejecutan en paralelo.

Cuantas más copias del motor antivirus estén en ejecución, más rápidamente se realizan las operaciones antivirus. Sin embargo, esto afecta al rendimiento general del servidor.

Además, la ejecución simultánea de numerosos procesos antivirus garantiza que el servidor estará siempre protegido, en caso de que uno de los motores encuentre un error.


Para distribuir automáticamente los procesos antivirus entre los procesadores del servidor, active la casilla **Utilizar un controlador especial para administrar procesos paralelos**.

Si la casilla está desactivada, puede controlar manualmente la carga del servidor, por ejemplo, cuando reserva una parte de los procesadores para el tratamiento antivirus y otra para las tareas relacionadas directamente con tareas del servidor. Para ello, desactive los procesadores dedicados al servidor en la sección **Procesadores utilizados**.

Kaspersky Lab le recomienda reservar al menos un procesado para tareas del servidor cuando se ejecuta en un servidor multiprocesador.

CAPÍTULO 7. PROTECCIÓN ANTIVIRUS DEL SISTEMA DE ARCHIVOS DEL SERVIDOR

Kaspersky Anti-Virus incluye un componente *Antivirus de archivos*, que protege su equipo contra infecciones. Se carga junto con el sistema operativo, se ejecuta en la memoria RAM del equipo, y analiza todos los archivos abiertos, guardados o ejecutados.

El icono de Kaspersky Anti-Virus for Windows Servers en la barra del sistema es un indicador de la actividad del componente, con la apariencia siguiente  cuando se analiza un archivo.

De forma predeterminada, el componente Antivirus de archivos sólo analiza *archivos nuevos o modificados* o, en otras palabras, los archivos nuevos o modificados desde el análisis anterior. Los archivos se analizan de acuerdo con el algoritmo siguiente:

1. El componente intercepta las operaciones de acceso de los usuarios o programas a cualquier archivo.
2. El componente Antivirus de archivos explora las bases iChecker™ e iSwift™ en busca de información sobre el archivo interceptado. La decisión de analizar el archivo se toma en función de la información obtenida.

El proceso de análisis incluye los pasos siguientes:

1. El archivo se analiza en busca de virus. Los objetos malintencionados son detectados por comparación con las *firmas de amenazas* del programa, que contienen descripciones de todos los programas malintencionados y amenazas, conocidos hasta la fecha, así como métodos para su neutralización.
2. Después del análisis, se pueden tomar tres acciones posibles:
 - a. Si detecta código malintencionado en el archivo, el componente Antivirus de archivos lo bloquea, coloca una copia en la zona de *Respaldo*, e intenta reparar el archivo. Si el archivo ha sido desinfectado con éxito, se pone de nuevo a la disposición del usuario. Si no, se elimina el archivo.

- b. Si en un archivo se detecta código de apariencia sospechoso pero sin seguridad, el archivo se mueve a *Cuarentena*.
- c. Si no se encuentra código malintencionado, el archivo es restaurado inmediatamente.

7.1. Selección de un nivel de seguridad para archivos

El componente Antivirus de archivos protege los archivos con los que trabaja de acuerdo con uno de los niveles siguientes (ver Figura 16):

- **Máximo:** el nivel de supervisión más completo para los archivos abiertos, guardados o ejecutados.
- **Recomendado:** Kaspersky Lab recomienda este nivel de configuración. Analiza las siguientes categorías de objetos:
 - Programas y archivos por contenido;
 - Sólo los objetos nuevos y modificados desde el análisis anterior;
 - Objetos OLE incorporados.
- **Mínimo:** nivel de configuración que le permite utilizar cómodamente otras aplicaciones que consumen una cantidad significativa de recursos del sistema, porque el conjunto de archivos explorados es reducido.

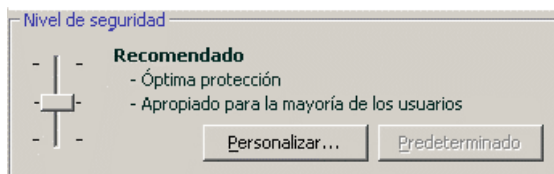


Figura 16. Nivel de seguridad del componente Antivirus de archivos

De forma predeterminada, el componente Antivirus de archivos utiliza el nivel **Recomendado**.

Puede aumentar o disminuir el nivel de protección de los archivos que utiliza, seleccionando el nivel deseado o modificando los parámetros del nivel actual.

Para modificar el nivel de seguridad,

Ajuste el cursor. El ajuste del nivel de seguridad le permite definir la relación entre la velocidad del análisis y el número total de archivos

examinados: cuantos menos archivos se examinan en busca de virus, mayor velocidad del análisis se consigue.

Si ninguno de los niveles de seguridad de archivos cumple sus necesidades, es posible personalizar los parámetros de protección. Para ello, seleccione el nivel más cercano a sus necesidades como punto de partida y modifique sus parámetros. En este caso, el nivel se establece en **Configuración personalizada**. Vamos a examinar un ejemplo en el que los niveles personalizados de seguridad en archivos resultan útiles.

Ejemplo:

El trabajo que realiza en su equipo le lleva a utilizar un gran número de tipos de archivos diferentes, algunos de los cuales pueden tener un gran tamaño. No desea correr el riesgo de pasar por alto archivos durante el análisis por culpa de su tamaño o extensión, aunque esto podría afectar el rendimiento de su equipo.

Consejo para seleccionar un nivel:

En función del origen de datos, es posible llegar a la conclusión de que existe un alto riesgo de infección por parte de un programa malintencionado. El tamaño y tipo de archivos controlados es muy variado y dejarlos fuera del análisis podría exponer los datos del equipo a grandes riesgos. Desea analizar los archivos utilizados en función de su contenido, no por su extensión.

Se recomienda utilizar el nivel de seguridad **Recomendado** como modelo, con los cambios siguientes: eliminar la restricción en el tamaño de archivos examinados y para optimizar la actividad del componente Antivirus de archivos, analizar únicamente los Archivos nuevos y modificados. De este modo, el análisis no consumirá tantos recursos del sistema y podrá seguir utilizando otras aplicaciones con comodidad.

Para modificar la configuración de un nivel de seguridad,

Haga clic en **Configuración** en la ventana de configuración del componente Antivirus de archivos. Modifique los parámetros del componente Antivirus de archivos en la ventana abierta y haga clic en **Aceptar**.

Tras esto, se creará un cuarto nivel de seguridad, **Configuración personalizada**, con los parámetros de protección definidos.

7.2. Configuración del componente Antivirus de archivos

La configuración que establezca determina cómo el componente Antivirus de archivos defenderá su equipo. Los parámetros pueden dividirse en los grupos siguientes:

- Parámetros que definen qué tipos de archivos (ver 7.2.1 en la página 73) serán analizados en busca de virus
- Parámetros que definen la cobertura de la protección (ver 7.2.2 en la página 76)
- Parámetros que definen cómo reacciona el programa ante objetos peligrosos (ver 7.2.5 en la página 81)
- Configuración avanzada del antivirus de archivos (ver 7.2.3 pág. 78)

En las secciones siguientes veremos estos grupos en detalle.

7.2.1. Definición de los tipos de los objetos que se analizarán

Para especificar los tipos de archivos analizados, debe definir los formatos y tamaños de archivos, así como las unidades exploradas en busca de virus, cuando los archivos se abren, se ejecutan o se guardan.

Para simplificar la configuración, todos los archivos se dividen en dos grupos: archivos *sencillos* y archivos *compuestos*. Los archivos sencillos no contienen ningún objeto, por ejemplo, archivos .txt. Los objetos compuestos pueden incluir varios objetos, cada uno de los cuales puede contener a su vez otros objetos. Existen varios ejemplos: archivos comprimidos, archivos con macros, hojas de cálculo, correos con adjuntos, etc.

Los tipos de archivos analizados se definen en la sección **Tipos de archivos** (ver Figura 17). Seleccione una de estas tres opciones:

- **Analizar todos los archivos.** Con esta opción seleccionada, todos los objetos del sistema de archivos que son abiertos, ejecutados o guardados serán sometidos al análisis sin excepción.
- **Analizar programas y documentos (por contenido).** Si selecciona este grupo de archivos, el componente Antivirus de archivos analizará sólo los archivos potencialmente infectados, es decir, archivos dentro de los cuales un virus puede haberse infiltrado.

Nota:

Un cierto número de formatos de archivos presentan un riesgo reducido de contener código malintencionado que pueda ser activado más tarde. Como ejemplo de este tipo están los archivos con formato .txt.

Inversamente, otros formatos de archivos contienen o pueden contener código ejecutable. Como ejemplo, tenemos los formatos .exe,.dll o .doc. El riesgo de infiltración y activación de código malintencionado en estos archivos es relativamente alto.

Antes de buscar virus en un archivo, se analiza su encabezado interno para conocer su formato de archivo (txt, doc, exe, etc.). Si el resultado del análisis indica que el formato del archivo es de un tipo que no puede infectarse, no se analiza y se devuelve inmediatamente para su uso. Si el formato del archivo permite que el archivo esté infectado, el archivo se analiza en busca de virus.

- ☉ **Analizar programas y documentos (por extensión).** Si selecciona esta opción, el componente Antivirus de archivos sólo analiza los archivos potencialmente infectados pero determinando su formato a partir de su extensión. Haga clic en el vínculo [extension](#) para examinar la lista de extensiones de archivo (ver A.1 en la página 187) que son analizados con esta opción.

Sugerencia:

No olvide que cualquier persona puede enviar un virus a su equipo con extensión.txt, aunque en realidad se trate de un archivo ejecutable renombrado como archivo .txt. Si selecciona ☉ **Analizar programas y documentos (por extensión)**, este archivo será ignorado durante el análisis. Si la casilla ☉ **Analizar programas y documentos (por contenido)** está seleccionada, el programa ignora su extensión y analiza los encabezados del archivo para descubrir si se trata de un archivo .exe. El componente Antivirus de archivos analizaría entonces el archivo en busca de virus.

En la sección **Productividad**, puede especificar que sólo los archivos nuevos y los modificados desde el análisis anterior deben ser analizados en busca de virus. Este modo de operación reduce de forma notable el tiempo de análisis y mejora la velocidad y rendimiento del programa. Para seleccionar este modo, active la casilla **Analizar sólo los archivos nuevos y modificados**. Este modo se aplica a archivos simples y compuestos.

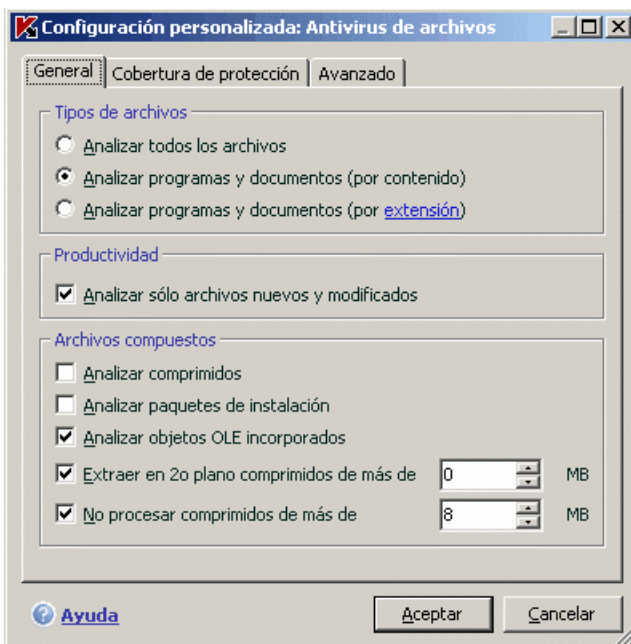


Figura 17. Selección de los tipos de archivos para analizar

En la sección **Archivos compuestos**, especifique qué tipos de archivos compuestos serán analizados en busca de virus:

- Analizar comprimidos Todos/Sólo nuevos**: analiza archivos.zip,.cab,.rar y.arj.
- Analizar paquetes de instalación Todos/Sólo nuevos**: analiza los archivos autoextraíbles en busca de virus.
- Analizar objetos OLE incorporados todos/sólo nuevos**: analiza los objetos incorporados en archivos (por ejemplo Microsoft Office Excel o macros incorporadas en un archivo de Microsoft Office Word, adjuntos de correo, etc.).

Para cada tipo de archivo compuesto, puede seleccionar y analizar todos los archivos o sólo los más recientes. Para ello, utilice el vínculo asociado al nombre del objeto para cambiar su valor. Si la sección **Productividad** está definida para analizar sólo los archivos nuevos y modificados, no podrá seleccionar el tipo de archivos compuestos examinados.

Para especificar qué archivos compuestos no deben analizarse en busca de virus, utilice los parámetros siguientes:

- Extraer en 2º plano comprimidos de más de... Mb.** Si el tamaño de un objeto compuesto supera este límite, el programa lo analizará como un objeto sencillo (analiza su encabezado) y lo devuelve al usuario. Los objetos que contiene se analizarán más tarde. Si la casilla no está activada, el acceso a los archivos mayores que el tamaño indicado quedará bloqueado hasta después de su análisis.
- No procesar comprimidos de más de... Mb.** En este caso, los archivos mayores que el tamaño especificado son ignorados durante el análisis.

7.2.2. Cobertura de protección

De forma predeterminada, el componente Antivirus de archivos analiza todos los archivos cuando son utilizados, sin tener en cuenta donde se encuentran, tanto en disco, como en CD/DVD-ROM o en disco de memoria flash.

Puede limitar la cobertura de la protección. Para ello:

1. Seleccione **Antivirus de archivos** en la ventana principal y abra la ventana de configuración del componente con un clic en Configuración.
2. Haga clic en **Configuración** y seleccione la ficha **Cobertura de protección** (ver Figura 18) en la ventana abierta.

La ficha muestra una lista de objetos que el componente Antivirus de archivos analizará. La protección está activa de forma predeterminada para todos los objetos en discos duros, medios extraíbles y unidades de red conectadas a su equipo. Puede completar y modificar la lista con los botones **Agregar**, **Modificar** y **Eliminar**.

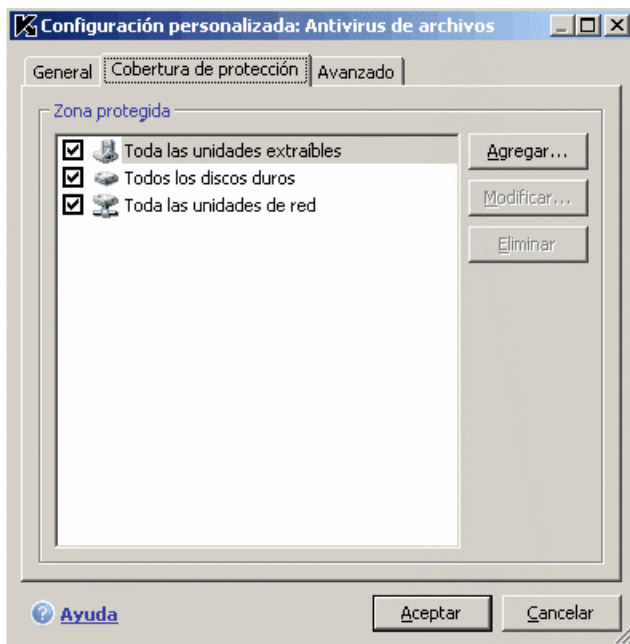


Figura 18. Creación de una zona protegida

Si desea reducir el rango de objetos protegidos, puede hacerlo con los métodos siguientes:

- Especifique sólo las carpetas, las unidades y los archivos que requieren protección.
- Cree una lista de objetos que no necesitan protección (ver 6.3 en la página 57).
- Combine los métodos uno y dos, es decir, cree una cobertura de protección de la que un cierto número de objetos quedarán fuera.

Puede utilizar máscaras cuando agrega objetos para su análisis. Observe que sólo puede incluir máscaras con rutas absolutas a objetos:

- **C:\dir*.*** ó **C:\dir*** ó **C:\dir**: todos los archivos de la carpeta **C:\dir**
- **C:\dir*.exe**: todos los archivos con extensión **.exe** en la carpeta **C:\dir**
- **C:\dir*.ex?**: todos los archivos con extensión **.ex?** en la carpeta **C:\dir**, donde **?** puede representar cualquier carácter
- **C:\dir\test**: sólo el archivo **C:\dir\test**

Para realizar un análisis recursivo, active la casilla **Incluir subcarpetas**.

Advertencia:

Recuerde que el componente Antivirus de archivos sólo analizará los archivos comprendidos dentro de la cobertura de protección creada. Los archivos que no están comprendidos dentro de la cobertura estarán disponibles sin análisis. Esto aumenta el riesgo de infección en su equipo.

7.2.3. Configuración avanzada

Los parámetros avanzados del componente Antivirus de archivos permiten especificar el modo de análisis del sistema de archivos y configurar las condiciones que suspenden temporalmente su ejecución.

Para configurar parámetros avanzados del componente Antivirus de archivos:

1. Seleccione **Antivirus de archivos** en la ventana principal y abra la ventana de configuración del componente con un clic en Configuración.
2. Haga clic en **Personalizar** y seleccione la ficha **Avanzado** en la ventana abierta (ver Figura 19).

El modo de análisis de los archivos condiciona el procesamiento realizado por el componente Antivirus de archivos. Dispone de las opciones siguientes:

- **Modo inteligente.** Este modo tiene por objetivo acelerar el procesamiento y entrega de los archivos al usuario. Cuando lo selecciona, la decisión de analizarlo se toma en función del análisis de las operaciones realizadas con el archivo.

Por ejemplo, Kaspersky Anti-Virus sólo analiza un archivo Microsoft Office la primera vez que lo abre y cuando lo cierra. Todas las operaciones intermedias que sobrescriben el archivo no son analizadas.

El modo inteligente es el predeterminado.

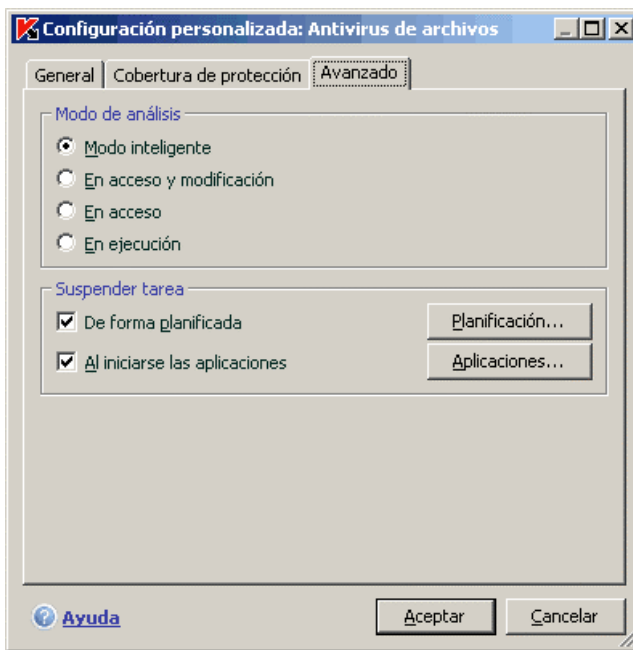


Figura 19. Configuración avanzada del componente Antivirus de archivos

- **En acceso y modificación:** el Antivirus de archivos analiza los archivos cuando son abiertos o modificados.
- **En acceso:** sólo se analizan los archivos al abrirlos.
- **En ejecución:** sólo se analizan los archivos al intentar ejecutarlos.

Es posible suspender el componente Antivirus de archivos cuando realiza tareas que consumen una gran cantidad de recursos del sistema operativo. Para disminuir la carga y permitir al usuario recuperar rápidamente el acceso a los archivos, recomendamos configurar el componente para se desactive durante un cierto tiempo o cuando se utilizan determinados programas.

Para suspender el componente, active la casilla **De forma planificada** y en la ventana abierta defina un intervalo de tiempo para detener e iniciar el componente (ver Figura 20) con el botón **Planificación**. Para ello, introduzca un valor en formato HH:MM en los campos correspondientes.

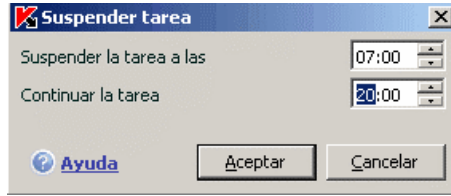


Figura 20. Pausa del componente

Para desactivar el componente cuando trabaje con programas que consumen una gran cantidad de recursos, active la casilla **Al iniciarse las aplicaciones** y modifique la lista de programas en la ventana abierta (ver Figura 21) con un clic en **Aplicaciones**.

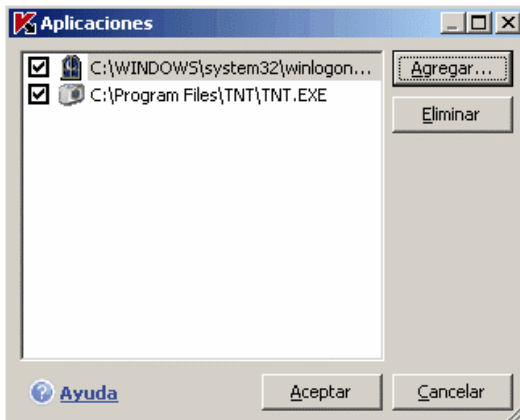


Figura 21. Creación de una lista de aplicaciones

Para agregar una aplicación a la lista, utilice **Agregar**. En el menú contextual que se abre, haga clic en **Examinar** para especificar la aplicación en una ventana de selección de archivos estándar. También puede ver la lista de aplicaciones en ejecución con el comando **Aplicaciones** y seleccionar la que desea.

Para eliminar una aplicación, selecciónela en la lista y haga clic en **Eliminar**.

Puede desactivar temporalmente la pausa que realiza el componente Antivirus de archivos cuando utilice una aplicación específica. Para ello, desactive el nombre de la aplicación. No es necesario eliminar su entrada de la lista.

7.2.4. Restauración de los parámetros predeterminados del componente Antivirus de archivos

Cuando configura el componente Antivirus de archivos, siempre es posible restablecer los parámetros de funcionamiento recomendados. Kaspersky Lab considera que son los óptimos y los ha combinado dentro del nivel de seguridad **Recomendado**.

Para restablecer la configuración predeterminada del componente Antivirus de archivos,

1. Seleccione **Antivirus de archivos** en la ventana principal y abra la ventana de configuración del componente con un clic en Configuración.
2. Haga clic en **Predeterminado** en la sección **Nivel de seguridad**.

Si modificó la lista de objetos incluidos en la zona protegida cuando configura el componente Antivirus de archivos, el programa le pregunta si desea guardar esa lista en caso de querer restaurar los valores iniciales. Para guardar la lista de objetos, active la casilla **Zona protegida** en la ventana **Restaurar la configuración** abierta.

7.2.5. Selección de acciones sobre objetos

Cuando el componente Antivirus de archivos analiza un archivo en busca de virus y descubre que está infectado o sospechosos de estarlo, las acciones siguientes del programa dependerán del estado del objeto y de la acción seleccionada.

El componente Antivirus de archivos puede etiquetar un objeto con uno de los estados siguientes:

- Programa dañino (por ejemplo, *virus*, *troyano*) (ver 1.1 pág. 9).
- *Potencialmente infectado*, cuando el análisis no puede determinar si el objeto está infectado. Significa que el programa detectó en el archivo una secuencia de código de un virus desconocido o la mutación de otro conocido.

De forma predeterminada, todos los archivos infectados son sometidos a desinfección y, si son sospechosos, se mueven a cuarentena.

Para cambiar la acción aplicada a un objeto,

Seleccione **Antivirus de archivos** en la ventana principal y abra la ventana de configuración del componente con un clic en Configuración. Todas las posibles acciones aparecen dentro de la sección apropiada (ver Figura 22).

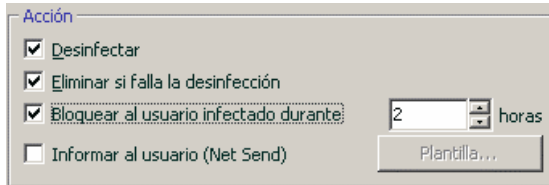


Figura 22. Acciones posibles del Antivirus de archivos ante objetos peligrosos

Si la acción seleccionada es	Cuando se detecta un objeto peligroso
<input checked="" type="checkbox"/> Desinfectar <input type="checkbox"/> Eliminar si falla la desinfección	<p>El acceso al objeto está bloqueado y se intentó acceder a él para desinfectarlo. Una copia del objeto se guarda en la zona de Respaldo. Si ha sido desinfectado con éxito, se pone de nuevo a la disposición del usuario. Si el objeto no se puede neutralizar, se mueve a Cuarentena. Este tipo de información se registra en el informe. Más tarde podrá intentar reparar este objeto.</p>
<input checked="" type="checkbox"/> Desinfectar <input checked="" type="checkbox"/> Eliminar si falla la desinfección	<p>El acceso al objeto está bloqueado y se intentó acceder a él para desinfectarlo. Una copia del objeto se guarda en la zona de Respaldo. Si ha sido desinfectado con éxito, se pone de nuevo a la disposición del usuario. Si el objeto no se puede reparar, se elimina.</p>
<input type="checkbox"/> Desinfectar <input checked="" type="checkbox"/> Eliminar	<p>El componente Antivirus de archivos bloqueará el acceso al objeto y lo eliminará.</p>

Si la acción seleccionada es	Cuando se detecta un objeto peligroso
<input checked="" type="checkbox"/> Bloquear al usuario infectado durante ... horas	<p>Bloquea el acceso del servidor al equipo que intentó copiar un archivo infectado o posiblemente infectado.</p> <p>Esta acción también puede aplicarse junto con las acciones de procesado del archivo (desinfección o eliminación).</p> <p>Observe que si el usuario abandona una sesión y se registra de nuevo en el sistema, Kaspersky Anti-Virus lo considera como una conexión diferente y levanta el bloqueo.</p>
<input checked="" type="checkbox"/> Informar al usuario (Net Send)	<p>Informa al usuario acerca del equipo que intentó copiar un archivo infectado o posiblemente infectado al servidor, mediante Net Send.</p> <p>Para configurar el modelo de notificación, haga clic en Plantilla (ver 7.2.6 pág. 83).</p>

Antes de reparar o eliminar un objeto, Kaspersky Anti-Virus crea una copia del objeto en la zona de Backup por si el objeto necesita ser restaurado o se produce la ocasión de neutralizarlo.

Advertencia. Las acciones **Bloquear usuario** y **NetSend** no están disponibles en la aplicación bajo Microsoft Windows NT Server.

7.2.6. Creación de una plantilla de notificación

Esta ventana le permite preparar un modelo de notificación para el usuario del equipo que intentó copiar un archivo infectado o potencialmente infectado al servidor.

Es posible incluir macros en el texto de la notificación para ofrecer más información: la ruta del objeto peligroso y el nombre de la amenaza. Para agregar macros al texto de la notificación, haga clic en **Macros**.

Para restablecer el texto original del modelo de notificación, haga clic en **Predeterminado**.

7.3. Desinfección pospuesta

Kaspersky Anti-Virus for Windows Servers bloquea el acceso a los archivos infectados cuando van a ser neutralizados o eliminados si no es posible.

Kaspersky Anti-Virus for Windows Servers bloquea el acceso a los archivos infectados cuando van a ser desinfectados, o eliminados si esto no es posible.

Para tener de nuevo acceso a los objetos bloqueados, éstos deben ser desinfectados. Para ello:

1. Seleccione **Antivirus de archivos** en la ventana principal del programa y haga clic en cualquier punto del cuadro **Estadísticas**.
2. Seleccione los objetos que le interesan en la ficha **Detectados** y haga clic en **Acciones** → **Neutralizar todo**.

Si han sido desinfectados con éxito, los archivos se ponen de nuevo a la disposición del usuario. Si no es posible la desinfección, se le presentan dos opciones: *eliminar* o *ignorar*. En el segundo caso, se recupera entonces el acceso al archivo. Sin embargo, esto aumenta significativamente el riesgo de infección en su equipo. Se desaconseja fuertemente ignorar los objetos peligrosos.

CAPÍTULO 8. ANÁLISIS ANTIVIRUS DE SU EQUIPO

Kaspersky Anti-Virus for Windows Servers puede buscar virus en elementos individuales (archivos, carpetas, discos, dispositivos plug-and-play) o en todo el conjunto del equipo. El análisis antivirus detiene cualquier código malintencionado que haya escapado a la vigilancia del componente Antivirus de archivos.

Kaspersky Anti-Virus for Windows Servers incluye las siguientes tareas de análisis predeterminadas:

Zonas críticas

Análisis antivirus de todas las zonas críticas del equipo, incluyendo: la memoria del sistema, los programas de inicio, los sectores de arranque en disco y los directorios de sistema *Windows* y *system32*. El objetivo es detectar con rapidez los virus activos en el sistema sin tener que realizar un análisis completo del equipo.

Mi PC

Busca virus en su equipo mediante un análisis completo de todos los discos, de la memoria y de los archivos.

Objetos de inicio

Analiza todos los programas cargados durante el arranque del sistema.

Los parámetros predeterminados de estas tareas son los recomendados. Puede modificar estos parámetros (ver 8.4 pág. 89) o definir una planificación (ver 6.5 pág. 66) de ejecución para las tareas.

También tiene la opción de crear sus propias tareas (ver 8.3 pág. 88) así como la de planificar su ejecución. Por ejemplo, puede planificar la ejecución de una tarea de análisis de las bases de correo una vez a la semana u otra que ejecute un análisis antivirus de la carpeta **Mis documentos**.


Adicionalmente, puede analizar cualquier objeto sin tener que crear una tarea de análisis especial. Puede seleccionar un objeto desde la interfaz de Kaspersky Anti-Virus for Windows Servers o con las herramientas estándar de Microsoft Windows Server (por ejemplo, en la ventana del **Explorador** o en su **Escritorio**, etc.).

Una lista completa de las tareas de análisis antivirus para su equipo se muestra en la sección **Analizar** en la parte izquierda de la ventana principal del programa.

8.1. Administración de tareas de análisis antivirus


Puede iniciar una tarea de análisis antivirus manualmente o planificar su ejecución automática (ver 6.5 pág. 66).

Para iniciar una tarea de análisis antivirus manualmente:


Active la casilla correspondiente al nombre de la tarea en la sección **Analizar** de la ventana principal del programa y haga clic en  en la barra de estado.

Las tareas en curso (incluyendo las tareas creadas mediante Kaspersky Administration Kit) se muestran en el menú contextual con un clic derecho en la barra del sistema.

Para suspender una tarea de análisis:

Haga clic en  en la barra de estado. El estado de la tarea cambia a *suspendido*. Esto suspende el análisis hasta que reanude la tarea de nuevo manualmente o ésta se vuelva a iniciar automáticamente en función de la planificación.

Para detener una tarea de análisis:

Haga clic en  en la barra de estado. El estado de la tarea cambia a *detenido*. La tarea de análisis se interrumpirá hasta que la reanude manualmente o se vuelva a iniciar automáticamente en función de la planificación. La próxima vez que ejecute la tarea, el programa le preguntará si desea continuar la tarea en el punto donde se detuvo o si debe empezar de nuevo.

8.2. Creación de una lista de objetos que deben analizarse

Para ver la lista de objetos analizados por una tarea particular, active la casilla junto al nombre de la tarea (por ejemplo, **Mi PC**) en la sección **Analizar** de la ventana principal del programa. La lista de objetos se mostrará en la parte derecha de la ventana bajo la línea de estado (ver Figura 23).

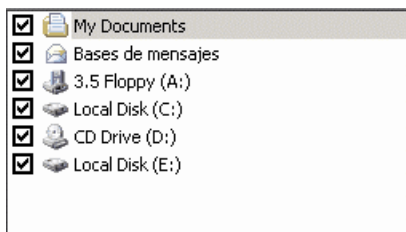


Figura 23. Lista de objetos que deben analizarse

Ya existen listas de objetos para analizar preparadas para las tareas predeterminadas creadas por la instalación del programa. Cuando crea sus propias tareas o cuando selecciona un objeto para una tarea de análisis antivirus, puede crear una lista de objetos.

Puede completar o modificar una lista de objetos analizados con los botones junto a la lista. Para agregar un nuevo objeto a la lista del análisis, haga clic en **Agregar** y en la ventana abierta seleccione el objeto que debe ser analizado.

Para mayor comodidad, puede asociar categorías a zonas de análisis, como los buzones de correo, la RAM, los objetos de inicio, las copias de respaldo del sistema operativo, y los archivos de la carpeta de cuarentena de Kaspersky Anti-Virus.

Además, cuando agrega a una zona de análisis una carpeta con objetos incorporados, también puede modificar el proceso de recursión. Para ello, seleccione un objeto en la lista de objetos correspondiente, abra el menú contextual y elija la opción **Incluir subcarpetas**.

Para eliminar un objeto, selecciónelo en la lista (al hacerlo, el nombre del objeto se visualiza en gris) y haga clic en **Eliminar**. Puede desactivar temporalmente el análisis de objetos individuales para cualquier tarea, sin eliminarlos de la lista. Para ello, desactive el objeto que no desea analizar.

Para iniciar una tarea de análisis, haga clic en **Analizar** o seleccione **Analizar** en el menú abierto cuando hace clic en **Acciones**.

Adicionalmente, para seleccionar y analizar un objeto, puede utilizar las herramientas estándar de Microsoft Windows Server (por ejemplo, en la ventana del Explorador o desde el Escritorio, etc.) (ver Figura 24). Para ello, sitúese sobre el objeto deseado, abra el menú contextual de Microsoft Windows Server con un clic derecho y elija **Buscar virus**.

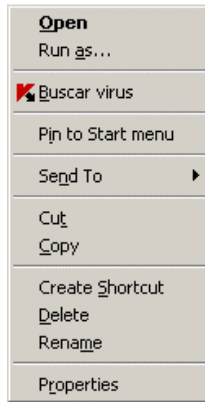


Figura 24. Análisis de objetos desde el menú contextual de Microsoft Windows

8.3. Creación de tareas de análisis antivirus

Para analizar objetos en su equipo en busca de virus, puede utilizar las tareas de análisis integradas incluidas con el programa, pero también puede crear sus propias tareas. Las nuevas tareas se crean a partir de otras existentes, utilizadas como modelo.

Para crear una nueva tarea de análisis antivirus:

1. Seleccione la tarea con la configuración más parecida a la que quiere aplicar en la sección **Analizar** de la ventana principal del programa.
2. Abra el menú contextual con un clic derecho o haga clic en **Acciones** a la derecha de la lista de objetos y elija **Guardar como...**
3. Escriba el nombre de la nueva tarea en la ventana abierta y haga clic en **Aceptar**. Una tarea con este nombre aparecerá en la lista de tareas de la sección **Analizar** de la ventana principal del programa.

Advertencia:

Existe un límite al número de tareas de actualización que es posible crear. El máximo son cuatro tareas.

La nueva tarea es una copia de la tarea utilizada como referencia. Para completar la configuración, cree una lista de objetos analizados (ver 8.2 pág. 86), configure la propiedades que gobiernan la tarea

(ver 8.4 pág. 89) y, si es necesario, define una planificación (ver 6.5 pág. 66) para ejecutar la tarea automáticamente.

Para renombrar una tarea creada:

Seleccione la tarea en la sección **Analizar** de la ventana principal del programa. Abra el menú contextual con un clic derecho en el nombre de la tarea o haga clic en **Acciones** a la derecha de la lista de objetos y elija **Renombrar**.

Escriba el nuevo nombre de tarea en la ventana abierta y haga clic en **Aceptar**. El nombre de la tarea aparecerá cambiado en la sección **Analizar**.

Para eliminar una tarea creada:

Seleccione la tarea en la sección **Analizar** de la ventana principal del programa. Abra el menú contextual con un clic derecho en el nombre de la tarea o haga clic en **Acciones** a la derecha de la lista de objetos y elija **Renombrar**.

El programa le pide que confirme la eliminación de la tarea. La tarea quedará eliminada de la lista de tareas en la sección **Analizar**.

Advertencia:

Sólo puede renombrar y eliminar las tareas que ha creado.

8.4. Configuración de tareas de análisis antivirus

El método utilizado para analizar objetos en su equipo viene determinado por un conjunto de propiedades asignadas a cada tarea.

Para configurar los parámetros de tarea:

abra la ventana de configuración y seleccione el nombre de la tarea en la entrada **Analizar**.

Puede utilizar la ventana de configuración de cada tarea para:

- Seleccionar el nivel de seguridad que utilizará la tarea (ver 8.4.1 pág. 90)
- Modificar parámetros avanzados:
 - definir qué tipos de archivos serán analizados en busca de virus (ver 8.4.2 pág. 91)

- configurar el inicio de la tarea con un perfil de usuario diferente (ver 6.4 pág. 64)
- definir parámetros avanzados de análisis (ver 8.4.5 en la página 96)
- Restaurar los parámetros de análisis predeterminados (ver 8.4.3 pág. 94)
- Seleccionar la acción aplicada por el programa cuando detecte un objeto infectado o posiblemente infectado (ver 8.4.4 en la página 94)
- definir una planificación (ver 6.5 en la pág. 66) para ejecutar automáticamente las tareas.

Adicionalmente, puede aplicar una configuración global (ver 8.4.6 en la página 98) de ejecución para todas las tareas.

En las secciones siguientes veremos la lista de parámetros de tarea en detalle.

8.4.1. Selección de un nivel de seguridad

Puede asignar a cada tarea de análisis un nivel de seguridad (ver Figura 25):

Máximo: el análisis integral del equipo completo o de discos, carpetas o archivos individuales. Le recomendamos utilizar este nivel si sospecha que su equipo está infectado por un virus.

Recomendado: los expertos de Kaspersky Lab recomiendan este nivel. Se analizarán los mismos archivos que para el nivel **Máximo**, salvo las bases de correo.

Mínimo: nivel de seguridad con una configuración que le permite utilizar cómodamente otras aplicaciones grandes consumidoras de recursos, al limitar la cobertura del análisis de archivos.

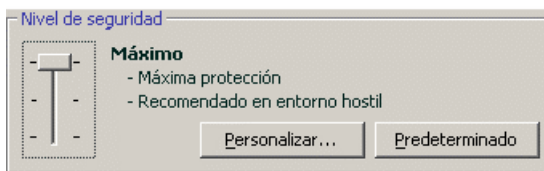


Figura 25. Selección de un nivel de seguridad para el análisis antivirus

De forma predeterminada, el nivel de análisis para archivos es el **Recomendado**.

Puede aumentar o disminuir el nivel de seguridad con la selección del nivel deseado, o modificando los parámetros del nivel actual.

Para modificar el nivel de seguridad,

Ajuste el cursor. El ajuste del nivel de seguridad le permite definir la relación entre la velocidad del análisis y el número total de archivos examinados: cuantos menos archivos se examinan en busca de virus, mayor velocidad del análisis se consigue.

Si ninguno de los niveles de seguridad de archivos cumple sus necesidades, es posible personalizar los parámetros de análisis. Para ello, seleccione el nivel más cercano a sus necesidades como punto de partida y modifique sus parámetros. En este caso, el nivel cambia a **Personalizado**.

Para modificar la configuración de un nivel de seguridad,

haga clic en **Configuración** en la ventana de configuración de la tarea. Modifique los parámetros de análisis de archivos en la ventana abierta y haga clic en **Aceptar**.

Tras esto, se creará un cuarto nivel de seguridad, **Configuración personalizada**, con los parámetros de protección definidos.

8.4.2. Definición de los tipos de objetos que se analizarán

Para especificar los tipos de objetos analizados, debe definir los formatos y tamaños de archivos, así como las unidades exploradas cuando se ejecute la tarea antivirus.

Los tipos de archivos analizados se definen en la sección **Tipos de archivos** (ver Figura 26). Seleccione una de estas tres opciones:

- Analizar todos los archivos.** Con esta opción, todos los archivos se analizará sin excepción.
- Analizar programas y documentos (por contenido).** Si selecciona este grupo de programas, se analizarán sólo los archivos potencialmente infectados, es decir, archivos dentro de los cuales un virus puede haberse infiltrado.

Nota:

Existen archivos en los que los virus no se pueden infiltrar porque el código de estos archivos no ofrece nada que permita al virus fijarse. Como ejemplo de este tipo están los archivos con formato .txt.

Inversamente, otros formatos de archivos contienen o pueden contener código ejecutable. Como ejemplo, tenemos los formatos .exe, .dll o .doc. El riesgo de infiltración y activación de código malintencionado en estos archivos es relativamente alto.

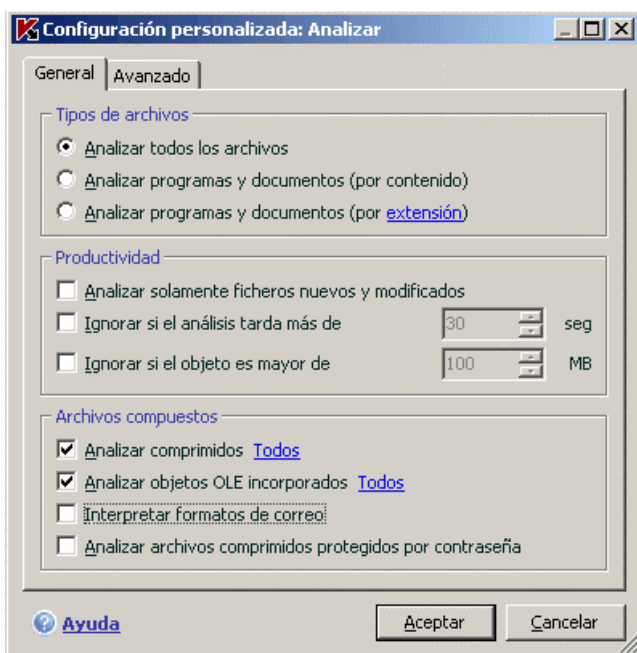


Figura 26. Configuración del análisis

Antes de buscar virus en un objeto, se analiza su encabezado interno para conocer su formato de archivo (txt, doc, exe, etc.).

- **Analizar programas y documentos (por extensión)**. En este caso, el programa sólo analiza los archivos potencialmente infectados y, al examinarlos, determina su formato a partir de su extensión. Abra este vínculo para examinar la lista de extensiones de archivos que son analizados con esta opción (ver A.1 en la página 187).

Sugerencia:

No olvide que un archivo con extensión.txt puede ser en realidad un archivo ejecutable renombrado como archivo .txt. Si selecciona la opción • **Analizar programas y documentos (por extensión)** este archivo será ignorado durante el análisis. Si la opción **Analizar programas y documentos (por contenido)** está seleccionada, el programa ignora las extensiones, y examina los encabezados de archivos para descubrir si se trata de archivos .exe, y poder analizarlos en profundidad.

En la sección **Productividad**, especifica que sólo los archivos nuevos y los modificados desde el análisis anterior deben ser analizados en busca de virus. Este modo de operación reduce de forma notable el tiempo de análisis y mejora la velocidad y rendimiento del programa. Para ello, active la casilla **Analizar sólo los archivos nuevos y modificados**. Este modo se aplica a archivos simples y compuestos.

También puede definir límites de tiempo para el análisis de objetos individuales en la sección **Productividad**.

Ignorar si el análisis tarda más de... (seg.) Active esta opción e indique el tiempo máximo de análisis por objeto. Si se supera este tiempo, el objeto se retirará de la cola de análisis.

Ignorar si el objeto es mayor de... Mb. Active esta opción e indique el tamaño máximo de un objeto. Si se supera este tamaño, el objeto se retirará de la cola de análisis.

En la sección **Archivos compuestos**, especifique qué tipos de archivos compuestos serán analizados en busca de virus:

Analizar archivos comprimidos Todos/Sólo nuevos analiza archivos.rar,.arj,.zip,.cab,.lha,.jar e.ice.

Advertencia:

Kaspersky Anti-Virus no elimina los formatos de archivo comprimidos (por ejemplo, .ha, .uee, .tar) no reconocidos automáticamente, aunque active la casilla para neutralizarlos o eliminarlos si no es posible neutralizarlos.

Para eliminar estos tipos de archivos comprimidos, haga clic en el vínculo [Eliminar](#) de la notificación de detección de un objeto peligroso La pantalla muestra este mensaje cuando se activa la opción **Preguntar al usuario durante el análisis/ Preguntar al usuario después de terminar el análisis** (ver 8.4.4 pág. 94). También puede eliminar los archivos infectados manualmente.

Analizar objetos OLE incorporados Todos/Sólo nuevos: analiza los objetos incorporados en archivos (por ejemplo, hojas Excel o macros incorporadas en un documento Microsoft Word, adjuntos de correo, etc.).

Para cada tipo de archivo compuesto, puede seleccionar y analizar todos los archivos o sólo los más recientes. Para ello, utilice el vínculo asociado al nombre del objeto. Cambia de valor cuando hace clic en él. Si la sección **Productividad** está definida para analizar sólo los archivos nuevos y modificados, no podrá seleccionar el tipo de archivos compuestos examinados.

Interpretar formatos de correo: analiza los formatos de correo y las bases de correo. Si desactiva esta casilla, los archivos de correo se analizarán como archivos binarios (sin examinar su formato interno) y, si el archivo no está infectado y el parámetro Analizar todos los archivos está activo, la

información será registrada en el informe con el estado *Correcto*. Si los parámetros de análisis de archivos fueron seleccionados por tipo y extensión, el archivo se pasará por alto, aplicando el tipo de amenaza *ignorado por su tipo*.

Nota. Cuando analiza bases de correo protegidas por contraseña:

- Kaspersky Anti-Virus for Windows Servers detecta código malintencionado en las bases de Microsoft Office Outlook 2000 pero no las desinfecta;
- Kaspersky Anti-Virus for Windows Servers no es capaz de buscar código malintencionado en las bases protegidas de Microsoft Office Outlook 2003.

Analizar archivos comprimidos protegidos por contraseña: analiza archivos comprimidos protegidos por contraseña. Activando esta característica, una ventana pedirá una contraseña antes de analizar los objetos comprimidos. Si la casilla no está activada, se pasarán por alto los archivos comprimidos protegidos por contraseña.

8.4.3. Restauración de los parámetros de análisis predeterminados

Cuando configura los parámetros de tarea, siempre es posible restablecer los parámetros recomendados del programa. Kaspersky Lab considera que son los óptimos y los ha combinado dentro del nivel de seguridad **Recomendado**.

Para restablecer la configuración predeterminada del análisis:

1. Seleccione el nombre de la tarea en la sección **Analizar** de la ventana principal y siga el vínculo Configuración para abrir la ventana de configuración de la tarea.
2. Haga clic en **Predeterminado** en la sección **Nivel de seguridad**.

8.4.4. Selección de acciones sobre objetos

Si cuando analiza un archivo se descubre que está infectado o sospechosos de estarlo, las acciones siguientes del programa dependerán del estado del objeto y de la acción seleccionada.

Uno de los siguientes estados puede ser asignado al objeto después de analizarlo:

- Programa dañino (por ejemplo, *virus*, *troyano*).

- *Potencialmente infectado*, cuando el análisis no puede determinar si el objeto está infectado. Es probable que el programa haya detectado en el archivo una secuencia de código de un virus desconocido o la mutación de otro conocido.

De forma predeterminada, todos los archivos infectados son sometidos a desinfección y, si están potencialmente infectados, se mueven a cuarentena.

Para cambiar la acción aplicada a un objeto,

seleccione el nombre de la tarea en la sección **Analizar** de la ventana principal del programa y utilice el vínculo Configuración para abrir la ventana de configuración de la tarea. Las posibles acciones aparecen dentro de las secciones apropiadas (ver Figura 27).

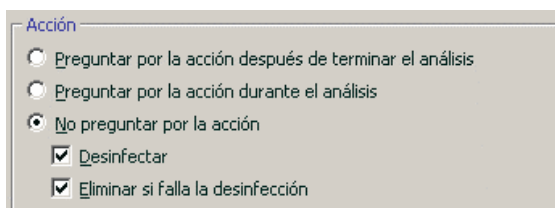


Figura 27. Selección de acciones sobre objetos peligrosos

Si la acción seleccionada es	En presencia de un objeto dañino o posiblemente infectado
<input type="radio"/> Preguntar por la acción después de terminar el análisis	El programa no procesa los objetos hasta el final del análisis. Cuando el análisis ha terminado, la ventana estadísticas se abre mostrando uno tras otro una lista de objetos detectados y el programa pregunta por la acción a aplicar a cada uno.
<input checked="" type="radio"/> Preguntar por la acción durante el análisis	El programa muestra un mensaje de advertencia con información acerca del código malintencionado que infecta (o posiblemente infecta) el archivo y le permite elegir entre una de las acciones siguientes.
<input checked="" type="radio"/> No preguntar por la acción	El programa registra información acerca de los objetos detectados en el informe, pero no los procesa ni los notifica al usuario. No le

Si la acción seleccionada es	En presencia de un objeto dañino o posiblemente infectado
	recomendamos utilizar esta característica, ya que los objetos infectados o potencialmente infectados permanecerán en su equipo, lo que hace prácticamente imposible evitar la infección.
<input checked="" type="radio"/> No preguntar por la acción <input checked="" type="checkbox"/> Desinfectar	El programa intenta neutralizar el objeto detectado sin pedirle confirmación al usuario. Si el archivo puede ser desinfectado, se desplaza a la zona de Respaldo para su posterior desinfección. Si el programa no puede desinfectar el objeto, bloquea el acceso al mismo.
<input checked="" type="radio"/> No preguntar por la acción <input checked="" type="checkbox"/> Desinfectar <input checked="" type="checkbox"/> Eliminar si falla la desinfección	El programa intenta neutralizar el objeto detectado sin pedirle confirmación al usuario. Si el objeto no se puede reparar, se elimina. Una copia se guarda en el Respaldo.
<input checked="" type="radio"/> No preguntar por la acción <input type="checkbox"/> Desinfectar <input checked="" type="checkbox"/> Eliminar	El programa elimina automáticamente el objeto

Antes de reparar o eliminar un objeto, Kaspersky Anti-Virus crea una copia del objeto en la zona de respaldo (ver 12.2 en la página 156) por si el objeto necesita ser restaurado o se produce la ocasión de neutralizarlo.

Si tiene el estado *potencialmente infectado*, el objeto se mueve a la Cuarentena sin intentar neutralizarlo.

8.4.5. Configuración avanzada del análisis antivirus

Además de configurar los parámetros básicos del análisis antivirus, también puede utilizar parámetros avanzados (ver Figura 28):

- Activar la tecnología iChecker:** utiliza una tecnología que permite mejorar la velocidad del análisis al excluir algunos objetos. La exclusión de un objeto

resulta de aplicar un algoritmo especial que considera la fecha de las bases de aplicación, la fecha del último análisis del objeto y los cambios en la configuración del análisis.

Por ejemplo, dispone de un archivo comprimido que el programa ya analizó y atribuyó el estado de no infectado. La vez siguiente, el programa ignorará el archivo comprimido a menos que haya sido modificado o la configuración del análisis haya cambiado. Si la estructura del archivo comprimido ha cambiado porque se agregó un nuevo objeto al mismo, los parámetros de análisis han cambiado o las bases de aplicación han sido actualizadas, entonces el programa analizará de nuevo el archivo comprimido.

Existen limitaciones al uso de iChecker™: no funciona con archivos de gran tamaño y sólo se aplica a objetos con estructura reconocida por Kaspersky Anti-Virus for Windows Servers (por ejemplo, .exe, .dll, .lnk, .tff, .inf, .sys, .com, .chm, .zip, .rar).

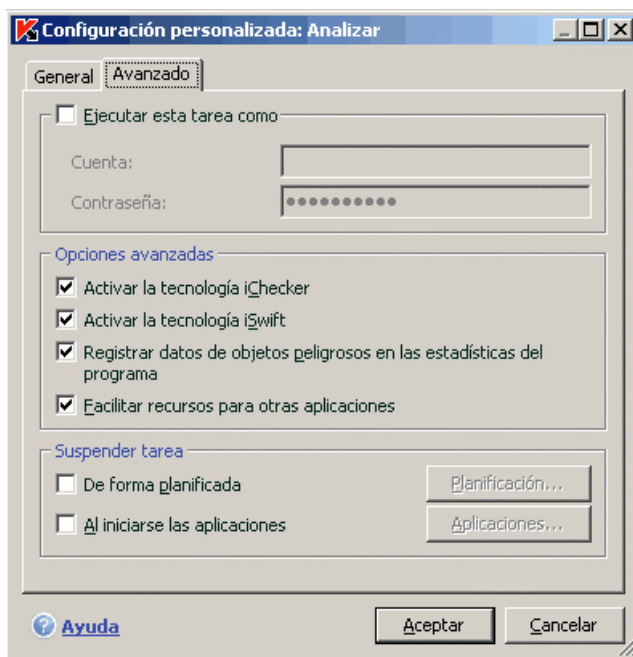


Figura 28. Configuración avanzada del análisis

- Activar la tecnología iSwift.** Esta tecnología es un desarrollo de la tecnología iChecker para equipos que utilizan el sistema de archivos NTFS. Existen limitaciones al uso de iSwift: está circunscrita a determinadas ubicaciones dentro del sistema de archivos y sólo para objetos del sistema de archivos NTFS.

- Registrar datos de objetos peligrosos en las estadísticas del programa:** registra información acerca de objetos peligrosos detectados en las estadísticas generales del programa y muestra una lista de amenazas detectadas durante el análisis en la ficha **Detectados** de la ventana de informe (ver 11.3.2 en la página 129). Si la opción no está activa, el informe no mostrará información acerca de objetos peligrosos y no será posible procesar los datos.
- Facilitar recursos para otras aplicaciones:** suspende la tarea de análisis antivirus si el procesador está ocupado por otra aplicación.

8.4.6. Aplicación de una configuración global a todas las tareas

Cada tarea de análisis se ejecuta de acuerdo con sus propios parámetros. De forma predeterminada, las tareas creadas cuando instala el programa en su equipo utilizan los parámetros recomendados por Kaspersky Lab.

Puede aplicar una configuración global para todas las tareas. Al principio, se utiliza un conjunto de propiedades para analizar un objeto individual en busca de virus.


Para aplicar una configuración global para todas las tareas:

1. Seleccione la entrada **Analizar** en la parte izquierda de la ventana principal del programa y haga clic en Configuración.
2. En la ventana de configuración abierta, configure los parámetros del análisis: Seleccione el nivel de seguridad (ver 8.4.1 pág. 90), configure los parámetros avanzados y seleccione una acción (ver 8.4.4 en la página 94) para los objetos.
3. Para aplicar estos nuevos parámetros a todas las tareas, haga clic en **Apply** en la sección **Otras tareas de análisis**. Confirme la configuración global seleccionada en el mensaje emergente.

CAPÍTULO 9. PRUEBAS DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Después de instalar y configurar Kaspersky Anti-Virus, le recomendamos poner a prueba la configuración y el funcionamiento del programa con un virus de prueba y sus modificaciones.

9.1. Prueba con el ‘virus’ EICAR y sus modificaciones

El virus de prueba ha sido especialmente diseñado por el organismo  (The European Institute for Computer Anti-Virus Research) con el fin de poner a prueba productos antivirus.

El virus de prueba NO ES UN VIRUS ni contiene código que pueda dañar su equipo. Sin embargo, la mayoría de los programas antivirus los identifican como un virus.

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

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

El archivo descargado desde el sitio de **EICAR** contiene el cuerpo de un virus de prueba estándar. Kaspersky Anti-Virus lo detectará, lo etiquetará como **virus** y aplicará la acción definida por objetos de este tipo.

Para poner a prueba las respuestas de Kaspersky Anti-Virus cuando detecta objetos de diferentes tipos, puede modificar el contenido estándar del virus de prueba agregándole alguno de los prefijos indicados en la tabla a continuación.

Prefijo	Estado del virus de prueba	Acción de la aplicación cuando procesa el objeto
Sin prefijo, virus de prueba estándar	El archivo contiene un virus de prueba. No puede neutralizar el objeto	La aplicación identifica el objeto como malintencionado, no susceptible de tratamiento, y lo elimina.
CORR-	Dañado.	La aplicación tiene acceso al objeto pero no puede analizarlo, porque está dañado (la estructura del archivo es inconsistente o tiene un formato de archivo incorrecto, por ejemplo).
SUSP- WARN-	El archivo contiene un virus de prueba (modificado). No puede neutralizar el objeto	Este objeto es la mutación de un virus conocido o un virus desconocido. En el momento de detectarse, la base de la aplicación no contiene la descripción del tratamiento para este objeto. La aplicación coloca el objeto en cuarentena, para procesarlo más tarde, con firmas de amenazas actualizadas.
ERRO-	Error de procesado.	Ocurrió un error mientras procesaba el objeto: la aplicación no tiene acceso al objeto analizado, porque la integridad del objeto se ha vuelto inconsistente (por ejemplo, no se encuentra el final de un archivo multivolumen) o porque no es posible conectar con él (si el objeto se analiza en una unidad de red).
CURE-	El archivo contiene un virus de prueba. Es posible neutralizarlo. Es posible reparar el objeto, el texto del cuerpo del virus cambia a CURE.	El objeto contiene un virus que es posible neutralizar. La aplicación analiza el objeto en busca de virus, tras lo cual éste queda completamente sanado.

Prefijo	Estado del virus de prueba	Acción de la aplicación cuando procesa el objeto
DELE-	El archivo contiene un virus de prueba. No puede neutralizar el objeto	El objeto contiene un virus que no se puede reparar o un troyano. La aplicación elimina estos objetos.

La primera columna de la tabla contiene los prefijos que deben incluirse delante de la cadena del virus de prueba estándar. La segunda columna describe el estado y la respuesta de Kaspersky Anti-Virus a diferentes tipos de virus de prueba. La tercera columna describe los objetos que, con el mismo estado, son procesados por la aplicación.

Los parámetros del análisis antivirus determinan las acciones que se toman con cada uno de estos objetos.

9.2. Prueba del componente Antivirus de archivos

Para poner a prueba el funcionamiento del componente Antivirus de archivos:

1. Cree una carpeta en disco, copie en ella el virus de prueba descargado desde el sitio Web oficial del organismo (ver 9.1 pág. 99) así como las modificaciones del virus de prueba que haya creado.
2. Autorice el registro de todos los eventos para que el informe muestre información acerca de los objetos dañados o no analizados por causa de errores. Para ello, active **Registrar los eventos sin gravedad** en la ventana de configuración del informe (ver 11.3.1 pág. 128).
3. Ejecute el virus de prueba o su modificación.

El componente Antivirus de archivos interceptará el intento de acceso al archivo, lo analizará y lo eliminará.

Cuando selecciona diferentes opciones de configuración predefinidas para tratar los objetos detectados, puede poner a prueba la reacción del componente Antivirus de archivos cuando detecta diferentes tipos de objetos.

Puede examinar los detalles del funcionamiento del componente Antivirus de archivos en el informe correspondiente.

9.3. Prueba de las tareas de análisis antivirus

Para poner a prueba las tareas de análisis antivirus:

1. Cree una carpeta en disco, copie en ella el virus de prueba descargado desde el sitio Web oficial del organismo (ver 9.1 pág. 99) así como las modificaciones del virus de prueba que haya creado.
2. Cree una nueva tarea de análisis antivirus (ver 8.3 pág. 88) e incluya la carpeta con el conjunto de virus de prueba dentro de los objetos que deben analizarse (ver 9.1 pág. 99).
3. Autorice el registro de todos los eventos para que el informe muestre información acerca de los objetos dañados o no analizados por causa de errores. Para ello, active **Registrar los eventos sin gravedad** en la ventana de configuración del informe.
4. Ejecute la tarea de análisis antivirus (ver 8.1 pág. 86).

Cuando ejecuta un análisis, a medida que se detectan los objetos sospechosos o infectados, aparecen notificaciones en pantalla con información acerca de estos objetos, invitando al usuario a que elija la acción aplicada:



Figura 29. Objeto peligroso detectado

De este modo, al seleccionar diferentes opciones de configuración predefinidas para las respuestas, puede poner a prueba las reacciones de Kaspersky Anti-Virus cuando detecta diferentes tipos de objetos.

Puede examinar los detalles de la tarea de análisis antivirus en el informe del componente.

CAPÍTULO 10.

ACTUALIZACIONES DEL PROGRAMA

Mantener actualizado su software antivirus es una garantía de seguridad. Con la aparición cotidiana de nuevos virus, troyanos y software malintencionado, es importante actualizar con regularidad la aplicación para mantener su información constantemente protegida.

La actualización de la aplicación implica que los siguientes componentes hayan sido descargados e instalados en su equipo:

- **Firmas de amenazas**

La aplicación utiliza firmas de amenazas para proteger la información en su equipo. Los componentes software responsables de la protección utilizan la base de la aplicación para buscar y reparar objetos dañinos en su equipo. Las firmas son completadas cada hora con nuevos registros de amenazas y métodos para luchar contra ellas. Por ello, se recomienda actualizarlas de forma regular.

Las versiones anteriores de las aplicaciones Kaspersky Lab disponían de soporte para conjuntos de amenazas de tipo *estándar* y *ampliado*. Cada uno se hacía cargo de la protección de su equipo contra diferentes clases de objetos peligrosos. En Kaspersky Anti-Virus for Windows Servers no necesita preocuparse del conjunto adecuado de las bases de aplicación seleccionadas. Ahora nuestros productos utilizan una base de firmas de amenazas que le protegen indistintamente contra cualquier objeto dañino y potencialmente peligroso y contra intrusiones de piratas.

- **Módulos de aplicación**

Además de las firmas, puede actualizar los módulos de Kaspersky Anti-Virus for Windows Servers. Se publican regularmente nuevas actualizaciones de aplicación.

El origen principal de actualizaciones para Kaspersky Anti-Virus for Windows Servers son los servidores de actualización de Kaspersky Lab.

Para descargar las actualizaciones desde estos servidores, su equipo debe estar conectado a Internet.

Si no tiene acceso a los servidores de actualización de Kaspersky Lab (por ejemplo, su equipo no está conectado a Internet), llame a la sede de Kaspersky Lab al +7 (495) 797-87-00, +7 (495) 645-79-39 o al +7 (495) 956-70-00 y solicite información para ponerse en contacto con los colaboradores de Kaspersky Lab

que puedan proporcionarle actualizaciones comprimidas en discos flexibles o en CD.

Es posible descargar las actualizaciones con alguno de los siguientes modos:

- *Automático.* Kaspersky Anti-Virus comprueba en los orígenes de actualizaciones la presencia de actualizaciones a intervalos especificados. Los análisis pueden ser configurados para realizarse con mayor frecuencia durante epidemias de virus, y con menor frecuencia el resto del tiempo. Si encuentra nuevas actualizaciones, las descarga e instala en el equipo. Es la configuración predeterminada.
- *Mediante planificación.* La actualización se planifica de forma que su inicio se produzca a una hora especificada.
- *Manual.* Con esta opción, el componente de actualización se inicia manualmente.

Durante la actualización, la aplicación compara las bases de aplicación y los módulos de aplicación en su equipo con las versiones disponibles en el servidor de actualizaciones. Si el servidor ya dispone de la última versión de firmas y módulos, aparece una nota relacionada dentro de la ventana de la aplicación. Si las bases y módulos en su equipo y en el servidor de actualizaciones difieren, la aplicación descarga tan sólo la parte de actualizaciones que falta. El servicio de actualización no descarga las bases y módulos de los que ya dispone, con lo que se acelera la velocidad y se ahorra tráfico Internet.

Antes de actualizar las bases de aplicación, Kaspersky Anti-Virus for Windows Servers crea una copia de respaldo de las mismas, que puede servir para deshacer la operación (ver 10.2 pág. 106). Por ejemplo, si el proceso de actualización daña las bases de aplicación de forma que puede utilizarlas, puede deshacer y volver a la versión anterior fácilmente, antes de intentar actualizar las firmas más tarde.

Puede distribuir las actualizaciones recuperadas cuando actualiza la aplicación (ver 10.4.4 pág. 115). Esta característica le permite actualizar las bases de datos y los módulos utilizados por las aplicaciones de la versión 6.0 en equipos de red, ahorrando tráfico de red.

10.1. Ejecución del componente de actualización

Puede iniciar el proceso de actualización en cualquier momento. Se ejecuta a partir del origen de actualizaciones seleccionado (ver 10.4.1 en la página 108).

Puede ejecutar el componente de actualizaciones desde:

- el menú contextual (ver 4.2 pág. 37).
- la ventana principal del programa (ver 4.3 en la página 38)

Para iniciar el componente de actualización desde el menú contextual:

1. Haga clic con el botón derecho en el icono de la aplicación en la barra del sistema para abrir el menú contextual.
2. Seleccione **Actualizar**.

Para iniciar la actualización desde la ventana principal del programa:

1. Seleccione **Actualizar** en la entrada **Servicio**.
2. Haga clic en **Actualizar ahora!** en el panel derecho de la ventana principal o utilice el icono ► en la barra de estado.

El progreso de la actualización del programa se muestra en una ventana especial, que puede ocultar con **Cerrar**. La actualización continúa con la ventana oculta.

Observe que las actualizaciones son copiadas al origen local durante el proceso de actualización, siempre que este servicio esté activado (ver 10.4.4 pág. 115).

10.2. Anulación de la actualización anterior

Cada vez que inicia la actualización, Kaspersky Anti-Virus for Windows Servers crea una copia de respaldo de las firmas de amenazas disponibles y después, inicia la descarga de actualizaciones. De este modo, puede volver a utilizar la versión anterior de las bases de aplicación en caso de que falle una actualización.

Para deshacer y volver a la versión anterior de las bases de aplicación:

1. seleccione la entrada **Actualizar** en la entrada **Servicio** de la ventana principal del programa.
2. Haga clic en **Deshacer** en el panel derecho de la ventana principal de la aplicación.

10.3. Creación de tareas de actualización

Kaspersky Anti-Virus dispone de una tarea de actualización integrada para módulos de programa y firmas de amenazas. También puede crear sus propias tareas de actualización con diferentes parámetros y planificar su ejecución.

Por ejemplo, ha instalado Kaspersky Anti-Virus en un portátil que utiliza en caso y en el trabajo. Desde su casa, la actualización se realiza desde los servidores de actualización de Kaspersky Lab y en el trabajo, desde una carpeta local donde se almacenan las actualizaciones que necesita. El uso de dos tareas diferentes evita tener que cambiar los parámetros de actualización cada vez que se desplaza.

Para crear una tarea de actualización avanzada:

1. Seleccione **Actualizar** desde la entrada **Servicio** de la ventana principal del programa, abra el menú contextual con un clic derecho y seleccione **Guardar como**.
2. Escriba el nombre de la tarea en la ventana abierta y haga clic en **Aceptar**. Una tarea con este nombre aparecerá en la entrada **Servicio** de la ventana principal del programa.

Advertencia.

Existe un límite al número de tareas de actualización que el usuario puede crear dentro de Kaspersky Anti-Virus. Número máximo: dos tareas.

La nueva tarea hereda todas las propiedades de la tarea de referencia, salvo los parámetros de planificación. La configuración predeterminada de análisis automático está desactivada para la nueva tarea. Para continuar la configuración, debe especificar el origen de actualizaciones (ver 10.4.1 pág. 108), la configuración de red (ver 10.4.3 pág. 113) y, si es necesario, active las tareas con privilegios de otro perfil (ver 6.4 pág. 64) y configure la planificación (ver 6.5 en la pág. 66).

Para renombrar una tarea:

Seleccione la tarea en la entrada **Servicio** de la ventana principal del programa, abra el menú contextual con un clic derecho y seleccione **Renombrar**.

Escriba el nuevo nombre de tarea en la ventana abierta y haga clic en **Aceptar**. El nombre de tarea aparecerá cambiado en la entrada **Servicio**.

Para eliminar una tarea:

Seleccione la tarea en la entrada **Servicio** de la ventana principal del programa, abra el menú contextual con un clic derecho y seleccione **Eliminar**.

Confirme la eliminación de la tarea en la ventana de confirmación. La tarea quedará eliminada de la lista de tareas en la entrada **Servicio**.

Advertencia.

El cambio de nombre y la eliminación son operaciones disponibles sólo para tareas personalizadas.

10.4. Configuración de la actualización

Para la configuración del servicio de actualizaciones, especifique los siguientes parámetros:

- El origen desde donde se descargan e instalan las actualizaciones (ver 10.4.1 en la página 108);
- Modo de actualización de la aplicación y para qué elementos específicos (ver 10.4.2 pág. 111);
- Frecuencia de las actualizaciones planificadas (ver 6.5 pág. 66);
- Cuenta utilizada para ejecutar la actualización (ver 6.4 pág. 64);
- Copia de las actualizaciones descargadas a un directorio local (ver 10.4.4 pág. 115);
- Qué acciones deben realizarse después de completar la actualización (ver 10.4.5 pág. 116).

En las secciones siguientes veremos estos aspectos en detalle.

10.4.1. Selección de un origen de actualizaciones

El *origen de actualizaciones* es cualquier origen que contiene actualizaciones de las bases de aplicación y de los módulos de aplicación de Kaspersky Anti-Virus.

Puede usar los siguientes orígenes de actualización:

- *Servidor de administración*: repositorio centralizado de actualizaciones ubicado en el servidor de administración de Kaspersky Administración Kit (para más detalles, consulte el Manual del administrador de Kaspersky Administration Kit 6.0).
- *Servidores de actualización de Kaspersky Lab*: son sitios Internet especiales que contienen las actualizaciones disponibles de las bases de aplicación y de los módulos de aplicación para todos los productos Kaspersky Lab.
- *Servidor HTTP, FTP, carpeta local o de red*: servidor o carpeta local con las últimas actualizaciones.

Si no tiene acceso a los servidores de actualización de Kaspersky Lab (por ejemplo, no dispone de conexión Internet), llame a la sede de Kaspersky Lab al +7 (495) 797-87-00, 7 (495) 645-79-39 o al +7 (495) 956-70-00 y solicite información para ponerse en contacto con los socios de Kaspersky Lab que podrán proporcionarle actualizaciones comprimidas en discos flexibles o en CD.

Advertencia.

Si solicita actualizaciones en soportes extraíbles, indique también si desea obtener las actualizaciones para los módulos de aplicación.

Puede copiar las actualizaciones desde un disco y transferirlas a un sitio FTP o HTTP, o guardarlas a una carpeta local o de red.

Seleccione el origen de actualización en la ficha **Origen de actualizaciones** (ver Figura 30).

De forma predeterminada, las actualizaciones son descargadas desde los servidores de actualización de Kaspersky Lab. No se pueden modificar las direcciones de esta lista. Durante la actualización, Kaspersky Anti-Virus for Windows Servers invoca esta lista, selecciona la primera dirección e intenta descargar los archivos desde el servidor correspondiente. Si no es posible descargar las actualizaciones desde el primer servidor, la aplicación intenta conectarse y recuperar las actualizaciones desde los servidores siguientes.

Para descargar las actualizaciones desde otro sitio FTP o HTTP:

1. Haga clic en **Agregar**.
2. En el cuadro de diálogo **Especificar un origen de actualizaciones**, seleccione el sitio FTP o HTTP o especifique la dirección IP, el nombre o la dirección URL del sitio en el campo **Origen**. Cuando selecciona un sitio FTP como origen de actualizaciones, debe introducir datos de autenticación en la dirección URL del servidor, con el formato ftp://<usuario>:<contraseña>@<host>:<puerto>.

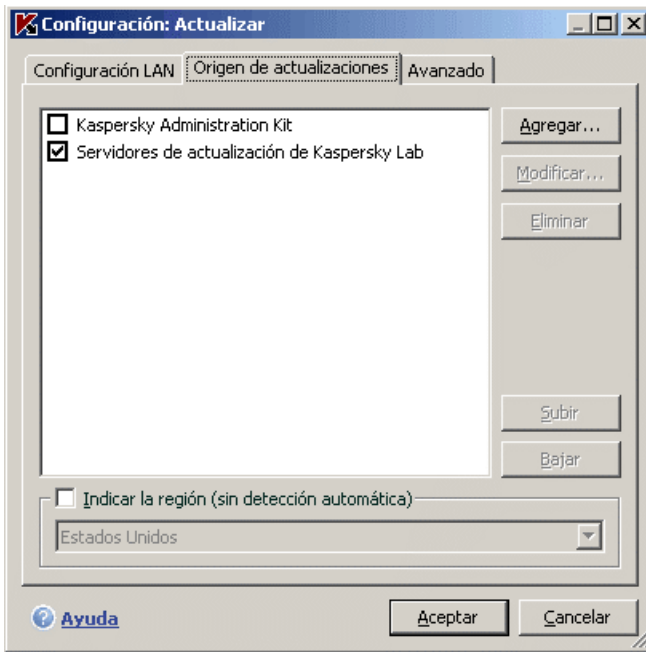


Figura 30. Selección de un origen de actualizaciones

Advertencia.

Si seleccionó un recurso ubicado fuera de la red local como origen de actualizaciones, será necesaria una conexión Internet para recuperar las actualizaciones.

Para descargar las actualizaciones desde una carpeta local:

1. Haga clic en **Agregar**.
2. En el cuadro de diálogo **Especificar un origen de actualizaciones**, seleccione una carpeta o indique su ruta completa en el campo **Origen**.

Kaspersky Anti-Virus for Windows Servers agrega los nuevos orígenes al principio de la lista y los habilita, con la casilla activada junto a su nombre.

Si se seleccionan varios recursos como origen de actualizaciones, la aplicación intenta conectarse a ellos uno tras otro, a partir del principio de lista y recupera las actualizaciones desde el primer origen disponible. Puede modificar el orden de los orígenes en la lista con los botones **Subir** y **Bajar**.

Para modificar la lista, utilice los botones **Agregar**, **Modificar** y **Quitar**. No puede modificar o eliminar los servidores de actualización de Kaspersky Lab o Kaspersky Administration Kit.

Si utiliza los servidores de actualización de Kaspersky Lab como origen de actualizaciones, puede activar la casilla que permite elegir el servidor óptimo en función de su ubicación. Kaspersky Lab posee servidores en varios países. Al elegir el servidor de actualización de Kaspersky Lab más cercano, ahorrará tiempo y la descarga de actualizaciones será más rápida.

Para elegir el servidor más cercano, active la casilla **Indicar la región (sin detección automática)** y seleccione el país más cercano a su ubicación en la lista desplegable. Si activa esta casilla, las actualizaciones se harán tomando en cuenta la región seleccionada en la lista. Esta casilla está desactivada de forma predeterminada porque la información acerca de la región actual se toma del registro del sistema operativo.

10.4.2. Selección del método y de los objetos que deben actualizarse

Cuando configura la actualización, es importante definir qué objetos serán actualizados y cómo se realiza el proceso (es decir, el modo de ejecución).

Objetos de actualización (ver Figura 31) son los componentes que serán actualizados:

- Firmas de amenazas;
- Módulos del programa.

Las firmas de amenazas siempre son actualizadas, en cambio los módulos de aplicación sólo se actualizan si activa el parámetro correspondiente.

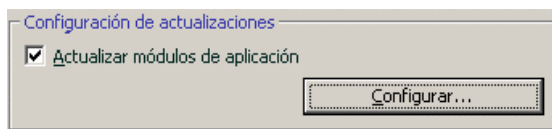


Figura 31. Selección de objetos de actualización

Si desea descargar e instalar las actualizaciones para módulos de aplicación:

Active **Actualizar módulos de aplicación** en la ventana **Actualizar**.

Si en el origen de actualizaciones existen actualizaciones para módulos de programa, la aplicación descarga las que necesita y las aplica después de reiniciar el equipo. Las actualizaciones de módulos descargadas no serán instaladas hasta que se reinicie el equipo.

Si se produce otra actualización del programa antes de haber reiniciado el equipo y antes de instalar las actualizaciones de los módulos de programa previamente descargadas, sólo se actualizarán las firmas de amenazas.

Modo de ejecución (ver Figura 32) define el método aplicado por el servicio Actualizar. Seleccione uno de los métodos siguientes en la entrada **Modo de ejecución**:

• **Automático.** Kaspersky Anti-Virus comprueba en los orígenes de actualizaciones la presencia de actualizaciones a intervalos especificados.10.4.1 en la página 108). Si encuentra nuevas actualizaciones, las descarga e instala en el equipo.

Si el origen de actualizaciones corresponde a un recurso de red, Kaspersky Anti-Virus intenta iniciar la actualización después de un cierto tiempo especificado en el paquete de actualización anterior.

Si selecciona una carpeta local como origen de actualizaciones, la aplicación intenta descargar las actualizaciones desde la carpeta local con la frecuencia indicada en el último paquete de actualización descargado. Esta opción permite a Kaspersky Lab regular la frecuencia de actualizaciones en caso de epidemias y otras situaciones de riesgo. Su aplicación recibirá las últimas actualizaciones de las bases de aplicación, ataques de red y módulos de software de forma periódica, evitando así la penetración de software malintencionado en el servidor.



Figura 32. Selección del modo de ejecución de las actualizaciones

• **Mediante planificación.** La actualización se planifica de forma que su inicio se produzca a una hora especificada. De forma predeterminada, las actualizaciones planificadas se producen cada dos horas. Para modificar la planificación predeterminada, haga clic en **Cambiar...** y aporte los cambios necesarios en la ventana abierta (para más detalles, ver 6.5 en la pág. 66). Este modo se utiliza de forma predeterminada.

• **Manual.** Con esta opción, debe iniciar el componente de actualización manualmente. Kaspersky Anti-Virus for Windows Servers le informa cuando la actualización es necesaria:

- En primer lugar, un mensaje emergente informándole de la necesidad de actualizar aparece por encima del icono de la aplicación en la barra del

sistema (si las notificaciones están activadas; ver 11.8.1 en la página 141);

- El segundo indicador de la ventana principal de la aplicación le informa de que la protección de su equipo está desfasada (ver 5.1.1 pág. 42);
- Aparece una recomendación para actualizar la aplicación en la sección de mensajes de la ventana principal de la aplicación (ver 4.3 en la página 38).

10.4.3. Configuración de la conexión

Si configuró la aplicación para recuperar actualizaciones desde los servidores de actualización de Kaspersky Lab o desde otro sitio FTP ó HTTP, le recomendamos comprobar primero sus parámetros de conexión.

Todos los parámetros están agrupados en una ficha especial: **Configuración LAN** (ver Figura 33).

Active **Usar modo FTP pasivo, si es posible** para descargar las actualizaciones desde un servidor FTP en modo pasivo (por ejemplo, a través de un cortafuegos). Si está trabajando en modo FTP activo, desactive esta casilla.

En el campo **Espera de conexión (seg.)**, asigne el tiempo de espera de la conexión con un servidor de actualización. Si la conexión no se establece después del tiempo asignado, el programa intenta conectarse al siguiente servidor de actualizaciones. Prosigue de este modo hasta conseguir una conexión o hasta agotar la lista de servidores disponibles.

Active **Usar servidor proxy** si se conecta a Internet a través de un servidor proxy y, si es necesario, especifique los parámetros siguientes:

- Seleccione los parámetros del servidor proxy utilizado durante la actualización:
 - **Configuración automática del proxy.** Al seleccionar esta opción, los parámetros del proxy son detectados automáticamente con el protocolo WPAD (Web Proxy Auto-Discovery Protocol). Si este protocolo no consigue obtener la dirección, Kaspersky Anti-Virus utiliza los parámetros de proxy definidos para Microsoft Internet Explorer.
 - **Usar parámetros personalizados del proxy:** Utiliza un proxy diferente del especificado en los parámetros de conexión del navegador. En el campo **Dirección**, indique la dirección IP o el nombre simbólico del servidor proxy y el número de puerto del proxy en el campo **Puerto**.

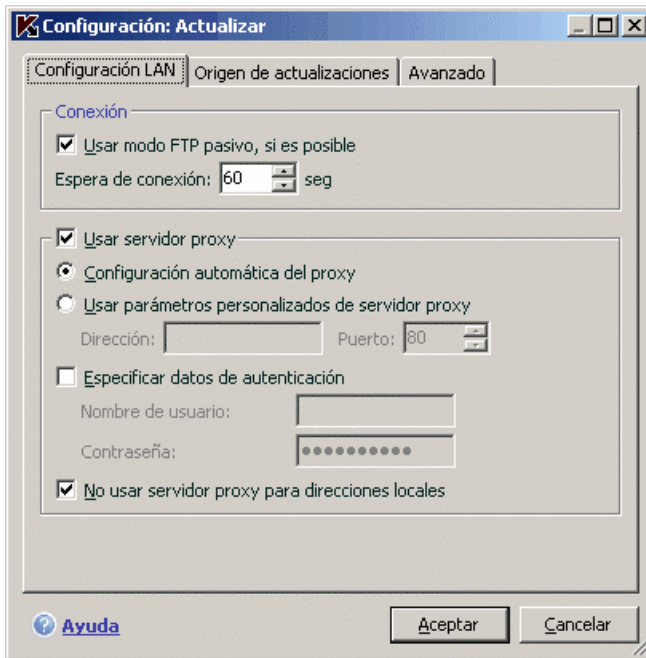


Figura 33. Configuración de la actualización

- Especifique si se requiere autenticación en el servidor proxy. *Autenticación* es el proceso que permite comprobar los datos de registro del usuario para su conexión.

Si la autenticación es obligatoria para conectarse al servidor, active la casilla **Especificar datos de autenticación** y especifique su nombre y contraseña en los campos de entrada. En este caso, se intenta primero con la autenticación NTLM y luego con la autenticación BASIC.

Si no selecciona la casilla, o si no se proporcionan datos, se intenta la autenticación NTLM con los datos de la cuenta de usuario utilizada para realizar la actualización (ver 6.4 en la página 64).

Si el servidor proxy requiere **autenticación** pero no indica el nombre de usuario o la **contraseña**, o los datos especificados no son aceptados por el servidor, se abre una ventana emergente al iniciar la actualización, preguntando por estos datos de autenticación. Si la autenticación tiene éxito, los datos de nombre de usuario y contraseña serán utilizados en las siguientes actualizaciones. En otro caso, los parámetros de autenticación se solicitan de nuevo.

Para evitar el uso de un proxy cuando el origen de actualizaciones es una carpeta local, active la casilla **No usar servidor proxy para direcciones locales.**

10.4.4. Distribución de actualizaciones

La característica de distribución de actualizaciones permite optimizar la carga de su red corporativa. La copia de actualizaciones se realiza en dos etapas:

1. Uno de los equipos de la red recupera un paquete de actualización de la aplicación y de las bases de aplicación desde los servidores Internet de Kaspersky Lab o desde otro recurso Internet donde se albergue un juego de actualizaciones recientes. Las actualizaciones recuperadas son colocadas en una carpeta de acceso público.
2. Otros equipos de la red se conectan a la carpeta de acceso público para recuperar las actualizaciones de aplicación.

Para activar la distribución de actualizaciones, active la casilla **Carpeta de distribución de las actualizaciones** en la ficha **Avanzado** (ver Figura 34), y en el campo inferior, indique la carpeta compartida donde se colocarán las actualizaciones. Puede indicar la ruta manualmente o en la ventana abierta con **Examinar**. Si la casilla está activa, las actualizaciones se copiarán automáticamente a la carpeta indicada cuando se obtengan.

También puede especificar el método de distribución de actualizaciones:

- *completo*, permite copiar las bases de aplicación y las actualizaciones de módulos de todas las aplicaciones Kaspersky Lab 6.0. Para seleccionar actualizaciones completas, active la casilla **Copiar actualizaciones de todos los componentes**;
- *personalizado*, en el que sólo se copian las bases de aplicación y las actualizaciones de los componentes de Kaspersky Anti-Virus 6.0 instalados. Si desea seleccionar este método, debe desactivar la casilla **Copiar actualizaciones de todos los componentes**.

Si desea que otros equipos de la red se actualicen desde la carpeta que contiene la copia de las actualizaciones de Internet, siga los pasos siguientes:

1. Autorice el acceso público a esta carpeta.
2. Especifique la carpeta compartida como origen de actualizaciones en los equipos de la red, en la Configuración de las actualizaciones.

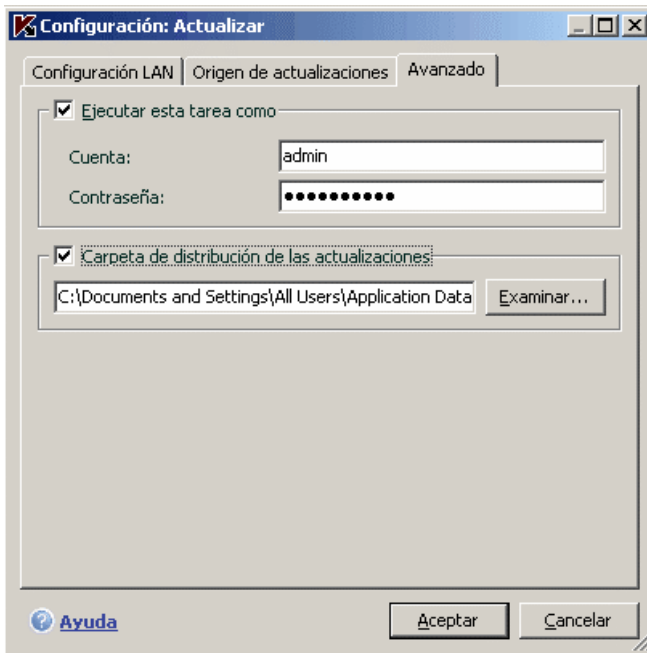


Figura 34. Configuración de la carpeta de actualizaciones

10.4.5. Acción después de actualizar

Cada actualización de las bases de aplicación incluye nuevos registros que protegen su equipo contra las amenazas más recientes.

Kaspersky Lab le recomiendan analizar los *objetos en cuarentena* y los *objetos de inicio* después de actualizar la base de datos.

¿Por qué deben analizarse estos objetos?

La zona de cuarentena contiene objetos que fueron marcados como sospechosos o posiblemente infectados (ver 11.1 pág. 119). Con la última versión de las bases de aplicación, es posible que Kaspersky Anti-Virus for Windows Servers pueda identificar la amenaza y eliminarla.

De forma predeterminada, la aplicación analiza los objetos en cuarentena después de cada actualización de las bases de aplicación. También recomendamos examinar regularmente los objetos en cuarentena porque su estado puede cambiar después de varios análisis. Algunos objetos pueden entonces ser restaurados a sus ubicaciones de origen para seguir trabajando con ellos.

Para desactivar los análisis de objetos en cuarentena, desactive la casilla **Analizar de nuevo la cuarentena** en la sección **Acción después de actualizar**.

Los objetos de inicio son críticos para la seguridad de su equipo. Si alguno de ellos queda infectado por una aplicación dañina, puede causar incluso un fallo de arranque del sistema operativo. Kaspersky Anti-Virus for Windows Servers cuenta con una tarea de análisis integrada para objetos de inicio (ver Capítulo 8 en la página 85). Le recomendamos definir una planificación para esta tarea para ejecutarla automáticamente después de cada actualización de las bases de aplicación (ver 6.5 en la pág. 66).

CAPÍTULO 11. OPCIONES AVANZADAS

Kaspersky Anti-Virus for Windows Servers dispone de otras características que amplían su funcionamiento.

Mientras trabaja, el programa coloca algunos objetos en zonas de almacenamiento especiales, para maximizar la protección de los datos y minimizar las pérdidas.

- La zona de respaldo contiene copias de los objetos modificados o eliminados por Kaspersky Anti-Virus for Windows Servers (ver 11.2 pág. 122). Si algún objeto contenía información importante que no pudo ser guardada durante el proceso antivirus, siempre podrá restaurar el objeto a partir de su copia de seguridad.
- La cuarentena contiene objetos potencialmente infectados que no pudieron procesarse con las firmas actuales de amenazas (ver 11.1 en la página 119).

Se recomienda que examine periódicamente esta lista de objetos almacenados. Es posible que algunos ya estén desfasados o hayan sido restaurados.

Las opciones avanzadas incluyen varias características útiles. Por ejemplo:

- El soporte técnico proporciona asistencia completa para Kaspersky Anti-Virus for Windows Servers (ver 11.6 pág. 137). Kaspersky le ofrece varias vías de soporte, como soporte en línea y un foro de preguntas y sugerencias de los usuarios del programa.
- Las notificaciones informan a los usuarios de los principales eventos de Kaspersky Anti-Virus for Windows Servers (ver 11.8.1 en la página 141). Pueden ser eventos de tipo informativos o errores críticos que deben eliminarse inmediatamente.
- El componente de autoprotección protege los propios archivos del programa contra modificaciones o daños de piratas, bloquea el uso de las características del programa y restringe los derechos administrativos de su equipo para evitar que otros usuarios utilicen ciertas características de Kaspersky Anti-Virus for Windows Servers (ver 11.8.2 pág. 145). Por ejemplo, modificar el nivel de protección puede influir significativamente en la seguridad de los datos de su equipo.
- El administrador de llaves de licencia puede obtener información detallada sobre la licencia utilizada, activar su copia del programa y administrar los archivos de licencia (ver 11.5 pág. 135).

El programa también dispone de una sección de Ayuda (ver 11.4 en la página 133) además de informes detallados (ver 11.3 en la página 125) sobre el funcionamiento del componente Antivirus de archivos y las tareas de análisis antivirus.

También puede cambiar la apariencia de Kaspersky Anti-Virus for Windows Servers y personalizar la interfaz del programa (ver 11.7 en la página 138).

Las secciones siguientes describen estas características con más detalle.

11.1. Cuarentena para objetos potencialmente infectados

La **cuarentena** es una zona de almacenamiento especial donde se guardan objetos posiblemente infectados por virus.

Los **objetos potencialmente infectados** son objetos sospechosos de estar infectados por algún virus o su mutación.

¿Por qué *potencialmente infectado*? No siempre es posible determinar exactamente a qué se debe la infección de un objeto.

- El código del objeto analizado recuerda una amenaza conocida aunque parcialmente modificada.

La base de amenazas contiene firmas que han sido en su momento estudiadas por Kaspersky Lab. Si un programa dañino ha sido modificado sin que sus cambios hayan sido incluidos en la base de firmas, Kaspersky Anti-Virus for Windows Servers clasifica el objeto modificado por el programa dañino como potencialmente infectado e indica a qué amenaza se parece su infección.

- La estructura del código del objeto detectado evoca la de un programa malintencionado, pero nada similar aparece registrado dentro de las firmas de amenazas.

Puede perfectamente ser un nuevo tipo de amenaza, por lo que Kaspersky Anti-Virus for Windows Servers clasifica este objeto como potencialmente infectado.

El analizador de *código heurístico* detecta virus potenciales. Este mecanismo es perfectamente eficaz y rara vez produce falsos positivos.

Un objeto potencialmente infectado es detectado y colocado en cuarentena por el componente Antivirus de archivos o en el transcurso de un análisis antivirus.

Para colocar un objeto en la cuarentena directamente, haga clic en **Cuarentena** en el mensaje de notificación mostrado cuando se detecta un objeto potencialmente infectado.

Cuando coloca un objeto en Cuarentena, éste es movido, no copiado. El objeto es eliminado del disco o del mensaje y guardado en la carpeta de cuarentena. Los archivos en cuarentena se guardan con un formato especial y no son peligrosos.

11.1.1. Acciones con objetos en cuarentena

El número total de objetos colocados en la cuarentena se obtiene desde la entrada **Archivos de datos** de la entrada **Servicio**. En la parte derecha de la ventana se encuentra una sección *Cuarentena* que indica:

- el número de objetos potencialmente infectados detectados durante el funcionamiento de Kaspersky Anti-Virus for Windows Servers;
- el tamaño actual de la cuarentena.

También puede eliminar todos objetos en la cuarentena con **Limpiar...**. Observe que de este modo, también se eliminan los archivos de respaldo y los informes.

Para trabajar con objetos en cuarentena:

haga clic en cualquier punto del cuadro **Cuarentena**.

La ficha **Cuarentena** le permite tomar las acciones siguientes (ver Figura 35):

- Mover un archivo a la cuarentena, cuando sospecha que está infectado sin que el programa lo detecte. Para ello, haga clic en **Agregar** y en la ventana de selección estándar, seleccione el archivo. El archivo se agrega a la lista con el estado *En cuarentena por el usuario*.
- Analizar y reparar todos los objetos potencialmente infectados en la cuarentena con las bases de aplicación actual, con **Analizar todo**.

El análisis y desinfección de un objeto en cuarentena puede cambiar su estado a *infectado*, *posiblemente infectado*, *falsa alarma*, *correcto*, etc.

El estado *infectado* significa que el objeto ha sido identificado como infectado pero no pudo ser neutralizado. Se recomienda eliminar estos objetos.

Todos los objetos con el estado *falsa alarma* pueden restaurarse sin inquietarse, porque su estado previo como *posiblemente infectado* no fue confirmado por el programa después de un nuevo análisis.

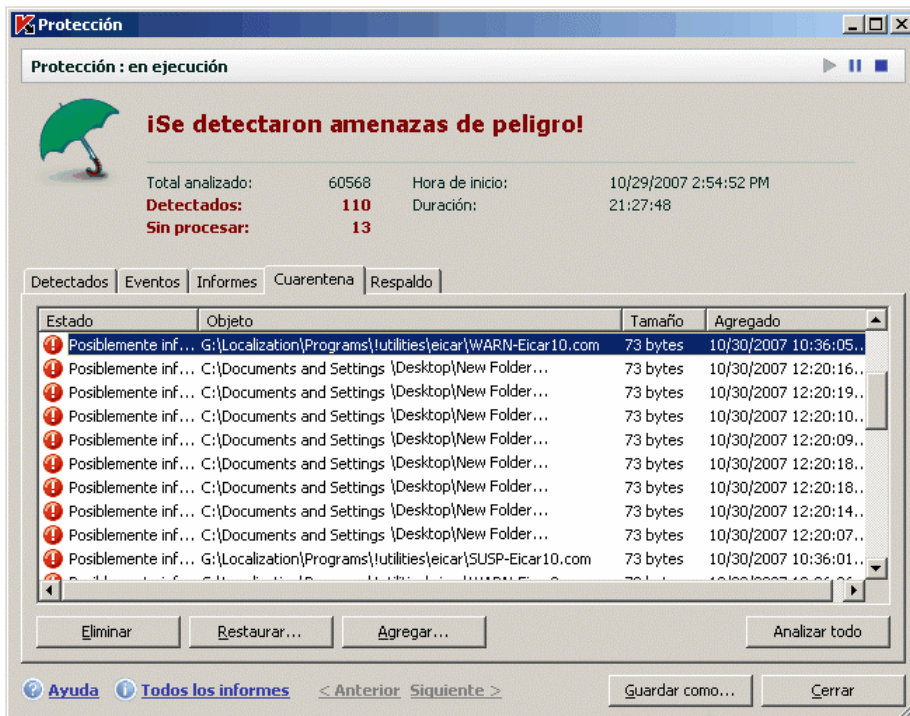


Figura 35. Lista de objetos en cuarentena

- Restaurar archivos desde la cuarentena, hacia la carpeta seleccionada por el usuario o su carpeta de origen (opción predeterminada). Para restaurar un objeto, selecciónelo en la lista y haga clic en **Restaurar**. Cuando restaura objetos en cuarentena que provienen de archivos comprimidos, bases o adjuntos de correo, debe también especificar el directorio de destino para restaurarlos.

Sugerencia:

Le recomendamos restaurar sólo los objetos con los estados *falsa alarma*, *correcto* y *desinfectado*, porque la restauración de los demás objetos podría originar la infección de su equipo.

- Eliminar cualquier objeto o grupo de objetos seleccionados en la cuarentena. Elimine sólo los archivos que no se pueden reparar. Para eliminar estos objetos, selecciónelos en la lista y haga clic en **Eliminar**.

11.1.2. Configuración de la cuarentena

Puede configurar los parámetros de presentación y funcionamiento de la cuarentena, en particular:

- Definir análisis automáticos de objetos en cuarentena después de cada actualización de las bases de aplicación (para más detalles, ver 10.4.4 pág. 115).

Advertencia:

El programa no podrá analizar los objetos en cuarentena inmediatamente, después de actualizar las bases de aplicación, si se encuentra trabajando con la cuarentena.

- Definir el tiempo de almacenamiento máximo en cuarentena.

El tiempo de conservación predeterminado es de 30 días, tras los cuales los datos son eliminados. Puede modificar el periodo máximo de almacenamiento en cuarentena o anular completamente esta restricción.

Para ello:

1. Abra la ventana de configuración de Kaspersky Anti-Virus for Windows Servers con un clic en el botón Configuración de la ventana principal de la aplicación.
2. Seleccione **Archivos de datos** en el árbol de configuración.
3. En la sección **Cuarentena y Respaldo** (ver Figura 36), indique el tiempo tras el cual se eliminarán automáticamente los objetos en cuarentena. También puede desactivar la casilla con la opción de eliminación automática.

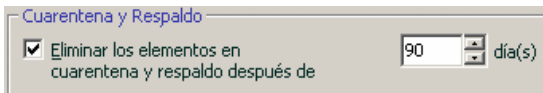


Figura 36. Configuración del periodo de conservación en cuarentena

11.2. Copias de respaldo de objetos peligrosos

A veces la desinfección daña la integridad de los objetos. Si un archivo desinfectado contenía información importante que, en parte o en totalidad, es

irrecuperable, puede intentar restaurar el objeto original a partir de su copia de respaldo.

Una **copia de respaldo** es una copia del objeto peligroso original, creada antes de reparar o eliminar el objeto. Se guarda en la zona de respaldo.

La **zona de respaldo** es un almacén especial que contiene copias de respaldo de los objetos peligrosos. Los archivos respaldados se guardan con un formato especial y no son peligrosos.

11.2.1. Operaciones con la zona de respaldo

El número total de copias de los objetos colocadas en el respaldo se muestra en la entrada **Archivos de datos** de la entrada **Servicio** de la ventana principal. En la parte derecha de la ventana se encuentra la sección *Respaldo* que indica:

- el número de copias de respaldo de objetos creadas por Kaspersky Anti-Virus for Windows Servers;
- el tamaño actual de la zona de respaldo.

También puede eliminar todas las copias de respaldo con **Limpiar...** Observe que de este modo, también se eliminan los archivos de cuarentena y los informes.

Para operar con copias de objetos peligrosos:

haga clic en cualquier punto del cuadro **Respaldo**.

Una lista de las copias de respaldo se muestra en la ficha **Respaldo** (ver Figura 37). La información siguiente está disponible para cada copia: el nombre y ruta completa de la ubicación de origen del objeto, el estado atribuido por el análisis y su tamaño.

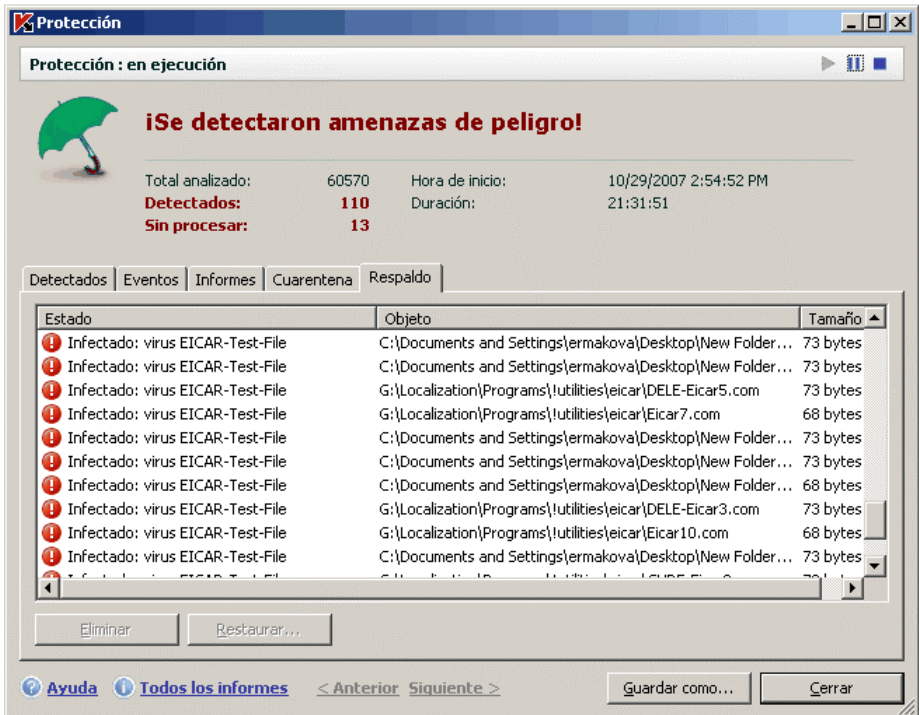


Figura 37. Copias de respaldo de objetos desinfectados o eliminados

Puede restaurar las copias seleccionadas con **Restaurar**. El objeto es restaurado a partir de la copia de respaldo, con su nombre anterior a la desinfección.

Si en la ubicación de origen ya existe un objeto con el mismo nombre (esto es posible con un objeto restaurado desde una copia anterior a la desinfección), se muestra la advertencia correspondiente. Puede modificar la ubicación o renombrar el objeto restaurado.

Le recomendamos analizar los objetos de respaldo inmediatamente después de restaurarlos. Es posible que con las firmas actualizadas, pueda reparar el archivo sin dañarlo.

No recomendamos restaurar copias de respaldo de objetos si no es absolutamente necesario. Esto podría causar la infección de su equipo.

Le recomendamos examinar y vaciar periódicamente la zona de respaldo con **Eliminar**. También puede configurar el programa para que elimine

automáticamente las copias más antiguas del respaldo (ver 11.2.2 en la página 125).

11.2.2. Configuración de los parámetros de respaldo

Puede definir el periodo máximo de conservación de la zona de respaldo.

El tiempo de conservación predeterminado es de 90 días, tras los cuales las copias de respaldo son eliminadas. Puede modificar el periodo de almacenamiento o anular completamente esta restricción. Para ello:

1. Abra la ventana de configuración de Kaspersky Anti-Virus for Windows Servers con un clic en el botón Configuración de la ventana principal de la aplicación.
2. Seleccione **Archivos de datos** en el árbol de configuración.
3. Establezca el tiempo de conservación de copias de respaldo en el repositorio en la sección **Cuarentena y Respaldo** (ver Figura 36) en la parte derecha de la ventana. También puede desactivar la casilla con la opción de eliminación automática.

11.3. Informes

Las operaciones del componente Antivirus de archivos, de las tareas antivirus y de actualización quedan registradas en informes.

El número total de informes creados por el programa en un momento dado y su tamaño total aparece en la entrada **Archivos de datos** en la entrada **Servicio** de la ventana principal del programa. Esta información se muestra en la sección *Informes*.

Para mostrar los informes:

Haga clic en cualquier punto del cuadro *Informes* para abrir la ventana Protección, con el resumen de los datos de protección proporcionados por la aplicación. La ventana se abre en la ficha **Informes** (ver Figura 38).

La ficha Informes contiene el listado de los informes más recientes del componente Antivirus de archivos y de las tareas de análisis antivirus ejecutadas durante la sesión actual de Kaspersky Anti-Virus for Windows Servers. Este estado aparece en relación al componente Antivirus de archivos o a la tarea, por ejemplo, *interrumpido* o *terminado*. Si desea ver el histórico completo del informe

creado durante la sesión actual del programa, active la casilla **Mostrar el histórico de informes**.

Protección : en ejecución

¡Se detectaron amenazas de peligro!

Total analizado: 60573 Hora de inicio: 10/29/2007 2:54:52 PM
Detectados: 110 Duración: 21:35:46
Sin procesar: 13

Componente	Estado	Iniciar	Terminar	Tamaño
Análisis antivirus	terminado	10/30/2007 12:19:09...	10/30/2007 12:20:22...	12.3 KB
Análisis antivirus	terminado	10/30/2007 10:35:53...	10/30/2007 10:36:09...	21.4 KB
Análisis antivirus	terminado	10/30/2007 10:35:29...	10/30/2007 10:36:10...	31.7 KB
Análisis antivirus	terminado	10/30/2007 10:34:48...	10/30/2007 10:36:10...	23.2 KB
Antivirus de archivos	en ejecución	10/29/2007 2:54:52 PM		56.8 KB
Analizar zonas críticas	terminado	10/30/2007 9:50:49 AM	10/30/2007 10:01:17...	0 bytes
Analizar objetos de inicio	terminado	10/29/2007 2:57:05 PM	10/29/2007 2:58:01 PM	0 bytes
Analizar Mi PC	terminado	10/30/2007 10:58:41...	10/30/2007 11:51:15...	0 bytes
Actualizar	error	10/30/2007 10:55:15...	10/30/2007 10:55:36...	159.9 KB
Actualizar	error	10/30/2007 9:52:16 AM	10/30/2007 9:53:04 AM	159.9 KB
Actualizar	error	10/30/2007 8:55:05 AM	10/30/2007 8:55:22 AM	159.9 KB

Mostrar el histórico de informes Detalles...

Ayuda Todos los informes < Anterior Siguiente > Guardar como... Cerrar

Figura 38. Informes sobre componentes

Para revisar todos los eventos registrados en el informe del componente Antivirus de archivos o de una tarea:

Seleccione el nombre del componente Antivirus de archivos o de la tarea en la ficha **Informes** y haga clic en **Detalles**.

Se abre entonces una ventana con información detallada sobre la actividad del componente Antivirus de archivos o de la tarea seleccionado. Las estadísticas de actividad se muestran en la parte superior de la ventana y la información detallada se facilita en las diferentes fichas centrales.

- La ficha **Detectados** contiene una lista de objetos peligrosos detectados por el componente Antivirus de archivos o por una tarea de análisis antivirus.
- La ficha **Eventos** muestra los eventos del Antivirus de archivos o de la tarea.

- La ficha **Estadísticas** contiene estadísticas detalladas sobre todos los objetos analizados.
- La ficha **Configuración** muestra los parámetros utilizados por el componente Antivirus de archivos, el análisis antivirus o la actualización de las bases de aplicación.
- La ficha **Usuarios vetados** muestra una lista de equipos vetados cuando intentaban copiar archivos infectados o posiblemente infectados al servidor.

Puede exportar el informe completo a un archivo de texto. Esto puede ser útil cuando ocurre un error durante la actividad del componente Antivirus de archivos o al terminar una tarea, que no puede resolver y necesita la asistencia de nuestro Servicio de soporte técnico. En este caso, debe enviar el informe en formato .txt al Soporte técnico para que nuestros especialistas puedan estudiar el problema en detalle y resolverlo tan pronto como resulte posible.

Para exportar el informe a un archivo de texto,

haga clic en **Guardar como** y especifique dónde desea guardar el archivo de informe.

Después de trabajar con el informe, haga clic en **Cerrar**.

Existe un botón Acciones en todas las fichas (excepto las fichas **Configuración** y **Estadísticas**) que permite definir respuestas a objetos de la lista. Cuando hace clic en él, se abre un menú contextual con la opciones siguientes (dependiendo del componente, el menú varía: la lista de todas las opciones posibles se indica a continuación):

Desinfectar: intenta reparar un objeto peligroso. Si el objeto no fue desinfectado con éxito, puede dejarlo en la lista y analizarlo más tarde con firmas actualizadas, o puede eliminarlo. Puede aplicar esta acción a un objeto individual de la lista o a varios objetos seleccionados.

Descartar: elimina la entrada del objeto detectado en el informe.

Agregar a zona de confianza: excluye el objeto de la protección. Se abrirá una ventana con una regla de exclusión para el objeto.

Ir al archivo: abre la carpeta donde está ubicado el objeto dentro del Explorador de Microsoft Windows.

Neutralizar todo: neutraliza todos los objetos de la lista. Kaspersky Anti-Virus for Windows Servers intentará procesar los objetos con las bases de aplicación.

Descartar todo: limpia el informe de objetos detectados. Cuando utiliza esta función, todos los objetos peligrosos detectados permanecerán en su equipo.

Buscar en www.viruslist.com: abre la descripción del objeto en la Enciclopedia de virus del sitio Internet de Kaspersky Lab.

Buscar en www.google.com: busca información acerca del objeto con este motor de búsqueda.

Buscar: introduce criterios de búsqueda por nombre o estado de los objetos en la lista.

Además, puede presentar la información dentro de la ventana en orden creciente o decreciente en cada columna, para ello, haga clic en su encabezado.

Para procesar los objetos peligrosos detectados por Kaspersky Anti-Virus, haga clic en **Neutralizar** (para un objeto o para un grupo de objetos seleccionados) o en **Neutralizar todo** (para procesar todos los objetos de la lista). Cuando se detecta un objeto, se muestra una notificación en pantalla, donde puede decidir qué acciones se tomarán a continuación.

Si activa la casilla **Aplicar a todo** en la ventana de notificación, la acción seleccionada se aplicará a todos los objetos con el mismo estado que hayan sido seleccionados en la lista.

11.3.1. Configuración de los parámetros de informe

Para configurar los parámetros para crear y guardar informes:

Abra la ventana de configuración de Kaspersky Anti-Virus for Windows Servers con un clic en el botón Configuración de la ventana principal de la aplicación.

1. Seleccione **Archivos de datos** en el árbol de configuración.
2. Modifique los parámetros en el cuadro **Informes** (ver Figura 39) como sigue:
 - active o desactive el informe de eventos informativos. En general estos eventos no son importantes para la seguridad. Para registrar los eventos, active la casilla **Registrar los eventos sin gravedad**;
 - Elija sólo guardar en el informe los eventos ocurridos desde la última ejecución de la tarea. Esto ahorra espacio en disco al reducir el tamaño del informe. Si la casilla **Conservar sólo los eventos recientes** está activada, la información del informe se actualizará cada vez que reinicie la tarea. Sin embargo, sólo se reemplaza la información sin importancia.
 - Defina el plazo de conservación de los informes. De forma predeterminada, el tiempo de conservación de los informes es de 90 días, tras los cuales son eliminados. Puede modificar el

periodo máximo de almacenamiento o anular completamente esta restricción.

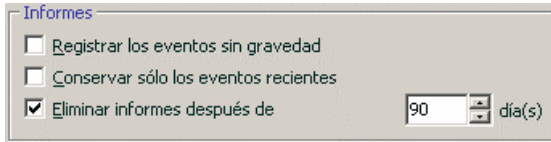


Figura 39. Configuración de los parámetros de informe

11.3.2. Detectados (ficha)

Esta ficha (ver Figura 40) contiene una lista de objetos peligrosos detectados por Kaspersky Anti-Virus for Windows Servers. Se indica el nombre completo de cada objeto, junto con el estado asignado por el programa cuando lo analizó o procesó.

Si desea que la lista incluya tanto los objetos peligrosos como los que han sido neutralizados con éxito, active **Mostrar los objetos neutralizados**.

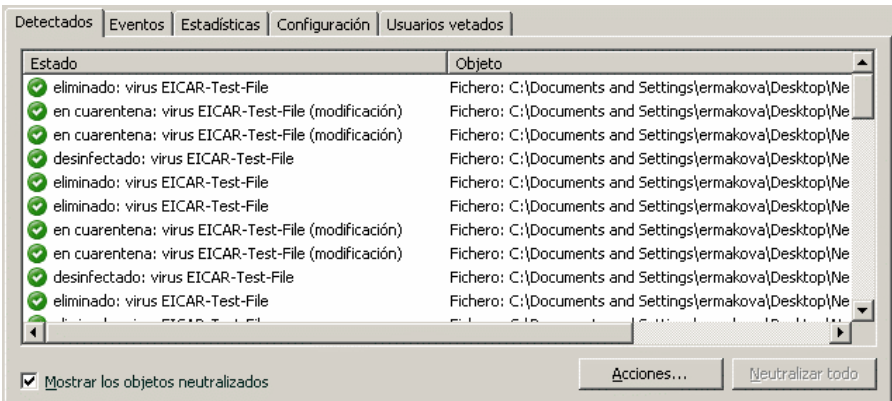


Figura 40. Lista de objetos peligrosos detectados

Para procesar los objetos peligrosos detectados por Kaspersky Anti-Virus, haga clic en **Neutralizar** (para un objeto o para un grupo de objetos seleccionados) o en **Neutralizar todo** (para procesar todos los objetos de la lista). Cuando se detecta un objeto, se muestra una notificación en pantalla, donde puede decidir qué acciones se tomarán a continuación.

Si activa la casilla **Aplicar a todo** en la ventana de notificación, la acción seleccionada se aplicará a todos los objetos con el mismo estado que hayan sido seleccionados en la lista.

11.3.3. **Eventos (ficha)**

Esta ficha (ver Figura 41) ofrece una lista completa de todos los eventos importantes ocurridos durante el funcionamiento del componente Antivirus de archivos, los análisis antivirus y las actualizaciones de las bases de aplicación.

Estos eventos pueden ser los siguientes:

Los eventos críticos que son eventos de gravedad que apuntan a problemas de funcionamiento del programa o vulnerabilidades en su equipo. Por ejemplo, *virus detectado*, *error de operación*.

Los eventos importantes son eventos que debe investigar, porque reflejan situaciones importantes en el funcionamiento del programa. Por ejemplo, *interrumpido*.

Los mensajes informativos sirven como referencia y en general no contienen información importante. Por ejemplo, *Correcto*, *no procesado*. Estos eventos sólo se reflejan en el informe de eventos cuando la casilla **Ver todos los eventos** está activada.

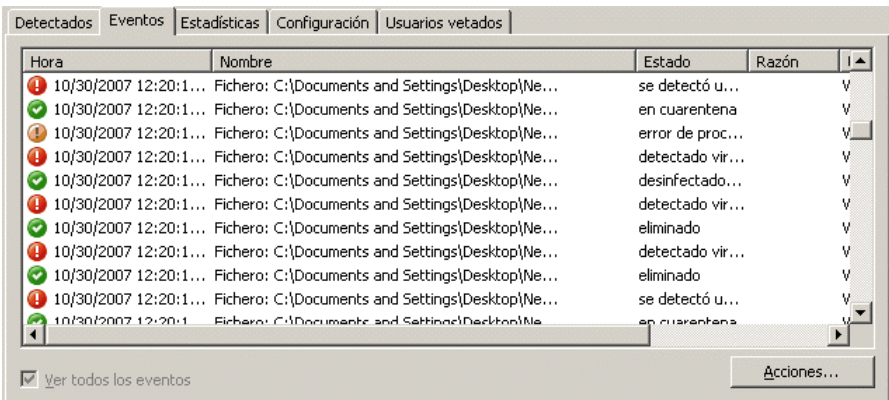


Figura 41. Eventos procesados por el componente

El formato de presentación de la ficha Eventos puede variar en función del componente o tarea. Por ejemplo, la información siguiente se suministra para las tareas de actualización:

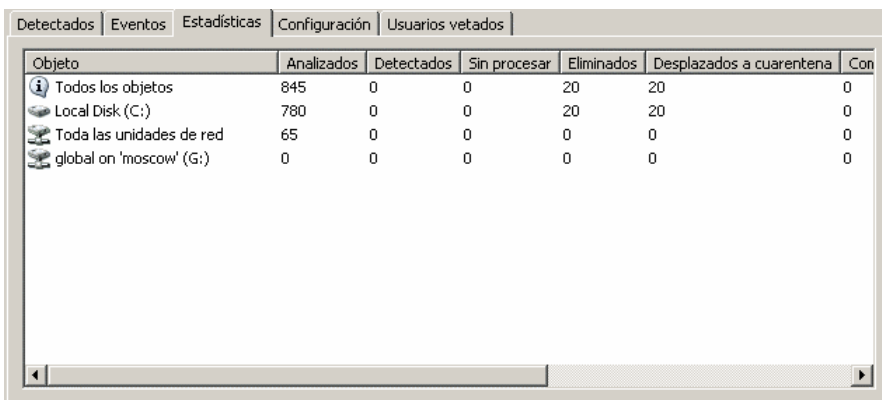
- Nombre del evento
- Nombre del objeto afectado por el evento
- Hora de activación del evento.
- Tamaño del archivo cargado.

En el caso de tareas de análisis antivirus, el informe de eventos contiene el nombre y estado atribuido al objeto analizado tras el análisis o procesado.

11.3.4. Estadísticas (ficha)

Esta ficha (ver Figura 42) proporciona estadísticas detalladas acerca del componente Antivirus de archivos y las tareas de análisis antivirus. Aquí también puede saber:

- Cuántos objetos fueron analizados en busca de objetos peligrosos durante esta sesión del componente Antivirus de archivos o tras terminar la tarea. Se muestra el número de paquetes y archivos comprimidos, los objetos protegidos con contraseña y dañados.
- Cuántos objetos peligrosos fueron detectados, no desinfectados, eliminados o movidos a cuarentena.



Objeto	Analizados	Detectados	Sin procesar	Eliminados	Desplazados a cuarentena	Con
Todos los objetos	845	0	0	20	20	0
Local Disk (C:)	780	0	0	20	20	0
Toda las unidades de red	65	0	0	0	0	0
global on 'moscow' (G:)	0	0	0	0	0	0

Figura 42. Estadísticas de actividad del componente

11.3.5. Configuración (ficha)

La ficha **Configuración** (ver Figura 43) presenta el conjunto de los parámetros aplicables al componente Antivirus de archivos, a los análisis antivirus y a las actualizaciones del programa. Le informa del nivel de seguridad del componente Antivirus de archivos o de los análisis antivirus, qué acciones se toman con los objetos peligrosos o los parámetros utilizados para las actualizaciones del programa. Utilice el vínculo [Cambiar configuración](#) para configurar rápidamente el componente.

Puede configurar parámetros avanzados para tareas antivirus:

- Establecer la prioridad de las tareas de análisis cuando el procesador está sobrecargado. La sección **Facilitar recursos para otras aplicaciones** está activada de forma predeterminada. Esta característica permite vigilar la carga del procesador y de los subsistemas de disco para conocer la actividad de otras aplicaciones. Si la carga de CPU aumenta hasta impedir que las aplicaciones de usuario puedan operar normalmente, el programa reduce su actividad de análisis. Esto aumenta el tiempo de análisis pero libera recursos para las demás aplicaciones del usuario.

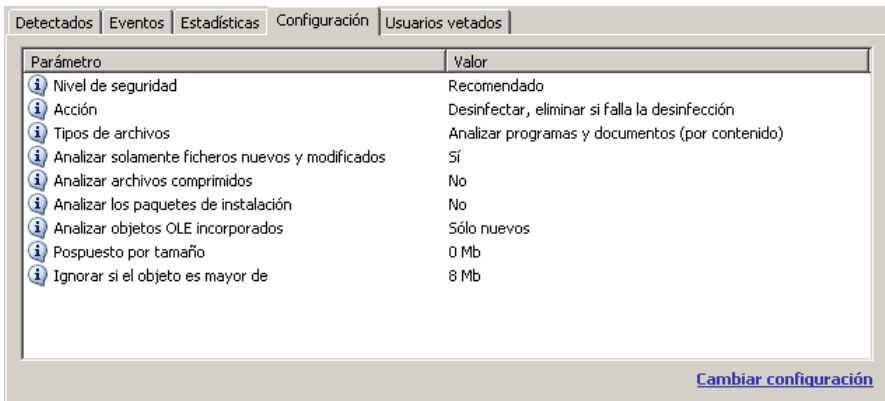


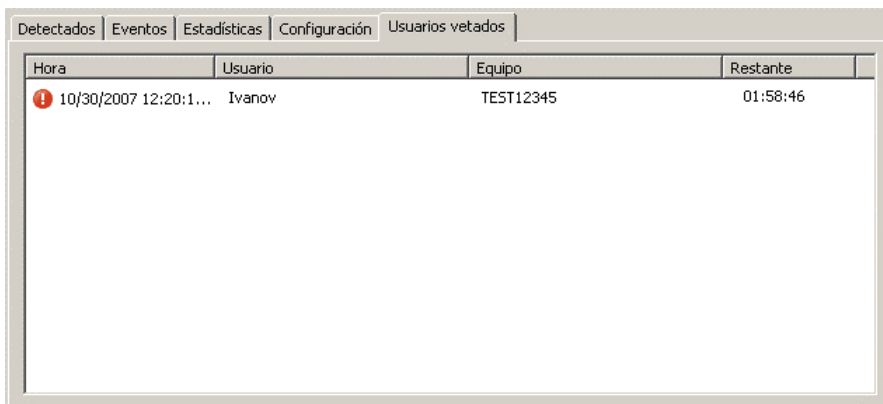
Figura 43. Configuración del componente

- Definir el comportamiento del equipo después de terminar un análisis antivirus. Por configuración, puede apagar, reiniciar, suspender o poner el equipo en espera. Para seleccionar una opción, haga clic en el vínculo hasta mostrar la opción deseada.

11.3.6. *Usuarios vetados (ficha)*

(ver Figura 44). Todos los equipos que intentan copiar un archivo infectado o potencialmente infectado al servidor son bloqueados. También es posible vetar un equipo relacionado con el procesamiento del archivo (desinfección o eliminación).

Esta ficha le indica qué equipos han sido vetados, así como la fecha y la hora en que ocurrió, y cuántas horas quedan hasta que concluya el veto.



Hora	Usuario	Equipo	Restante
! 10/30/2007 12:20:1...	Ivanov	TEST12345	01:58:46

Figura 44. Lista de usuarios vetados

11.4. Información general acerca del programa

La información general acerca del programa aparece en la sección **Servicio** de la ventana principal (ver Figura 45).



Figura 45. Información del programa, llave de licencia y sistema operativo instalados

Toda la información está dividida en tres secciones:

- La versión del programa, la fecha de última actualización y el número de amenazas conocidas hasta la fecha se muestran en el cuadro **Información del producto**.
- La información básica del sistema operativo instalado en su equipo se muestra en el cuadro **Información del sistema**.
- La información básica sobre la licencia adquirida para Kaspersky Anti-Virus aparece en el cuadro **Información de llave licencia**.

Necesitará toda esta información para ponerse en contacto con el Soporte técnico de Kaspersky Lab (ver 11.6 pág. 137).

11.5. Administración de licencias

Kaspersky Anti-Virus for Windows Servers necesita una *llave de licencia* para funcionar. Recibe una llave cuando adquiere el programa. Le da derecho a utilizar el programa a partir del día en que instala la llave.

Sin una llave de licencia, y si la versión de evaluación del programa no ha sido activada, Kaspersky Anti-Virus se ejecutará en modo limitado a una sola actualización. El programa no descargará nuevas actualizaciones.

Si activó la versión de evaluación del programa, tras este plazo, Kaspersky Anti-Virus dejará de funcionar.

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

Para evitar la infección de su equipo por nuevos virus, le recomendamos renovar su licencia para Kaspersky Anti-Virus for Windows Servers. El programa le notificará con dos semanas de antelación de la cancelación de su licencia y, durante estas dos semanas, el programa mostrará dicho mensaje cada vez que lo abra.

Para renovar su licencia, debe adquirir e instalar una nueva llave de licencia o introducir un código de activación de la aplicación. Para ello:

Póngase en contacto con el proveedor del producto y compre una llave de licencia o un código de activación.

o bien:

Compre una llave de licencia o un código de activación directamente en Kaspersky Lab, para ello haga clic en el vínculo [Adquirir licencia](#) en la ventana de la llave de licencia (ver Figura 46). Complete el formulario en nuestro sitio Internet. Después de realizar el pago, le enviaremos un vínculo a la dirección de correo indicada en el formulario de pedido. El vínculo le permite descargar la llave de licencia u obtener un código de activación de la aplicación.

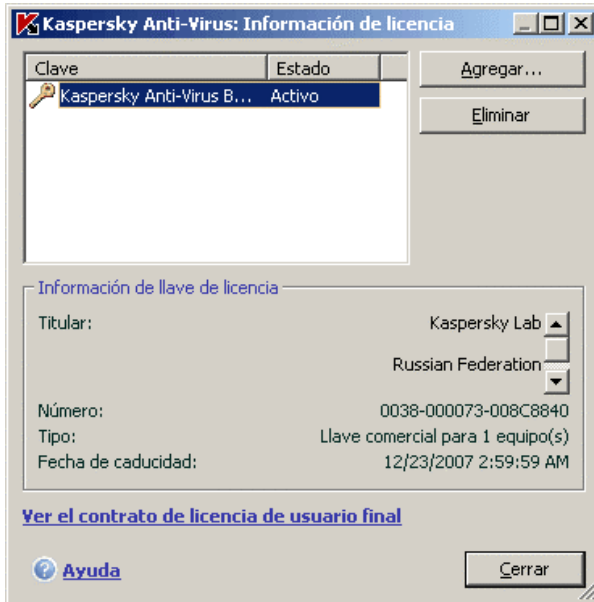


Figura 46. Información de licencia

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

La información acerca de la llave de licencia actual está disponible en la sección **Información de llave de licencia** de la entrada **Servicio** de la ventana principal de la aplicación. Para abrir la ventana del administrador de licencias, haga clic en cualquier punto del cuadro. En la ventana abierta (ver Figura 46), puede ver la información acerca de la llave actual, agregar una llave o eliminarla.

Cuando selecciona una llave en la lista del cuadro **Información de llave de licencia**, se ve la información acerca del número, tipo y caducidad de la licencia. Para agregar una nueva llave de licencia, haga clic en **Agregar** y active la aplicación con el Asistente de activación (ver 11.5 en la pág. (ver 11.6 pág. 137)). Para eliminar una llave de la lista, haga clic en **Eliminar**.

Para examinar los términos del CLUF, haga clic en Ver el contrato de licencia de usuario final. Para obtener una licencia por Internet en el sitio de Kaspersky Lab, haga clic en Adquirir licencia.

11.6. Soporte técnico

Kaspersky Anti-Virus for Windows Servers ofrece un amplio abanico de soluciones a sus preguntas y problemas relacionados con el funcionamiento del programa. Las encontrará en la entrada **Soporte** (ver Figura 47) en la entrada **Servicio**.

En función del problema, disponemos de varios servicios de asistencia técnica:

Foro de usuarios. Este recurso es una sección separada del sitio de Kaspersky Lab y contiene preguntas, comentarios y sugerencias escritas por los usuarios del programa. Puede examinar los temas básicos del foro y dejar sus propios comentarios. También puede encontrar la respuesta a su pregunta.

Para tener acceso a este recurso, utilice el vínculo [Foro de usuarios](#).

Base de conocimientos. Este recurso es también una sección separada del sitio Internet de Kaspersky Lab y contiene las recomendaciones del Soporte técnico para el uso del software de Kaspersky Lab, con respuestas a las preguntas frecuentes. Intente encontrar una respuesta a su pregunta o una solución a sus problemas dentro de este recurso.

Para obtener soporte técnico en línea, utilice el vínculo [Base de conocimientos](#).

Comentarios acerca del funcionamiento del programa. Este servicio está diseñado para enviar comentarios sobre el programa o para describir un problema surgido durante el funcionamiento del programa. Debe completar un formulario especial en el sitio Internet de la organización que describe la situación en detalle. Para poder atender mejor el problema, Kaspersky Lab necesitará cierta información sobre su sistema. Puede describir personalmente su sistema o recuperar automáticamente la información en su equipo.

Para abrir el formulario de comentarios, utilice el vínculo [Enviar un informe de error o una sugerencia](#).

Soporte técnico. Si necesita ayuda con Kaspersky Anti-Virus, haga clic en el vínculo ubicado en la entrada **Servicio de soporte local**. Se abrirá el sitio de Kaspersky Lab con información para ponerse en contacto con nuestros especialistas.



Figura 47. Información de soporte técnico

11.7. Configuración de la interfaz de Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers le ofrece la posibilidad de modificar la apariencia del programa con la creación y utilización de combinaciones de color. También puede configurar el uso de los elementos activos de la interfaz como el icono de la barra del sistema o los mensajes emergentes.

Para configurar la interfaz del programa, aplique los pasos siguientes:

1. Abra la ventana de configuración de Kaspersky Anti-Virus for Windows Servers desde el vínculo [Configuración](#) de la ventana principal.
2. Seleccione **Apariencia** en la entrada **Servicio** de la ventana de configuración del programa (ver Figura 48).

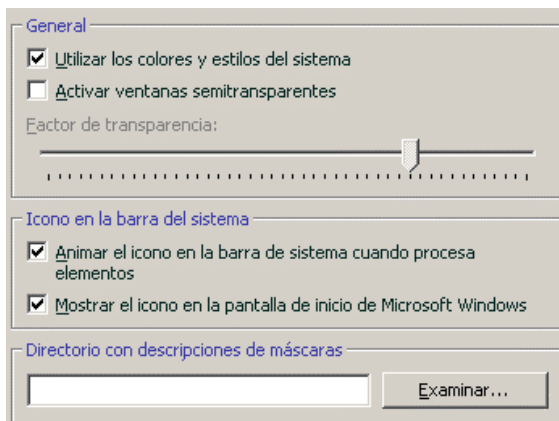


Figura 48. Configuración de la apariencia del programa

En la parte derecha de la ventana de configuración, puede configurar:

- Si debe aparecer el indicador de protección de Kaspersky Anti-Virus for Windows Servers al arrancar el sistema operativo.

Este indicador aparece de forma predeterminada en el ángulo superior derecho de la pantalla cuando se carga el programa. Le informa de que su equipo está protegido contra cualquier tipo de amenaza. Si no desea utilizar el indicador de protección, desactive la casilla **Mostrar el icono en la pantalla de inicio de sesión de Microsoft Windows**.

- Si desea utilizar animaciones en el icono de la barra del sistema.

En función de la operación realizada por el programa, el icono de la barra del sistema se modifica. De forma predeterminada, se utiliza la animación del icono. Si desea desactivar la animación, desactive la casilla **Animar el icono en la barra de sistema cuando procesa elementos**. A continuación, el icono sólo indicará el estado de protección de su equipo: si la protección está activa, el icono es de color y si la protección está suspendida o detenida, el icono se vuelve gris.

- Grado de transparencia de los mensajes emergentes.

Todas las operaciones de Kaspersky Anti-Virus for Windows Servers que necesitan su atención inmediata o requieren una decisión suya son presentados como mensajes emergentes por encima del icono de la barra del sistema. Las ventanas de los mensajes se transparentan para no interferir con otras operaciones. Si desplaza el apuntador sobre el mensaje, la transparencia desaparece. Puede modificar el grado de transparencia de estos mensajes. Para ello, ajuste el **Factor de**

transparencia al nivel deseado. Para eliminar la transparencia de los mensajes, desactive la casilla **Activar ventanas semitransparentes**.

- Utilice sus propias máscaras para la interfaz del programa.

Todos los colores, fuentes, iconos y textos utilizados en la interfaz de Kaspersky Anti-Virus for Windows Servers pueden modificarse. Puede crear sus propios gráficos para el programa o traducirlo a otros idiomas. Para utilizar una máscara de presentación, especifique el directorio con sus parámetros en el campo **Directorio con descripciones de máscaras**. Utilice el botón **Examinar** para seleccionar el directorio.

De forma predeterminada, la máscara del programa utiliza los colores y estilos del sistema. Para eliminarlos puede desactivar la casilla **Utilizar los colores y estilos del sistema**. A continuación, se aplicarán los estilos especificados en la configuración del tema de pantalla.

Observe que los parámetros personalizados de la interfaz de Kaspersky Anti-Virus no se conservan cuando restablece los parámetros predeterminados o desinstala el programa.

11.8. Trabajar con opciones avanzadas

Kaspersky Anti-Virus for Windows Servers le ofrece las características avanzadas siguientes:

- Notificaciones de ciertos eventos que se producen en el programa.
- Autoprotección de Kaspersky Anti-Virus for Windows Servers contra la desactivación, eliminación o modificación de módulos, así como la protección por contraseña del programa
- Solución de conflictos entre Kaspersky Anti-Virus y otros programas.

Para configurar estas características:

1. Abra la ventana de configuración del programa con el vínculo Configuración de la ventana principal.
2. Seleccione **Servicio** en el árbol de configuración.

En la parte superior derecha de la ventana, puede decidir utilizar funciones avanzadas del programa.

11.8.1. Notificaciones de eventos de Kaspersky Anti-Virus for Windows Servers

Durante el funcionamiento de Kaspersky Anti-Virus for Windows Servers, pueden producirse diferentes tipos de eventos. Pueden tener un contenido informativo o al contrario, información importante. Por ejemplo, un evento puede informarle del éxito de una actualización terminada o registrar un error en un componente determinado, que debe ser eliminado inmediatamente.

Para recibir actualizaciones sobre el funcionamiento de Kaspersky Anti-Virus for Windows Servers, utilice la característica de notificación.

Las notificaciones pueden entregarse por los medios siguientes:

- Mensajes emergentes por encima del icono del programa en la barra del sistema
- Sonidos
- Mensajes
- Registrar evento

Para poder usar esta característica, debe:

1. Active **Activar las notificaciones** en la sección **Interacción con el usuario** (ver Figura 49).

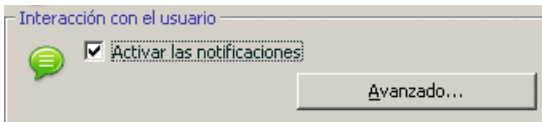


Figura 49. Activación de las notificaciones

2. Defina los tipos de eventos de Kaspersky Anti-Virus for Windows Servers sobre los que desea recibir notificaciones y el modo de recibirlas (ver 11.8.1.1 pág. 142).
3. Configure los parámetros de envío de notificaciones por correo, si éste es el método de notificación utilizado (ver 11.8.1.2 en la página 143).

11.8.1.1. Tipos de eventos y modos de entrega de las notificaciones

Durante el funcionamiento de Kaspersky Anti-Virus for Windows Servers, pueden producirse los siguientes tipos de eventos:

Eventos críticos: eventos de importancia grave. La notificaciones son muy recomendables, porque apuntan a problemas de funcionamiento del programa o vulnerabilidades en la protección del equipo. Por ejemplo, *firmas de amenazas dañadas o licencia caducada*.

Fallo de funcionamiento: eventos que indican que el programa no está funcionando. Por ejemplo, falta la licencia o las bases de aplicación.

Notificaciones importantes: eventos a los que debe prestar atención, porque reflejan situaciones importantes en el funcionamiento de la aplicación. Por ejemplo, *protección desactivada o Hace mucho que no analiza el equipo completo*.

Notificaciones no importantes: sirven como referencia y en general no contienen información importante. Por ejemplo, *todos los objetos peligrosos neutralizados*.

Para especificar de qué eventos el programa debe informarle y cómo:

1. Haga clic en el vínculo Configuración de la ventana principal del programa.
2. En la ventana de configuración del componente, seleccione **Servicio**, y active la casilla **Activar las notificaciones** y, para modificar en detalle los parámetros, haga clic en **Avanzado**.

Puede configurar los métodos de notificación siguientes para los eventos anteriores, en la ventana **Configuración de notificaciones** abierta (ver Figura 50):

- *Mensajes emergentes* que aparecen por encima del icono del programa en la barra del sistema, con información acerca del evento ocurrido.

Para utilizar este tipo de notificaciones, active la casilla en la sección **Globo** asociada al evento sobre el que desea recibir notificaciones.

- *Notificación con sonido*

Si desea acompañar la notificación con un archivo sonoro active la casilla **Sonido** asociada al evento.

- *Notificación por correo*

Para utilizar este tipo de notificaciones, active la columna **Correo** asociada al evento sobre el que desea recibir notificaciones y configure los parámetros de envío de notificaciones (ver 11.8.1.2 pág. 143).

- *Registrar evento*

Para registrar en el informe información acerca de cualquier evento ocurrido, active la casilla correspondiente en la columna **Informe** y configure el informe de eventos (ver 11.8.1.3 pág. 145).

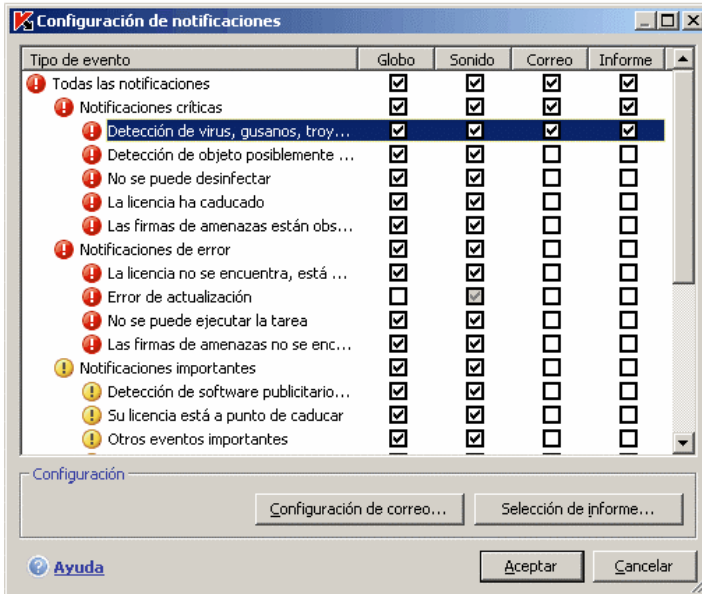


Figura 50. Eventos del programa y modos de entrega de las notificaciones

11.8.1.2. Configuración de notificaciones por correo

Después de seleccionar los eventos (ver 11.8.1.1 pág. 142) sobre los que desea recibir información por correo, debe configurar las notificaciones. Para ello:

1. Abra la ventana de configuración del programa con el vínculo Configuración de la ventana principal.
2. Seleccione la entrada **Servicio** en el árbol de configuración.
3. Haga clic en **Avanzado** en la sección **Interacción con el usuario** de la parte derecha de la pantalla.

4. En la ficha **Configuración de notificaciones** active la casilla en la columna **Correo** para los eventos que deben desencadenar el envío de un mensaje de correo.
5. En la ventana abierta cuando hace clic en **Configuración de correo**, configure el envío de notificaciones por correo siguientes:
 - Configure el envío de notificaciones en la sección **Para: Dirección de correo**.

Configuración de notificaciones

De

Dirección de correo: admin@myhost.com

Servidor SMTP: mail.server.com Puerto: 25

Nombre de cuenta: administrator

Contraseña: •••••

Para

Dirección de correo: test@myhost.com

Modo de envío

Inmediatamente al producirse el evento

Cada 1 día(s) Cambiar...

[Ayuda](#) Aceptar Cancelar

Figura 51. Configuración de notificaciones por correo

- Especifique la dirección de destino de las notificaciones en **Para: Dirección de correo**.
- Defina un modo de notificación en **Modo de envío**. Para que el programa envíe un mensaje tan pronto como se produzca el evento, seleccione **Inmediatamente al producirse el evento**. Para notificar eventos dentro de un cierto plazo de tiempo y definir la planificación del envío de correos informativos, haga clic en **Cambiar**. La notificaciones se envían diariamente de forma predeterminada.

11.8.1.3. Configuración de los parámetros del registro de eventos

Para configurar el informe de eventos:

1. Abra la ventana de configuración del programa con el vínculo Configuración en la ventana principal.
2. Seleccione la entrada **Servicio** en el árbol de configuración.
3. Haga clic en **Avanzado** en la sección **Interacción con el usuario** de la parte derecha de la pantalla.

En la ventana **Configuración de notificaciones** active la opción para registrar información acerca de un evento y haga clic en **Configuración de informes**.

Kaspersky Anti-Virus permite registrar información acerca de los eventos que se producen cuando el programa está en ejecución, tanto en el informe de eventos general de MS Windows (**Aplicación**) como en un registro de eventos dedicado de Kaspersky Anti-Virus (**Informe de eventos de Kaspersky**).

Los informes pueden examinarse con el **Visor de sucesos**, de Microsoft Windows, que puede abrir desde **Inicio** → **Configuración** → **Panel de Control** → **Administración** → **Mostrar eventos**.

11.8.2. Autoprotección y restricción de acceso

Kaspersky Anti-Virus for Windows Servers se responsabiliza de la seguridad de su equipo contra programas nocivos y, por ello, puede convertirse a su vez en objetivo de programas malintencionados que intentan bloquear el programa o incluso eliminarlo del equipo.

Por otro lado, muchas personas pueden utilizar el mismo equipo, todas con diferentes niveles de experiencia informática. Si deja libre el acceso al programa y a su configuración, puede disminuir considerablemente la seguridad del equipo en su conjunto.

Para garantizar la estabilidad del sistema de seguridad de su equipo, se han incluido mecanismos de autoprotección, de protección contra accesos remotos y de protección con contraseña.

Activar la autoprotección

1. Abra la ventana de configuración del programa con el vínculo Configuración en la ventana principal.

2. Seleccione **Servicio** en el árbol de configuración.

Aplique la configuración siguiente en la sección **Autoprotección** (ver Figura 52):

- Activar la autoprotección.** Al activar esta casilla, se activan los mecanismos de autoprotección del programa contra la eliminación o modificación de los archivos en disco, procesos en memoria y entradas en el Registro del sistema del propio programa.
- Desactivar el control externo de servicios.** Si activa esta casilla, cualquier programa de administración remota que intente utilizar el programa quedará bloqueado.

Ante un intento de cualquiera de las acciones anteriores, se mostrará un mensaje por encima del icono del programa en la barra del sistema (a menos que el usuario desactive las notificaciones).

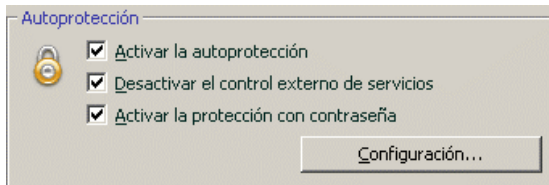


Figura 52. Configuración de la autoprotección

Para proteger el programa con una contraseña, active la casilla **Activar la protección con contraseña.** Haga clic en **Configuración** para abrir la ventana **Protección con contraseña** y escriba la contraseña y la cobertura de acceso restringido (ver Figura 53).

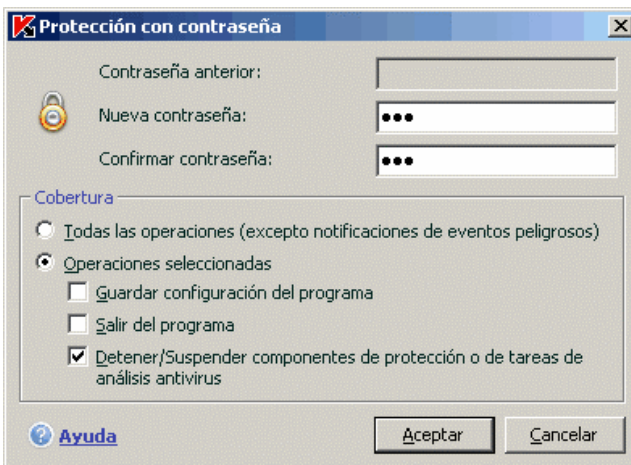


Figura 53. Configuración de la protección con contraseña

Puede bloquear cualquier operación del programa excepto las notificaciones de detección de objetos peligrosos o impedir la ejecución de cualquiera de las acciones siguientes:

- Modificar los parámetros de rendimiento del programa
- Cerrar Kaspersky Anti-Virus for Windows Servers
- Desactivar o suspender la protección de su equipo

Cada una de estas acciones reduce el nivel de protección del equipo, por lo que debe determinar qué usuarios podrán trabajar con el servidor.

Ahora, siempre que un usuario intente realizar las acciones seleccionadas, el programa preguntará por una contraseña.

11.8.3. Solución de conflictos con otras aplicaciones

En ciertos casos, Kaspersky Anti-Virus puede provocar conflictos con otras aplicaciones instaladas en un equipo. Esto se debe a que estos programas disponen de mecanismos de autoprotección que se activan cuando Kaspersky Anti-Virus intenta inspeccionarlos. Entre estas aplicaciones está el complemento Authentica para Acrobat Reader, que comprueba los accesos a los archivos .PDF; el producto Oxygen Phone Manager II, y algunos juegos de ordenador que utilizan herramientas de administración de derechos digitales.

Para corregir este problema, active la casilla **Compatibilidad con los métodos de autoprotección** de otros programas en la entrada **Servicio** de la ventana de configuración de la aplicación. Debe reiniciar el sistema operativo para que los cambios tengan efecto.

11.9. Importación y exportación de la configuración de Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers le permite importar y exportar sus parámetros.

Los parámetros se guardan en un archivo de configuración especial.

Para exportar la configuración actual del programa:

1. Abra la ventana principal de Kaspersky Anti-Virus for Windows Servers.

2. Seleccione la entrada **Servicio** y haga clic en Configuración.
3. Haga clic en **Guardar** en la sección **Administrador de configuraciones**.
4. Indique un nombre para el archivo de configuración y seleccione su ubicación de destino.

Para importar parámetros desde un archivo de configuración:

1. Abra la ventana principal de Kaspersky Anti-Virus for Windows Servers.
2. Seleccione la entrada **Servicio** y haga clic en Configuración.
3. Haga clic en **Cargar** y seleccione el archivo desde el que desea importar la configuración de Kaspersky Anti-Virus for Windows Servers.

11.10. Restablecimiento de la configuración predeterminada

Siempre es posible restablecer los parámetros predeterminados del programa, que se consideran óptimos y son los recomendados por los expertos de Kaspersky Lab. Para ello, puede utilizar el Asistente de instalación.

Para restablecer los parámetros de protección:

1. Seleccione la entrada **Servicio** y haga clic en Configuración para abrir la ventana de configuración del programa.
2. Haga clic en **Restablecer** en la sección **Administrador de configuraciones**.

La ventana que se abre le permite definir qué parámetros es necesario restablecer a sus valores predeterminados.

De forma predeterminada, el programa guarda todos los parámetros personalizados de la lista (las casillas no están activadas). Si no necesita guardar alguno de los parámetros, active la casilla correspondiente.

Después de configurar los parámetros, haga clic en **Siguiente** (ver 3.2 pág. 27). Se abre el Asistente de configuración. Siga sus instrucciones.

Después de terminar el Asistente de instalación, el nivel de seguridad **Recomendado** quedará definido para el componente Antivirus de archivos, con la excepción de los valores que decidió conservar. Además, los parámetros configurados desde el Asistente de configuración también se aplicarán.

CAPÍTULO 12.

ADMINISTRACIÓN DEL PROGRAMA CON KASPERSKY ADMINISTRATION KIT

Kaspersky Administración Kit es un sistema centralizado de administración de tareas clave dentro del sistema de seguridad de la red corporativa, que se apoya en las aplicaciones incluidas en los productos Kaspersky Anti-Virus Business Optimal y Kaspersky Corporate Suite.

Kaspersky Anti-Virus 6.0 for Windows Servers es uno de los productos de Kaspersky Lab que pueden administrarse desde una interfaz propia, desde la línea de comandos (estos métodos se describen más arriba en este documento) o desde Kaspersky Administración Kit (si el equipo forma parte del sistema centralizado de administración a distancia).

Siga los pasos siguientes para administrar Kaspersky Anti-Virus 6.0 for Windows Servers con Kaspersky Administración Kit:

- Despliegue el *Servidor de administración* en su red local; instale la *consola de administración* en el puesto de trabajo administrador (para más detalles, vea la Guía del administrador de Kaspersky Administration Kit 6.0);
- En los servidores de archivos, despliegue Kaspersky Anti-Virus 6.0 for Windows Servers y *NAgent* (incluido con Kaspersky Administración Kit) en los equipos de la red. Para obtener más información acerca de la instalación remota de la consola de administración, consulte la Guía del administrador acerca de la implementación de Kaspersky Administration Kit 6.0.

Después de actualizar el complemento de administración de Kaspersky Lab desde Kaspersky Administración Kit, cierre la consola de administración.

Consola de administración (ver Figura 54) permite administrar la aplicación con Kaspersky Administration Kit. Ofrece una **interfaz MMC** (Microsoft Management Console) integrada en estándar y permite al administrador ejecutar las funciones siguientes:

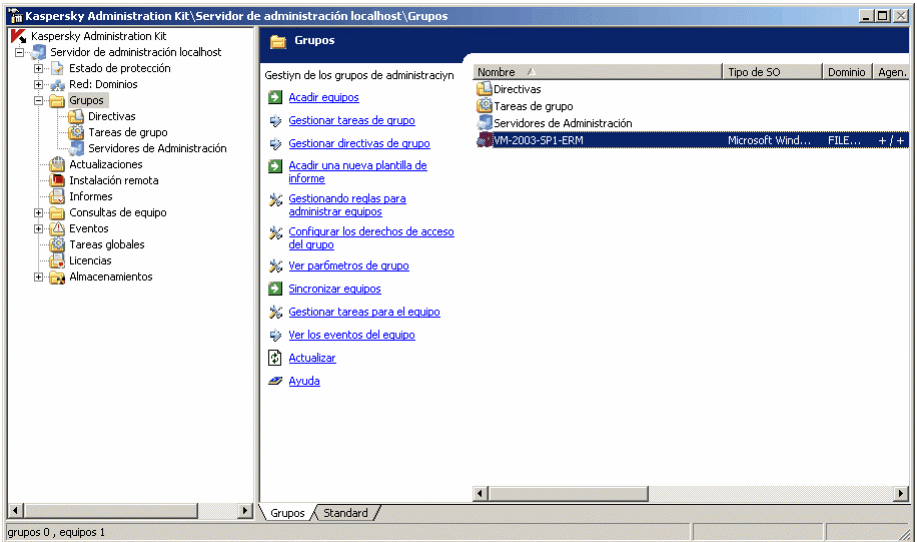


Figura 54. Consola de administración de Kaspersky Administration Kit

- Instalar en remoto Kaspersky Anti-Virus 6.0 for Windows Servers y el programa *NAgent* en los equipos de la red
- Configurar en remoto Kaspersky Anti-Virus en los equipos de la red
- Actualizar las bases de aplicación y los módulos de aplicación de Kaspersky Anti-Virus.
- Administrar las licencias de la aplicación en los equipos de la red
- muestra información acerca del funcionamiento del programa en equipos remotos

Quando administra de forma centralizada el programa con Kaspersky Administration Kit, el administrador configura las directivas, las tareas y la propia aplicación.

La **configuración de la aplicación** abarca un conjunto de parámetros generales para el funcionamiento del programa, inclusive los parámetros de protección generales, la configuración de la cuarentena y del respaldo, la generación de informes, etc.

Una **tarea** es una acción específica ejecutada por la aplicación. Las tareas para Kaspersky Anti-Virus for Windows Servers se dividen por su tipo (tareas de análisis a petición, actualización de la base antivirus y los módulos de aplicación, anulación de la actualización, instalación de llaves de licencia,). Cada tarea

específica cuenta con un conjunto de parámetros de ejecución de Kaspersky Anti-Virus utilizados para su ejecución (*parámetros de tarea*).

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

Una **Directiva** es un conjunto de parámetros de funcionamiento del programa para grupos de equipos en la red, que cuenta con restricciones a nivel de grupo contra la reconfiguración de la aplicación o de tareas en un equipo cliente individual.

Una directiva incluye todos los parámetros necesarios para ejecutar cada una de las características implementadas en la aplicación. Las directivas incluyen parámetros para el programa y todos los tipos de tareas, salvo tareas de cierto tipo.

12.1. Administración de la aplicación

Kaspersky Administration Kit le permite iniciar y suspender en remoto Kaspersky Anti-Virus en equipos clientes individuales, así como configurar parámetros generales de aplicación, como la activación o desactivación de la protección del equipo, los parámetros de Respaldo y Cuarentena y los parámetros de creación de informes.

Para administrar los parámetros de la aplicación:

1. Seleccione la carpeta de grupo que contiene la carpeta **Grupos** (ver Figura 54).
2. En el panel de resultados, seleccione el equipo del que desea modificar los parámetros de aplicación. En el menú contextual o en el menú **Acciones**, seleccione **Propiedades**.
3. La ficha **Aplicaciones** en la ventana de propiedades del equipo cliente (ver Figura 55) muestra la lista completa de las aplicaciones Kaspersky Lab instaladas en el equipo cliente.

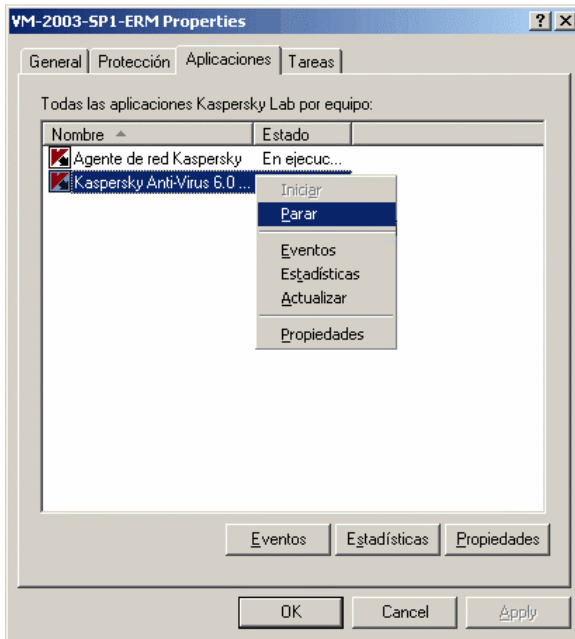


Figura 55. Lista de aplicaciones de Kaspersky Lab

Dispone de botones bajo la lista de programas que puede utilizar para:

- Mostrar una lista de eventos de aplicación ocurridos en el servidor y registrados en el servidor de administración.
- Ver las estadísticas actuales de funcionamiento del programa
- Configurar los parámetros del programa (ver 12.1.2 pág. 153)

12.1.1. Iniciando/deteniendo la aplicación

Puede ejecutar o suspender Kaspersky Anti-Virus en un equipo remoto con los comandos del menú contextual en la ventana de propiedades del equipo (ver Figura 55).

Puede ejecutar las mismas acciones con los botones **Ejecutar/Detener** de la ventana de configuración de la ficha **General** (ver Figura 56).

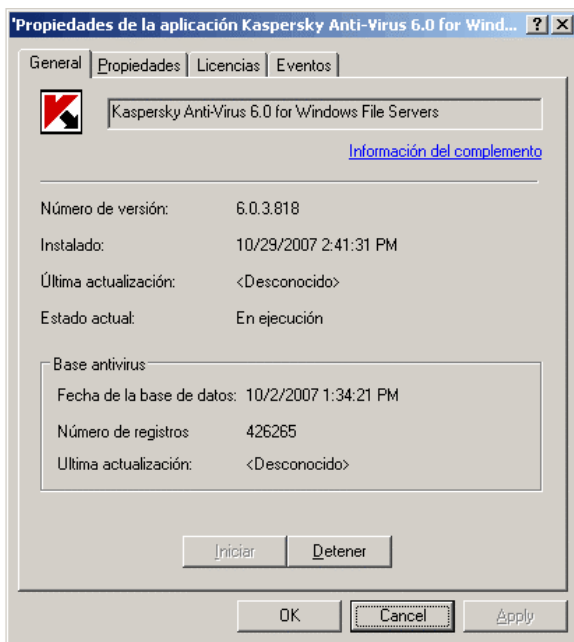


Figura 56. Configuración de Kaspersky Anti-Virus.
Ficha General

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

12.1.2. Configuración de los parámetros de la aplicación

Para mostrar o modificar los parámetros de aplicación:

1. Abra la ventana de propiedades del equipo cliente en la ficha **Aplicaciones** (ver Figura 54).
2. Seleccione **Kaspersky Anti-Virus 6.0 for Windows Servers**. Haga clic en **Propiedades** para abrir la ventana de configuración.

Todas las fichas, con excepción de la ficha **Propiedades** son fichas estándar de Kaspersky Administración Kit 6.0. Para más información acerca de la fichas estándar, consulte la Guía del administrador.

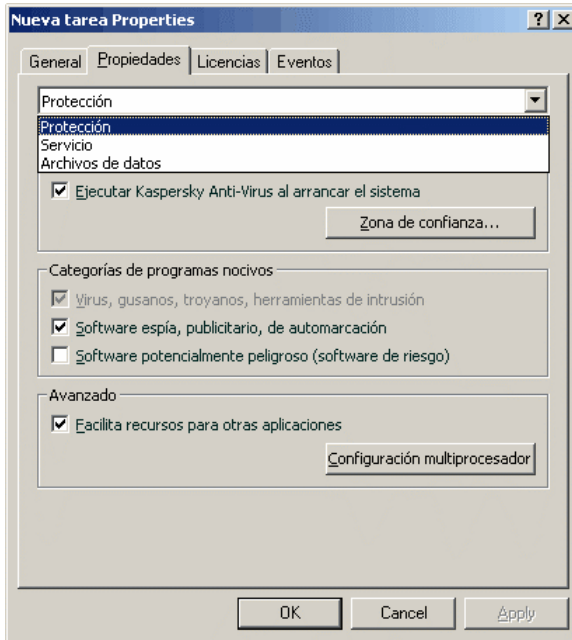


Figura 57. Configuración de Kaspersky Anti-Virus.
Ficha **Propiedades**

Si se crea una directiva para la aplicación (ver 12.3.1 pág. 163) que evita la reconfiguración de ciertos parámetros, éstos no podrán modificarse durante la configuración de la aplicación.

En la ficha **Configuración**, puede definir los parámetros generales y de funcionamiento de la protección, la cuarentena y respaldo y la generación de informes. Para ello, seleccione el valor necesario en la lista desplegable de la parte superior de la ventana y defina los parámetros:

Protección

En esta ventana, puede:

- Activar o desactivar la protección de un equipo (ver 6.1 pág. 52)
- Configurar la ejecución automática de la aplicación al encender el equipo (ver 6.1.5 pág. 56)
- Crear un zona de confianza o una lista de exclusiones (ver 6.3 pág. 57)

- Seleccionar los tipos de programas malintencionados supervisados por la aplicación (ver 6.2 pág. 56)
- Configurar los parámetros de rendimiento de la aplicación y del multi-procesador (ver 6.7 pág. 69)

Servicio

La configuración de los servicios incluye:

- Configurar las notificaciones de los eventos que se producen (ver 11.8.1 pág. 141)
- Administrar las características de autoprotección y los parámetros de protección por contraseña de la aplicación (ver 11.8.2 pág. 145)
- Configurar la apariencia de la aplicación (ver 12.3.1 pág. 163)
- Configurar la compatibilidad entre Kaspersky Anti-Virus y otros programas (ver 11.8.3 pág. 147)

Archivos de datos

Esta ventana permite configurar la generación de informes estadísticos acerca del funcionamiento de la aplicación (ver 11.3.1 pág. 128) y especificar cuánto tiempo deben conservarse los archivos en las zonas de Respaldo (ver 11.2.2 pág. 123) y Cuarentena (ver 11.1.2 pág. 120).

12.1.3. Parámetros específicos

Cuando administra Kaspersky Anti-Virus desde Kaspersky Administration Kit, puede activar o desactivar la interactividad y modificar la información de Soporte técnico. Para ello:

1. Abra la ventana de propiedades del equipo cliente en la ficha **Aplicaciones** (ver Figura 55).
2. Seleccione **Kaspersky Anti-Virus 6.0 for Windows Servers** y haga clic en **Propiedades**. Se abre una ventana de configuración de la aplicación (ver Figura 57). Seleccione **Servicio** desde el menú desplegable de la parte superior de la ventana.

En la ventana **Servicio**, puede activar o desactivar la interfaz interactiva de Kaspersky Anti-Virus en un equipo remoto: mostrar el icono de Kaspersky Anti-Virus en la barra del sistema, abrir notificaciones con los eventos que se producen en la aplicación (por ejemplo, la detección de un objeto peligroso).

Si la casilla **Activar la interactividad** está activada, el usuario de un equipo remoto verá el icono del antivirus y los mensajes emergentes y podrá tomar decisiones sobre las acciones presentadas en las ventanas de notificación acerca de los eventos que se produzcan. Para desactivar la interactividad de la aplicación, desactive la casilla.

En la ficha **información de soporte personal** de la ventana **Configuración**, puede modificar la información de soporte técnico al usuario, presente bajo la entrada **Servicio**, cuadro **Soporte** en Kaspersky Anti-Virus (ver Figura 47).

Para modificar la información del campo superior, indique el nuevo texto acerca del soporte ofrecido. En el campo inferior, modifique los vínculos mostrados en el cuadro **Soporte técnico en línea** mostrado cuando selecciona **Soporte** en la entrada **Servicio**.

Puede modificar la lista con los botones **Agregar**, **Modificar** y **Eliminar**. Kaspersky Anti-Virus agrega un nuevo vínculo al principio de la lista. Para modificar el orden de los vínculos en la lista, utilice **Subir** y **Bajar**.

Si la ventana no contiene ningún dato, no se puede modificar la información predeterminada del soporte técnico.

12.2. Administración de tareas

Esta sección incluye información para administrar tareas de Kaspersky Anti-Virus 6.0 for Windows Servers. Para obtener más información acerca de la administración de tareas desde Kaspersky Administración Kit 6.0, consulte el Manual del administrador del programa.

Durante la instalación de la aplicación, se crea un conjunto de tareas de sistema para cada equipo. Esta lista (ver Figura 58) incluye tareas de protección en tiempo real (Antivirus de archivos), tareas de análisis antivirus (Mi PC, Objetos de inicio, Zonas críticas) y tareas de actualización (actualizaciones de firmas de amenazas y módulos de aplicación, anulación de actualización y distribución de actualizaciones).

Puede ejecutar tareas de sistema, configurarlas y planificarlas, pero no puede eliminarlas.

Adicionalmente, puede crear sus propias tareas de análisis antivirus, de actualización o de anulación de actualización, así como tareas de instalación de llave de licencia.

Para ver la lista completa de tareas creadas para el equipo cliente:

1. Seleccione la carpeta de grupo que contiene la carpeta **Grupos** (ver Figura 54).
2. En el panel de resultados, seleccione el equipo para el que desea crear una tarea local y utilice el comando **Tareas** desde el menú contextual o el menú **Acción**. A continuación, se abrirá una ventana con las propiedades del equipo cliente.
3. La ficha **Tareas** (ver Figura 58) muestra una lista completa de tareas creadas para el equipo cliente.

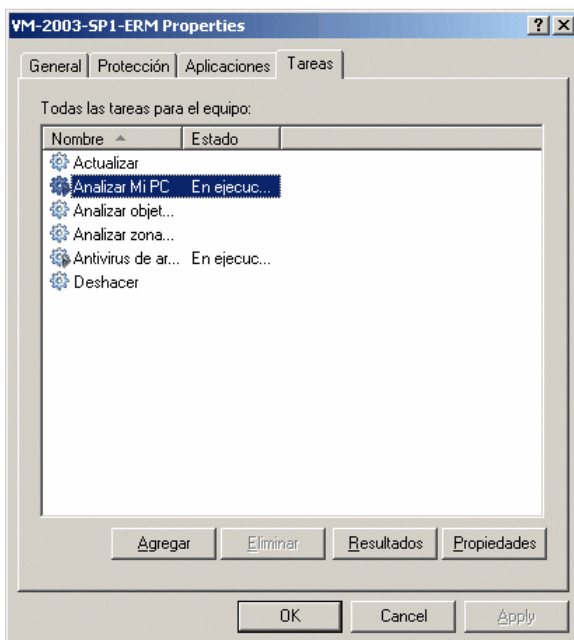


Figura 58. Lista de tareas de aplicación.

12.2.1. Inicio y detención de tareas

Las tareas se ejecutan en el equipo cliente sólo si la aplicación correspondiente está en ejecución (ver 12.1.1 pág. 152). Si la aplicación se detiene, todas las tareas iniciadas terminarán también.

Es posible iniciar y detener las tareas de forma automática, de acuerdo con la planificación, o manual, con las opciones del menú contextual o desde la

ventana de configuración de la tarea. También puede suspender y reanudar tareas.

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

Seleccione la tarea necesaria (de grupo o global) en el panel de resultados, abra el menú contextual, y elija **Ejecutar/Detener/Suspender/Continuar** o utilice el mismo comando del menú **Acción**.

Puede realizar las mismas operaciones para todos los tipos de tareas desde la ventana de configuración de tarea, en la ficha **General** (ver Figura 59) con los botones correspondientes.

12.2.2. Creación de tareas

Cuando trabaja con la aplicación desde Kaspersky Administration Kit, puede crear:

- Tareas locales, configuradas para equipos locales
- Tareas de grupo, configuradas para equipos para formar un grupo de red
- Tareas globales, configuradas para cualquier selección de equipos, en cualquier grupo de red

Puede modificar los parámetros de tarea, supervisar su ejecución, copiar y desplazar tareas de un grupo a otro e incluso eliminarlos con los comandos estándar **Copiar/Pegar**, **Cortar/Pegar** y **Modificar** en el menú contextual o en el menú **Acción**.

12.2.2.1. Creación de tareas locales

Para crear una tarea local, siga los pasos siguientes:

1. Abra la ventana de propiedades del equipo cliente en la ficha **Tareas** (ver Figura 58).
2. Para agregar una nueva tarea, haga clic en **Agregar**. Se abre la ventana Crear una nueva tarea, diseñada como un Asistente estándar de Windows: consta de una serie de etapas entre las cuales puede desplazarse con los botones **Anterior** y **Siguiente**, a las que pone fin con el botón **Terminar**. El botón **Cancelar** interrumpe el Asistente en cualquier punto.

Paso 1. Datos generales sobre la tarea

La primera ventana es introductoria: se especifica aquí el nombre de la tarea (campo **Nombre**).

Paso 2. Selección de una aplicación y del tipo de tarea

En esta etapa, debe especificar para qué aplicación va a crear la regla (Kaspersky Anti-Virus 6.0 for Windows Servers). También debe activar el tipo de tarea. Las posibles tareas para Kaspersky Anti-Virus 6.0 son:

- *Análisis antivirus*: busca virus en las zonas especificadas por el usuario
- *Update*: recupera y aplica paquetes de actualización para el programa
- *Anular la actualización*: anula la última actualización del programa
- *Instalar una llave de licencia*: agrega una nueva llave de licencia de uso de la aplicación

Paso 3. Configuración del tipo de tarea seleccionado

El contenido de la siguiente ventana del asistente depende del tipo de tarea seleccionada en la etapa anterior.

VIRUS SCAN

En la ventana de configuración de tareas de análisis antivirus, debe definir una lista de objetos para analizar (ver 8.2 pág. 86) y especificar la acción tomada por Kaspersky Anti-Virus cuando detecta un objeto peligroso (ver 8.4.4 pág. 94).

UPDATE

En el caso de las tareas de actualización de las firmas de amenazas y de los módulos de aplicación, especifique el origen utilizado para descargar las actualizaciones (ver 10.4.1 pág. 108). El origen de actualizaciones predeterminado es el servidor de actualizaciones de Kaspersky Administración Kit.

UPDATE ROLLBACK

La tarea de anulación de las actualizaciones más recientes no tiene parámetros específicos.

INSTALL LICENSE KEY

Para tareas de instalación de llaves de licencia, especifique la ruta del archivo llave con **Examinar**. Para convertir una llave en llave de reserva, active la casilla **Agregar como llave de reserva**. La llave de reserva se convertirá en llave activa cuando caduque la actual.

La información de la llave agregada (número de licencia, tipo y fecha de caducidad) se muestra en el campo inferior.

Paso 4. Ejecución de una tarea con una cuenta de usuario diferente

En esta etapa, debe configurar la ejecución de tareas con cuenta de usuario que disponga de permisos suficientes para tener acceso al objeto analizado o al origen de actualizaciones (ver 6.4 pág. 64).

Paso 5. Configuración de la planificación

Después de configurar la tarea, podrá programar la planificación automática de tareas.

Para ello, seleccione la frecuencia de ejecución de la tarea en el menú desplegable y ajuste los parámetros de planificación en la parte inferior de la ventana.

Paso 6. Finalizar la creación de una tarea

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

12.2.2.2. Creación de tareas de grupo

Para crear una tarea de grupo, siga los pasos siguientes:

1. Seleccione el grupo para el que desea crear una tarea desde el árbol de consola.
2. Seleccione la entrada **Tareas de grupo**, abra el menú contextual y seleccione **Crear**→**Tarea**, o utilice el mismo comando del menú **Acción**. El asistente de creación de tarea se inicia, parecido al utilizado para la creación de tareas locales (para más información, ver 12.2.2.1 pág. 158). Siga sus instrucciones.

Cuando termina el Asistente, la tarea se agrega a la entrada **Tareas de grupo** del grupo y de todos los subgrupos, y se muestra en el panel de resultados.

12.2.2.3. Creación de tareas globales

Para crear una tarea global, siga los pasos siguientes:

1. Seleccione la entrada **Tareas globales** en el árbol de consola, abra el menú contextual y seleccione **Crear→Tarea**, o utilice el mismo comando del menú **Acción**.
2. El asistente de creación de tarea se inicia, parecido al utilizado para la creación de tareas locales (para más información, ver 12.2.2.1 pág. 158). La excepción es que aquí se incluye una etapa para crear una lista de equipos clientes de la red, para los cuales se crea la tarea.
3. Seleccione los equipos de la red que ejecutarán la tarea. Puede seleccionar equipos en varias carpetas o seleccionar una carpeta completa (para obtener más detalles, consulte el Manual del administrador de Kaspersky Administration Kit 6.0).

Las tareas globales se aplican tan sólo a un conjunto específico de equipos. Si se agregan nuevos equipos clientes a un grupo, una tarea de instalación remota ya creada para los equipos existentes no se ejecutará en los nuevos equipos. Debe crear una nueva tarea o introducir los cambios necesarios en la configuración de la tarea existente.

Cuando termina el Asistente, la tarea global se agrega a la entrada **Tareas globales** del árbol de consola y se muestra dentro del panel de resultados.

12.2.3. Configuración de tarea

Para ver y modificar los parámetros de la tarea en los equipos clientes,

1. Abra la ventana de propiedades del equipo cliente en la ficha **Tareas** (ver Figura 58).
2. Seleccione la tarea en la lista y haga clic en **Propiedades**. Se abre una ventana de configuración de la tarea (ver Figura 60).

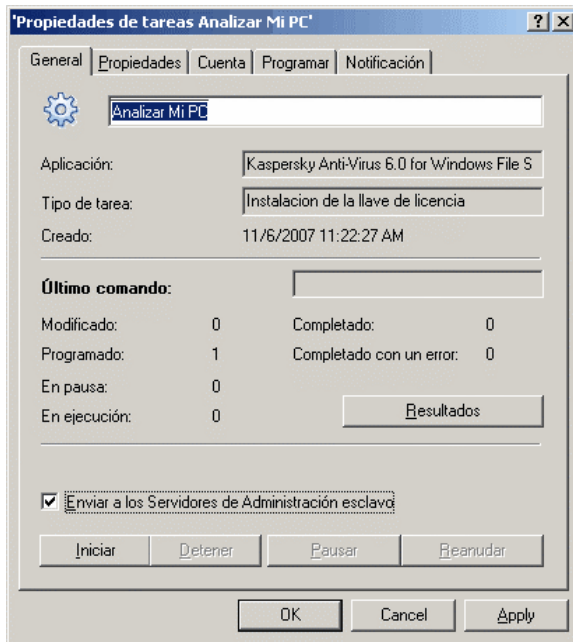


Figura 59. Configuración de tarea

Todas las fichas, con excepción de la ficha **Configuración** son fichas estándar de Kaspersky Administración Kit 6.0 6.0. Están descritas con mayor profundidad en el Manual de administrador. La ficha **Configuración** contiene parámetros específicos de Kaspersky Anti-Virus. El contenido de esta ficha depende del tipo de tarea seleccionada.

La interfaz de configuración de tareas de Kaspersky Administración Kit es similar a la interfaz local de Kaspersky Anti-Virus, salvo para los parámetros específicos de la tarea. Vea Capítulo 7 – Capítulo 10 en las páginas 70 – 104 de esta guía del usuario para una descripción más detallada de la configuración de tareas.

Si se crea una directiva para la aplicación (ver 12.3 pág. 162) que evita la reconfiguración de ciertos parámetros, éstos no podrán modificarse durante la configuración de la aplicación.

12.3. Control de directivas

La configuración de directivas permite aplicar de forma universal parámetros de aplicación y de tareas en equipos clientes que pertenecen al mismo grupo de red.


Esta sección incluye información acerca de la creación y configuración de directivas para Kaspersky Anti-Virus 6.0 for Windows Servers. Para obtener más información acerca de la administración de directivas desde Kaspersky Administración Kit 6.0, consulte el Manual del administrador del programa.

12.3.1. Creación de directivas

Para crear una directiva para Kaspersky Anti-Virus, siga los pasos siguientes:

1. En la carpeta **Grupos** (ver Figura 54), seleccione el grupo cuya directiva desea crear.
2. Seleccione la entrada **Directivas** que pertenece al grupo seleccionado, abra el menú contextual y utilice **Crear**→**Directiva**. Se abrirá una ventana de creación de nueva directiva.

Se abre la ventana Crear una nueva directiva, diseñada como un Asistente estándar de Windows: consta de una serie de etapas entre las cuales puede desplazarse con los botones **Anterior** y **Siguiente**, a las que pone fin con el botón **Terminar**. El botón **Cancelar** interrumpe el Asistente en cualquier punto.

En cada etapa de la creación de una directiva, los parámetros introducidos pueden bloquearse con el botón . Si el cerrojo está cerrado, en adelante los valores establecidos por la directiva serán los utilizados cuando la aplique en equipos remotos.

Paso 1. Datos generales sobre la directiva

El primer paso del Asistente es introductorio: Debe especificar el nombre de la directiva (campo **Nombre**), seleccionar **Kaspersky Anti-Virus 6.0 for Windows Servers** en el menú desplegable **Nombre de la aplicación**. Si desea que los parámetros de directiva se apliquen inmediatamente después de crearla, active la casilla **La directiva está activa**.

Paso 2. Selección de un estado de directiva

Esta ventana le pregunta si desea especificar el estado de directiva. Para ello, mueva el cursor a la posición adecuada: directiva activa o inactiva.

Puede crear varias directivas en el grupo de una aplicación, pero sólo una de ellas puede estar activa a un tiempo.

Paso 3. Selección y configuración de los componentes de protección

Esta etapa le permite activar o desactivar la protección y el componente Antivirus de archivos del equipo. De forma predeterminada, la protección está activada y el componente Antivirus de archivos está en ejecución.

Para ajustar los parámetros de protección o el componente Antivirus de archivos, selecciónelo en la lista y haga clic en **Configuración**.

Paso 4. Configuración de tareas de análisis antivirus

Esta etapa le permite configurar los parámetros utilizados por las tareas de análisis antivirus.

En el cuadro **Nivel de seguridad**, seleccione uno de los tres niveles de protección preinstalados (ver 7.1 en la pág. 71). Haga clic en **Configuración** para ajustar el nivel seleccionado. Para restablecer el nivel **Recomendado**, haga clic en **Predeterminado**.

En la sección **Acción**, especifique la acción tomada por el antivirus cuando detecta un objeto peligroso (ver 8.4.4 pág. 94).

Paso 5. Configuración de la actualización

Esta ventana permite configurar la característica de distribución de actualizaciones de Kaspersky Anti-Virus.

En la sección **Configuración de actualizaciones**, especifique qué módulos de programa deben actualizarse (ver 10.4.2 pág. 108). En la ventana abierta cuando hace clic en **Configuración**, defina los parámetros de red local (ver 10.4.3 pág. 113) y especifique el origen de actualizaciones (ver 10.4.1 pág. 108).

En la sección **Acción después de actualizar**, active o desactive el análisis de la cuarentena tras recibir un nuevo paquete de actualización (ver 10.4.4 pág. 115).

Paso 6. Control de directiva

En este paso, seleccione el método de distribución de la directiva a los clientes del grupo (para más detalles, consulte el Manual del administrador de Kaspersky Administration Kit 6.0).



Paso 7. Determinación del método de primera aplicación de la directiva

En este paso, seleccione el método de primera aplicación de la directiva para los equipos clientes del grupo, en la ventana **Cumplir directiva** (para más detalles, consulte el Manual del administrador de Kaspersky Administration Kit 6.0).

Paso 8. Finalizar la creación de una 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 Kaspersky Anti-Virus se muestra en el panel de resultados y se agrega a la carpeta de **Directivas** del grupo correspondiente.

Puede modificar los parámetros de la directiva y definir restricciones para la modificación de su configuración con el  botón  para cada parámetro del grupo. El usuario de un equipo cliente no podrá modificar los parámetros bloqueados de este modo. La directiva se aplicará a los equipos clientes la primera vez que éstos se sincronicen con el servidor.

Puede copiar o desplazar directivas de un grupo a otro o eliminarlas, con los comandos **Copiar/Pegar**, **Cortar/Pegar** o **Eliminar** en el menú contextual o en el menú Acción.

12.3.2. Examen y modificación de la configuración de la directiva

Durante la etapa de modificación, puede modificar y prohibir la modificación de los parámetros en grupos anidados, en la aplicación y en las tareas.

Para ver y modificar los parámetros de la directiva:

1. Seleccione el grupo de equipos cuya configuración quiere modificar, en el árbol de consola, en la carpeta **Grupos**.

2. Seleccione la entrada **Directivas** que pertenece al grupo seleccionado. Al hacerlo, el panel de resultados mostrará todas la directivas creadas para el grupo.
3. Seleccione la directiva que necesita en la lista de directivas para **Kaspersky Anti-Virus 6.0 for Windows Servers** (el nombre de la aplicación se especifica en el campo **Aplicación**).
4. Abra el menú contextual de la directiva seleccionada y haga clic en **Propiedades**. En pantalla se muestra la ventana de configuración de directivas para Kaspersky Anti-Virus 6.0 (ver Figura 60).

Todas las fichas, con excepción de la ficha **Configuración** son fichas estándar de Kaspersky Administration Kit 6.0. Están descritas con mayor profundidad en el Manual de administrador.

La ficha **Configuración** presenta la configuración de directivas para Kaspersky Anti-Virus 6.0. Los parámetros de directiva incluyen la configuración del programa (ver 12.1.2 en la página 153) y la configuración de tareas (ver 12.2 en la página 156).

Para configurar los parámetros, seleccione el valor necesario en la lista desplegable de la parte superior de la ventana y defina los parámetros.

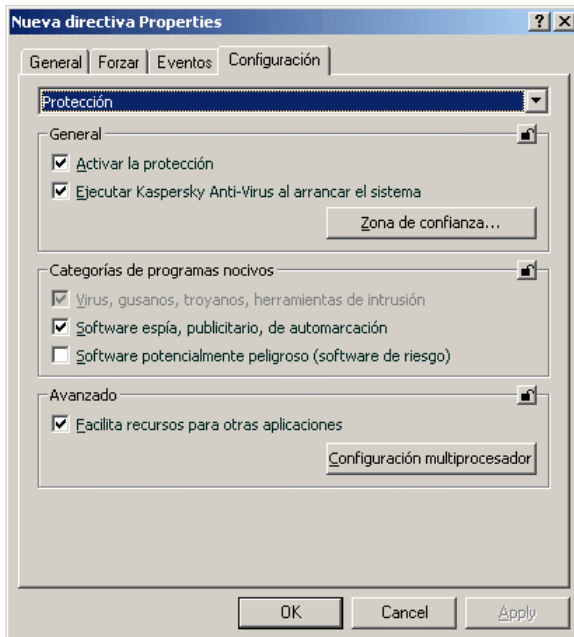


Figura 60. Configuración de la directiva

CAPÍTULO 13. OPERACIONES DESDE LA LÍNEA DE COMANDOS

Puede utilizar Kaspersky Anti-Virus for Windows Servers desde la línea de comandos. Son posibles las operaciones siguientes:

- Iniciar, detener, suspender y reanudas la actividad componente Antivirus de archivos
- Iniciar, detener, suspender y reanudar los análisis antivirus
- Obtención de información acerca del estado actual del componente Antivirus de archivos, las tareas y las estadísticas
- Análisis de los objetos seleccionados
- Actualice las bases de aplicación y los módulos de programa
- Obtener Ayuda sobre la sintaxis de la línea de comandos
- Obtener Ayuda sobre la sintaxis de comandos

La sintaxis de la línea de comandos es:

```
avp.com <comando> [parámetros]
```

Debe utilizar la línea de comandos desde la carpeta de instalación del programa, o especificando la ruta completa del archivo avp.com.

Los siguientes pueden utilizarse como **<comandos>**:

ADDKEY	Activa el programa con un archivo llave de licencia (el comando sólo puede ejecutarse entrando la contraseña establecida desde la interfaz del programa)
ACTIVATE	Activa la aplicación en línea mediante un código de activación
START	Inicia el Antivirus de archivos o una tarea
PAUSE	Suspende el Antivirus de archivos o una tarea (el comando sólo puede ejecutarse entrando la contraseña)

	establecida desde la interfaz del programa)
RESUME	Reanuda el Antivirus de archivos o una tarea
STOP	Detiene el Antivirus de archivos o una tarea (el comando sólo puede ejecutarse entrando la contraseña establecida desde la interfaz del programa)
STATUS	Muestra el estado actual del Antivirus de archivos o de la tarea en pantalla
STATISTICS	Muestra las estadísticas del Antivirus de archivos o de la tarea en pantalla
HELP	Ayuda sobre la sintaxis y lista de comandos
SCAN	Analiza objetos en busca de virus
UPDATE	Inicia la actualización del programa
ROLLBACK	Anula la última actualización del programa realizada (el comando sólo puede ejecutarse entrando la contraseña establecida desde la interfaz del programa)
EXIT	Cierra el programa (sólo puede ejecutar este comando con una contraseña definida desde la interfaz del programa)
IMPORT	Importa la configuración de Kaspersky Anti-Virus for Windows Servers (el comando sólo puede ejecutarse entrando la contraseña establecida desde la interfaz del programa)
EXPORT	Exportar la configuración de Kaspersky Anti-Virus for Windows Servers

Cada comando dispone de su propio conjunto de parámetros, específicos para esta instalación de Kaspersky Anti-Virus for Windows Servers.

13.1. Activación de la aplicación

Existen dos métodos de activar la aplicación:

- por Internet mediante un código de activación (comando ACTIVATE)
- mediante un archivo llave de licencia (comando ADDKEY)

Sintaxis del comando:

```
ACTIVATE <código_activación>
ADDKEY <nombre_archivo> /password=<su_contraseña>
```

Parámetros:

<nombre_archivo>	Nombre del archivo llave con la extensión .key.
<código_activación>	Código de activación de la aplicación suministrado con la compra.
<su_contraseña>	Contraseña de Kaspersky Anti-Virus definida en la interfaz del programa.
Nota: no puede ejecutar este comando sin la contraseña.	

Ejemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<su_contraseña>
```

13.2. Administración del Antivirus de archivos y las tareas

Sintaxis del comando:

```
avp.com <comando> <perfil|nombre_tarea>
[/R[A]:<archivo_informe>]
avp.com STOP|PAUSE <perfil|nombre_tarea>
/password=<contraseña> [/R[A]:<archivo_informe>]
```

Parámetros:

<comando>	Kaspersky Anti-Virus permite administrar tareas y componentes desde la línea de comandos, con
------------------------	---

	<p>los parámetros siguientes:</p> <p>START: inicia un componente de protección en tiempo real o una tarea.</p> <p>STOP: detiene un componente de protección en tiempo real o una tarea.</p> <p>PAUSE: suspende un componente de protección en tiempo real o una tarea.</p> <p>RESUME: reanuda un componente de protección en tiempo real o una tarea.</p> <p>STATUS: muestra el estado de un componente de protección en tiempo real o tarea.</p> <p>STATISTICS: muestra las estadísticas de actividad de un componente de protección en tiempo real o tarea.</p> <p>Observe que los parámetros PAUSE y STOP están protegidos con contraseña.</p>
<perfil nombre_tarea>	<p>El parámetro <perfil> puede tomar el valor de cualquier componente de seguridad o módulo en tiempo real de la aplicación, tarea de análisis a petición o de actualización (los valores predeterminados utilizados por la aplicación se muestran a continuación).</p> <p>Los valores aceptados del parámetro <nombre_tarea> pueden incluir el nombre de cualquier tarea a petición o de actualización personalizada.</p>
<su_contraseña>	<p>Contraseña de Kaspersky Anti-Virus definida en la interfaz del programa.</p>
/R[A]:<archivo_informe>	<p>R:<archivo_informe>: registra sólo los eventos importantes</p> <p>/RA:<archivo_informe>: registra todos los eventos en el informe.</p> <p>Puede utilizar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, los resultados del análisis se muestran en pantalla, con todos los eventos.</p>

Uno de los valores siguientes se atribuye a `<perfil>`:

PTR	<p>Todos los componentes</p> <p>El comando <code>avp.com START RTP</code> inicia el componente Antivirus de archivos si fue detenido con <code> </code> en la interfaz de usuario o con el comando <code>PAUSE</code> desde la línea de comandos.</p> <p>Si el componente fue desactivado con <code>■</code> en la interfaz de usuario o con el comando <code>STOP</code> desde la línea de comandos, debe ejecutar el comando <code>avp.com START FM</code> para poder iniciarlo.</p>
FM	Antivirus de archivos
UPDATER	Actualizador
RetranslationCfg	Copiar actualizaciones a un origen local
Rollback	Anula la última actualización del programa
SCAN_OBJECTS	Tarea de análisis antivirus
SCAN_MY_COMPUTER	Tarea Analizar Mi PC
SCAN_CRITICAL_AREAS	Tarea de análisis de zonas críticas
SCAN_STARTUP	Tarea de análisis de objetos de inicio
SCAN_QUARANTINE	Tarea de análisis de objetos en cuarentena
<p>Los componentes y tareas invocados desde la línea de comandos se ejecutan con los parámetros definidos desde la interfaz del programa.</p>	

Ejemplos:

Para activar el componente Antivirus de archivos, escriba la línea de comandos siguiente:

```
avp.com START FM
```

Para detener la tarea Analizar Mi PC desde la línea de comandos, escriba:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<su_contraseña>
```

13.3. Análisis antivirus

La sintaxis para ejecutar el análisis antivirus y la neutralización de objetos malintencionados en una cierta zona, desde la línea de comandos, suele presentarse como sigue:

```
avp.com SCAN [<objeto analizado>] [<acción>] [<tipos
de archivos>] [<exclusiones>] [<archivo de
configuración>] [<parámetros de informe>]
[<parámetros avanzados>]
```

Para analizar objetos, también puede ejecutar alguna de las tareas creadas en Kaspersky Anti-Virus for Windows Servers desde la línea de comandos (ver 13.2 pág. 169). La tarea se ejecutará con los parámetros especificados en la interfaz del programa.

Descripción de los parámetros:

<objeto analizado>: este parámetro indica la lista de objetos que se van a analizar en busca de código malintencionado.

Puede incluir una lista de varios valores separados por espacios, de la lista siguiente.

<archivos>	<p>Lista de rutas a los archivos o carpetas que se van a analizar.</p> <p>Puede indicar rutas absolutas o relativas. Los elementos de la lista están separados por espacios.</p> <p>Notas:</p> <p>Si el nombre del objeto contiene un espacio, debe escribirse entre comillas</p> <p>Si especifica una carpeta en concreto, se analizan todos los archivos contenidos en ella.</p>
/MEMORY	Objetos en la memoria del sistema
/STARTUP	Objetos de inicio

/MAIL	Bases de correo
/REMDRIVES	Todas las unidades de medios extraíbles
/FIXDRIVES	Todas las unidades internas
/NETDRIVES	Todas las unidades de red
/QUARANTINE	Objetos en cuarentena
/ALL	Análisis completo
/@:<listaarchivos.lst>	Ruta del archivo con una lista de objetos y carpetas incluidos en el análisis. El archivo debe estar en formato texto y cada objeto analizado en una línea. Puede indicar la ruta absoluta o relativa al archivo. La ruta debe escribirse entre comillas si contiene algún espacio.
<acción> : este parámetro determina las acciones realizadas sobre los objetos malintencionados detectados durante el análisis. Si este parámetro no está definido, la acción predeterminada es /i8 .	
/i0	no toma ninguna acción sobre el objeto; sólo registra información en el informe.
/i1	Neutralizar los objetos infectados, ignorar si la desinfección no es posible
/i2	Neutraliza los objetos infectados y si falla la desinfección, los elimina. Excepciones: no elimina los objetos infectados de objetos compuestos; elimina objetos compuestos con encabezados ejecutables, como archivos sfx comprimidos (predeterminado).
/i3	Neutraliza los objetos infectados y si falla la desinfección, los elimina. Elimina también todos los objetos compuestos si los contenidos infectados no pueden eliminarse.

/i4	Neutraliza los objetos infectados y si falla la desinfección, los elimina. Elimina también todos los objetos compuestos si los contenidos infectados no pueden eliminarse.
/i8	Preguntar al usuario en caso de detectarse un objeto infectado
/i9	Preguntar al usuario al finalizar el análisis
<tipos de archivos> : este parámetro define los tipos de archivos sometidos a análisis antivirus. Si este parámetro no está definido, la acción predeterminada es /fi.	
/fe	Analizar sólo archivos posiblemente infectados por extensión
/fi	Analizar sólo archivos posiblemente infectados por contenido (predeterminado)
/fa	Analizar todos los archivos
<exclusiones> : este parámetro define qué objetos son excluidos del análisis. Puede incluir una lista de varios valores separados por espacios.	
-e:a	No analizar archivos comprimidos
-e:b	No analizar bases de correo
-e: m	No analizar los mensajes en formato texto sencillo
-e:<máscara archivos>	de No analizar los objetos incluidos en la máscara
-e:<segundos>	Ignorar objetos cuyo análisis se prolonga más tiempo del especificado en el parámetro <segundos>
-es:<tamaño>	Ignora los archivos mayores (en Mb) que el tamaño especificado por <tamaño> .

<p><archivo de configuración>: define la ruta del archivo de configuración con los parámetros del programa para el análisis.</p> <p>El archivo de configuración se guarda en formato binario (.dat), a menos que especifique otro formato o no especifique ninguno, y puede utilizarse más tarde para importar parámetros de aplicación en otros equipos.</p> <p>Puede indicar la ruta absoluta o relativa al archivo. Si este parámetro no está definido, utiliza los valores definidos en la interfaz de Kaspersky Anti-Virus for Windows Servers.</p>	
<code>/C:<nombre_archivo></code>	Utiliza los parámetros definidos en el archivo <code><nombre_archivo></code>
<p><parámetros de informe>: este parámetro determina el formato del informe con los resultados del análisis.</p> <p>Puede utilizar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, los resultados del análisis se muestran en pantalla, con todos los eventos.</p>	
<code>/R:<archivo_informe></code>	Registrar sólo los eventos importantes en el archivo
<code>/RA:<archivo_informe></code>	Registrar todos los eventos en el archivo
<p><parámetros avanzados>: parámetros que definen el uso de las tecnologías de análisis antivirus.</p>	
<code>/iChecker=<on off></code>	Activa o desactiva iChecker.
<code>/iSwift=<on off></code>	Activa o desactiva iSwift.

Ejemplos:

*Ejecutar un análisis de la RAM, los programas de inicio, las bases de correo, los directorios **Mis documentos** y **Archivos de programa**, así como del archivo **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Mis Documentos" "C:\Archivos de programa" "C:\Downloads\test.exe"
```

Suspender el análisis de los objetos seleccionados e iniciar un análisis completo de equipo y, al finalizar, reanudar la búsqueda antivirus en los objetos seleccionados:

```
avp.com PAUSE SCAN_OBJECTS /password=<su_contraseña>
```

```
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Analizar la RAM y la lista de objetos en el archivo **object2scan.txt**. Utilizar el archivo de configuración **scan_setting.txt**. Después del análisis, generar un informe con todos los eventos registrados:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Ejemplo de archivo de configuración:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

13.4. Actualizaciones del programa

La sintaxis para la actualización de módulos de programa y firmas base de amenazas de Kaspersky Anti-Virus for Windows Servers desde la línea de comandos es la siguiente:

```
avp.com UPDATE [<origen_actualización>]
[/R[A]:<archivo_informe>] [/C:<nombre_archivo>]
[/APP=<on|off>]
```

Descripción del parámetro:

<origen_actualización>	Servidor HTTP o FTP o carpeta de red para descargar las actualizaciones. Puede especificar la ruta completa al origen de actualizaciones o una dirección URL como valor de este parámetro. Si no selecciona una ruta, el origen de actualizaciones se toma de los parámetros de actualización.
/R[A]:<archivo_informe>	<p>/R:<archivo_informe>: registra sólo los eventos importantes del informe.</p> <p>/R[A]:<archivo_informe>: registra todos los eventos en el informe.</p> <p>Puede utilizar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, los resultados del análisis se muestran en pantalla, con todos los eventos.</p>

<code>/C:<nombre_archivo></code>	<p>Ruta del archivo de configuración con los parámetros para las actualizaciones del programa.</p> <p>El archivo de configuración es un archivo de texto con un grupo de parámetros de línea de comandos para la actualización del programa.</p> <p>Puede indicar la ruta absoluta o relativa al archivo. Si este parámetro no está definido, utiliza los valores definidos en la interfaz de Kaspersky Anti-Virus for Windows Servers.</p>
<code>/APP=<on off></code>	Activa o desactiva las actualizaciones de los módulos de aplicación

Ejemplos:

Actualizar las bases de aplicación después de registrar todos los eventos en el informe:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Actualizar los módulos de programa de Kaspersky Anti-Virus for Windows Servers con los parámetros del archivo de configuración **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Ejemplo de archivo de configuración:

```
"ftp://mi_servidor/kav updates" /RA:avbases_upd.txt
/app=on
```

13.5. Parámetros para deshacer la actualización

Sintaxis del comando:

```
ROLLBACK
[/R[A]:<archivo_informe>][/password=<su_contraseña>]
```

/R[A]:<archivo_informe>	<p>/R:<archivo_informe>: registrar sólo los eventos importantes del informe.</p> <p>/R[A]:<archivo_informe>: registrar todos los eventos en el informe.</p> <p>Puede utilizar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, los resultados del análisis se muestran en pantalla, con todos los eventos.</p>
<su_contraseña>	Contraseña de acceso a Kaspersky Anti-Virus definida en la interfaz del programa.
<p>Nota: no puede ejecutar este comando sin introducir la contraseña.</p>	

Ejemplos:

```
avp.com ROLLBACK /RA:deshacer.txt
[/password=<contraseña>]
```

13.6. Exportación de la configuración

Sintaxis del comando:

```
avp.com EXPORT <perfil> <nombre_archivo>
```

Descripción del parámetro:

<perfil>	<p>Antivirus de archivos o tarea con los parámetros para exportar.</p> <p>Puede utilizar cualquier valor para el parámetro <perfil> en la lista 13.2 pág. 169.</p>
-----------------------	---

<nombre_archivo>	<p>Ruta del archivo donde se va a exportar la configuración de Kaspersky Anti-Virus for Windows Servers. Puede utilizar una ruta absoluta o relativa.</p> <p>El archivo de configuración se guarda en formato binario (.dat), a menos que especifique otro formato o no especifique ninguno, y puede utilizarse más tarde para importar parámetros de aplicación en otros equipos. Puede exportar el archivo de configuración a un archivo de texto. Para ello, especifique la extensión .txt extensión en el nombre de archivo. Nota: los parámetros de protección no pueden ser importados desde un archivo de texto. Este archivo sólo puede utilizarse para especificar los parámetros principales de funcionamiento del programa.</p>
------------------	--

Ejemplos:

```
avp.com EXPORT c:\settings.dat
```

13.7. Importación de la configuración

Sintaxis del comando:

```
avp.com IMPORT <archivo> [/password=<su_contraseña>]
```

<nombre_archivo>	<p>Ruta del archivo desde el cual se va a importar la configuración de Kaspersky Anti-Virus for Windows Servers. Puede utilizar una ruta absoluta o relativa.</p> <p>Los parámetros sólo pueden leerse de archivos binarios.</p> <p>Si instala el programa en modo desatendido desde la línea de comandos o con el Editor de objetos de directiva de grupo, el nombre del archivo de configuración debe ser <i>install.cfg</i>. En otro caso, el programa no lo reconoce.</p>
<su_contraseña>	Contraseña de Kaspersky Anti-Virus definida en la interfaz del programa.

Nota: no puede ejecutar este comando sin la contraseña.

Ejemplos:

```
avp.com IMPORT c:\settings.dat /password=<su_contraseña>
```

13.8. Ejecución del programa

Sintaxis del comando:

```
avp.com
```

13.9. Detención del programa

Sintaxis del comando:

```
EXIT /password=<contraseña>
```

<contraseña>	Contraseña de Kaspersky Anti-Virus definida en la interfaz del programa.
---------------------------	--

Nota: no puede ejecutar este comando sin la contraseña.

Nota: no puede ejecutar este comando sin introducir la contraseña.

13.10. Obtención de un archivo de depuración

Un archivo de depuración puede ser necesario, ante problemas en tiempo de ejecución, para que los especialistas del Soporte técnico puedan localizar el origen del problema.

Sintaxis del comando:

```
avp.com TRACE [file] [on|off] [<nivel_depuración>]
```

[on off]	Activa o desactiva la generación del archivo de depuración.
[file]	Genera y guarda en un archivo de depuración.

<nivel_depuración>	<p>Este parámetro puede tomar valores numéricos en el intervalo de 0 (nivel menor, sólo eventos críticos) a 700 (nivel mayor, todos los eventos).</p> <p>Al ponerse en contacto con el Soporte técnico, un especialista debe especificar el nivel de depuración necesario. Si no lo especifica, le recomendamos utilizar el nivel 500.</p>
<p>¡Cuidado! La generación de un archivo de depuración sólo debe activarse para la resolución de un problema específico. Si la función de depuración permanece siempre activa, esto puede disminuir el rendimiento del equipo y terminar saturando el disco duro.</p>	

Ejemplos:

Desactivar la depuración:

```
avp.com TRACE file off
```

Generar un archivo de depuración para el Soporte técnico con el nivel 500 máximo:

```
avp.com TRACE file on 500
```

13.11. Visualización de la Ayuda

Para ver la ayuda sobre la sintaxis de la línea de comandos, dispone del siguiente comando:

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

Para obtener ayuda sobre la sintaxis de un comando específico, puede utilizar uno de los comandos siguientes:

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

13.12. Códigos de retorno de la interfaz de la línea de comandos

Esta sección contiene una lista de códigos de retorno para la línea de comandos. Los códigos generales pueden ser devueltos por cualquier comando

escrito en la línea de comandos. Los códigos de retorno incluyen códigos generales y códigos específicos de un cierto tipo de tareas.

Códigos de retorno generales	
0	Operación terminada con éxito
1	Valor del parámetro no válido
2	Error desconocido
3	La tarea terminó con un error
4	Tarea cancelada
Códigos de retorno de la tarea de análisis antivirus	
101	Todos los objetos peligrosos procesados
102	Objetos peligrosos detectados

CAPÍTULO 14. MODIFICACIÓN, REPARACIÓN Y DESINSTALACIÓN DEL PROGRAMA

Puede desinstalar la aplicación con los métodos siguientes:

- Con el Asistente de instalación (ver 14.2 pág. 186);
- Desde la línea de comandos (ver 14.2 pág. 186);
- Utilización de Kaspersky Administración Kit (ver la Guía de implementación de Kaspersky Administration Kit);
- Utilización de directivas de dominios y grupos Microsoft Windows Server 2000/2003 (ver 3.4.3 pág. 35).

14.1. Modificación, reparación y desinstalación del programa con el Asistente de instalación

Puede resultar necesario reparar el programa si detecta errores en su funcionamiento después de una configuración incorrecta o de producirse daños en archivos.

Para reparar o modificar componentes ausentes de Kaspersky Anti-Virus for Windows Servers o para desinstalar el programa:

1. Inserte el CD de instalación en la unidad de CD-ROM, si la utilizó para instalar el programa. Si instaló Kaspersky Anti-Virus for Windows Servers desde otro origen (carpeta pública, carpeta del disco, etc.), asegúrese de que el paquete de instalación está presente en esta carpeta y que tiene permisos de lectura.
2. Seleccione **Inicio → Programas → Kaspersky Anti-Virus 6.0 for Windows Servers → Modificar, Reparar o Eliminar**.

Un Asistente de instalación abrirá entonces el programa. Presentamos a continuación los pasos del proceso de reparación, modificación o desinstalación.

Paso 1. Pantalla de bienvenida del instalador

Si siguió todos los pasos descritos antes, para reparar o modificar el programa, la ventana bienvenida del programa de instalación de Kaspersky Anti-Virus for Windows Servers aparece. Para continuar, haga clic en **Siguiente**.

Paso 2. Selección de una operación

En este paso, debe seleccionar la operación que desea ejecutar. Puede modificar los componentes del programa, reparar los componentes ya instalados o bien desinstalar algunos componentes o el programa completo. Para ejecutar la operación deseada, haga clic en el botón apropiado. La respuesta del programa dependerá de la operación seleccionada.

La modificación del programa es similar a una instalación personalizada (ver Paso 7 en la pág. 25), en la que especifica qué componentes desea instalar o desinstalar.

La reparación del programa depende de los componentes de programa instalados. Los archivos de todos los componentes instalados serán reparados y se aplicará el nivel de seguridad Recomendado para todos ellos.

Advertencia:

Si Kaspersky Anti-Virus 6.0 se desinstala de forma remota, el servidor no se reiniciará automáticamente. Sin embargo, para eliminar completamente los componentes de la aplicación y para que el equipo pueda funcionar adecuadamente en el futuro, recomendamos reiniciarlo manualmente.

Si elimina el programa, puede seleccionar qué datos creados y utilizados por el programa desea guardar en su equipo. Para eliminar todos los datos de Kaspersky Anti-Virus for Windows Servers, seleccione **Desinstalación completa**. Para guardar los datos, seleccione **Guardar objetos de la aplicación** y especifique en la lista qué objetos no desea eliminar:

- *Datos de activación*: información acerca de la activación del programa.
- *Firmas de amenazas*: conjunto completo de firmas de programas peligrosos, virus y otras amenazas incluidas en la última actualización.
- *Archivos de respaldo*: copias de respaldo de objetos desinfectados o eliminados. Se recomienda guardarlos, por si necesita restaurarlos más tarde.

- *Archivos de cuarentena*: archivos posiblemente infectados por algún virus o su mutación. Estos archivos contienen código similar al de un virus conocido pero sin que se pueda determinar si es dañino. Le recomendamos guardarlos ya que pueden no estar realmente infectados o podrán ser desinfectados después de una actualización de las bases de aplicación.
- *Configuración de la aplicación*: configuraciones del componente Antivirus de archivos.
- *Datos iSwift*: base con información acerca de los objetos analizados en sistemas de archivos NTFS, que permite incrementar la velocidad del análisis. Cuando utiliza esta base, Kaspersky Anti-Virus for Windows Servers analiza sólo los archivos nuevos y los que han sido modificados desde el último análisis.

Advertencia:

Si transcurre un largo periodo de tiempo entre la desinstalación de una versión y la reinstalación de otra versión de Kaspersky Anti-Virus for Windows Servers, no le recomendamos utilizar la base *iSwift* de la instalación anterior. Un programa peligroso puede penetrar en el equipo en el intervalo y sus efectos no serían detectados gracias a la base, lo que causaría una infección.

Para ejecutar la operación seleccionada, haga clic en **Siguiente**. El programa comenzará a copiar los archivos necesarios en su equipo o a eliminar los componentes y datos seleccionados.

Paso 3. Fin de la modificación, reparación o desinstalación

El proceso de modificación, reparación o desinstalación se realiza en pantalla y el programa le informa de su finalización.

La desinstalación del programa suele necesitar el reinicio del equipo, para aplicar las modificaciones en el sistema. El programa le pregunta si desea reiniciar su equipo. Haga clic en **Sí** para reiniciar inmediatamente. Para reiniciar su equipo más, haga clic en **No**.

14.2. Desinstalación del programa desde la línea de comandos

Para desinstalar Kaspersky Anti-Virus 6.0 for Windows Servers desde la línea de comandos, escriba:

```
msiexec /x <nombre_paquete>
```

Se abre el Asistente de configuración. Puede utilizarlo para desinstalar la aplicación (ver Capítulo 14 en la pág. 183).

Para desinstalar la aplicación en modo desatendido sin reiniciar el equipo (debe reiniciar manualmente el equipo después de la desinstalación), escriba:

```
msiexec /x <nombre_paquete> /qn
```

Para instalar la aplicación en modo desatendido y a continuación, reiniciar el equipo, escriba:

```
msiexec /x <nombre_paquete> ALLOWREBOOT=1 /qn
```

Cuando instaló el programa, si optó por la protección con contraseña para evitar la desinstalación, deberá introducir la contraseña para poder desinstalar el programa. En caso contrario, no podrá desinstalar el programa.

Para eliminar la aplicación utilizando la contraseña, escriba:


```
msiexec /x <nombre_paquete> KLUNINSTPASSWD=***** -  
para eliminar la aplicación en modo interactivo;
```

```
msiexec /x <nombre_paquete> KLUNINSTPASSWD=***** /qn  
- para eliminar la aplicación en modo desatendido;
```

ANEXO A. INFORMACIÓN DE REFERENCIA

Este anexo contiene material de referencia acerca de los formatos, extensiones y máscaras de archivos utilizados para la configuración de Kaspersky Anti-Virus for Windows Servers.

A.1. Lista de archivos analizados por extensión

Si selecciona  **Analizar programas y documentos (por extensión)**, el componente Antivirus de archivos analizará en profundidad los archivos con las extensiones siguientes en busca de virus.

com: archivo ejecutable de un programa

exe: archivo ejecutable o archivo comprimido autoextraíble

sys: controlador de sistema

prg: programa de texto para dBase, Clipper o Microsoft Visual FoxPro, o programa WAVmaker

bin: archivo binario

bat: archivo por lotes

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo.bat para DOS), OS/2

dpl: biblioteca comprimida de Borland Delphi

dll: biblioteca de vínculos dinámicos

scr: pantalla de presentación en Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto Microsoft OLE (Object Linking and Embedding)

tsp: programa ejecutable en modo de tiempo fraccionado

drv: controlador de dispositivo

vxd: controlador de dispositivo virtual de Microsoft Windows

pif: archivo de información de programa

lnk: archivo de acceso directo de Microsoft Windows

reg: archivo de entradas del Registro de Microsoft Windows

ini: archivo de inicio

cla: clase Java

vbs: secuencia de comandos Visual Basic
vbe: extensión de vídeo del BIOS
js, jse: código fuente JavaScript
htm: documento hipertexto
htt: encabezado de hipertexto de Microsoft Windows
hta: programa hipertexto para Microsoft Internet Explorer
asp: secuencia de comandos Active Server Pages
chm: archivo HTML compilado
pht: archivo HTML con secuencias PHP integradas
php: secuencia de comandos integrada en archivos HTML
wsh: archivo Windows Script Host
wsf: secuencia de comandos de Microsoft Windows
the: papel tapiz del escritorio de Microsoft Windows 95
hlp: archivo de Ayuda de Microsoft Windows
eml: archivo de correo de Microsoft Outlook Express
nws: archivo de noticias de Microsoft Outlook Express
msg: archivo de correo Microsoft Mail
plg: correo
mbx: extensión para mensajes guardados de Microsoft Office Outlook
*doc**: un documento Microsoft Word como: *doc*: un documento Microsoft Word, *docx*: un documento Microsoft Word 2007 con soporte XML, *docm*: un documento Microsoft Word 2007 con soporte para macros.
*dot**: una plantilla de Microsoft Word, como, *dot* – plantilla de Microsoft Word, *dotx*: plantilla de Microsoft Word 2007, *dotm*: plantilla de Microsoft Word 2007 con soporte para macros
fpm: programa de bases de datos, archivo de inicio para Microsoft Visual FoxPro
rtf: documento en formato de texto enriquecido (Rich Text Format)
shs: controlador de objetos recortes del Shell
dwg: base de datos blueprint de AutoCAD
msi: paquete de instalación de Microsoft Windows
otm: proyecto VBA para Microsoft Office Outlook
pdf: documento Adobe Acrobat
swf: archivo Shockwave Flash
jpg, jpeg, png: formato gráfico para imágenes comprimidas
emf: formato de metadatos ampliado para la próxima generación de metadatos de Microsoft Windows. Los archivos EMF no son reconocidos por las versiones de 16 bits de Microsoft Windows

ico: archivo de icono

ov?: Archivos ejecutables Microsoft DOC

*xl**: documentos y archivos Microsoft Office Excel, como: *xla*: extensión Microsoft Office Excel, *xlc*: diagrama, *xlt*: plantillas de documentos. *xlsx*: libro Microsoft Excel 2007, *xltm* : libro Microsoft Excel 2007 con soporte para macros, *xlsb*: formato binario Microsoft Excel 2007 (no XML), *xltx*: plantilla Microsoft Excel 2007, *xlsm*: plantilla Microsoft Excel 2007 con soporte para macros, *xlam*: complemento Microsoft Excel 2007 con soporte para macros.

*pp**: documentos y archivos Microsoft Office Excel, como: *xla*: extensión Microsoft Office Excel, *xlc*: diagrama, *xlt*: plantillas de documentos. *xlsx*: libro Microsoft Excel 2007, *xltm* : libro Microsoft Excel 2007 con soporte para macros, *xlsb*: formato binario Microsoft Excel 2007 (no XML), *xltx*: plantilla Microsoft Excel 2007, *xlsm*: plantilla Microsoft Excel 2007 con soporte para macros, *xlam*: complemento Microsoft Excel 2007 con soporte para macros.

*md**: documentos y archivos Microsoft Office Access, como: *mda*: grupo de trabajo de Microsoft Office Access, *mdb* - base de datos, etc.

sldx: diapositivas Microsoft PowerPoint 2007.

sldm: diapositivas Microsoft PowerPoint 2007 con soporte para macros.

thmx: un tema Microsoft Office 2007.

Recuerde que el formato real de un archivo puede no corresponder al formato indicado por la extensión de archivo.

A.2. Máscaras aceptadas para exclusión de archivos

Estos son algunos ejemplos de máscaras que puede utilizar para crear listas de exclusión de archivos:

- Máscaras sin rutas de archivos:
 - ***.exe**: todos los archivos con extensión `.exe`
 - ***.ex?**: todos los archivos con extensión `.ex?`, dónde ? puede representar cualquier carácter
 - **test**: todos los archivos con nombre `test`
- Máscaras con rutas de archivos absolutas:
 - **C:\dir*.*** ó **C:\dir*** ó **C:\dir**: todos los archivos de la carpeta `C:\dir\`

- **C:\dir*.exe**: todos los archivos con extensión.exe en la carpeta C:\dir\
 - **C:\dir*.ex?**: todos los archivos con extensión.ex? en la carpeta C:\dir\, dónde ? puede representar cualquier carácter
 - **C:\dir\test**: sólo el archivo C:\dir\test
 - Si no desea que el programa analice los archivos en las subcarpetas de esta carpeta, desactive la casilla **Incluir subcarpetas** cuando cree la máscara.
- Máscaras con rutas de archivos relativa:
- **dir*. * ó dir* ó dir**: todos los archivos en todas las carpetas dir\
 - **dir\test**: todos los archivos test en las carpetas de dir\
 - **dir*.exe**: todos los archivos con extensión .exe en todas las carpetas dir\
 - **dir*.ex?**: todos los archivos con extensión.ex? en todas las carpetas C:\dir\, dónde ? puede representar cualquier carácter único

Si no desea que el programa analice los archivos en las subcarpetas de esta carpeta, desactive la casilla **Incluir subcarpetas** cuando cree la máscara.

Sugerencia:

Las máscaras de exclusión *. * y * sólo pueden utilizarse si estableció un tipo de amenaza de exclusión de amenazas de acuerdo con la Enciclopedia del virus. De otro modo, la amenaza especificada no será detectada en ningún objeto. Estas máscaras permiten básicamente desactivar la supervisión sin tener que seleccionar un tipo de amenaza.

Tampoco recomendamos seleccionar como exclusión un disco virtual creado en el sistema de archivos con el comando *SUBST*. No hay razón para hacerlo, porque durante su análisis, el programa reconoce el disco virtual como carpeta y por consiguiente, lo explora.

A.3. Posibles máscaras de exclusión en la clasificación de la Enciclopedia del virus

Para excluir cierta clasificación de amenazas mediante un tipo de amenaza de exclusión de la Enciclopedia de virus, puede especificar:

- el nombre completo de la amenaza tal y como aparece en la Enciclopedia de virus en la dirección www.viruslist.com (por ejemplo, **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**);
- el nombre de la amenaza por su nombre. Por ejemplo:
 - **not-a-virus***: excluye del análisis los programas potencialmente peligrosos así como los programas de broma.
 - ***Riskware.***: excluye el software de riesgo del análisis.
 - ***RemoteAdmin.***: excluye todos los programas de administración remota del análisis.

A.4. Parámetros del archivo *setup.ini*

El archivo *setup.ini*, ubicado en la carpeta de instalación de Kaspersky Anti-Virus, se utiliza para la instalación del programa en modo desatendido desde la línea de comandos (ver 3.3 pág. 32) o con el Editor de objetos de directiva de grupo (ver 3.4 pág. 33). El archivo contiene los parámetros siguientes:

[Setup]: configuración general para la instalación del programa.

InstallDir=<ruta de la carpeta de instalación del programa>.

Reboot=yes|no: reinicio del equipo después de la instalación del programa (no se reinicia de forma predeterminada).

SelfProtection=yes|no: activación de la autoprotección por Kaspersky Anti-Virus durante la instalación (activado de forma predeterminada).

MSExclusions=yes|no: si deben agregarse a la lista de exclusiones de Kaspersky Anti-Virus las recomendaciones de Microsoft para servidores.

AddPath=yes|no: si debe agregarse la ruta de avp.com a la variable de entorno %PATH%.

[Components]: selección de los componentes para instalar. Si no se especifican, se instalarán todos los componentes.

FileMonitor=yes|no: instala el componente Antivirus de archivos

[Tasks]: activa tareas de Kaspersky Anti-Virus. Si no se especifican, todas las tareas se ejecutarán después de la instalación. Si se especifican tareas, se desactivan las tareas no incluidas en la lista.

ScanMyComputer=yes|no: tarea de análisis completo del equipo

ScanStartup=yes|no: tarea de análisis de objetos de inicio

ScanCritical=yes|no: tarea de análisis de zonas críticas

Updater=yes|no: tarea de actualización de las firmas de amenazas y los módulos de programa

En lugar del valor **yes**, puede utilizar los valores **1**, **on**, **enable** ó **enabled**, y en lugar del valor **no**, puede utilizar: **0**, **off**, **disable** ó **disabled**.

ANEXO B. 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 cualquier tipo de programa malintencionado, 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 Alemania, países del Benelux, Francia, Polonia, Reino Unido, Rumanía, Estados Unidos y Canadá, Japón y China. 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 450 especialistas, cada uno de los cuales es un experto en tecnología antivirus, con 10 de ellos en posesión de un M.B.A., otros 16 con un Doctorado, y dos expertos miembros permanentes de la CARO (Computer Anti-Virus Researcher's Organization).

Kaspersky Lab aporta soluciones punteras de seguridad, gracias a su experiencia exclusiva y conocimientos acumulados durante más de 14 años de lucha antivirus. Un análisis avanzado de la actividad vírica permite a esta 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 equipos de una red: estaciones de trabajo, servidores de archivos, sistemas de correo, cortafuegos y pasarelas Internet, así como equipos portátiles. Sus herramientas de administración adaptadas y sencillas 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) y BorderWare (Canadá).

Los clientes de Kaspersky Lab se benefician de una amplia oferta de servicios adicionales que garantizan no sólo un funcionamiento estable de nuestros productos sino también la compatibilidad con cualquier necesidad específica de negocio. La base antivirus de Kaspersky Lab se actualiza cada hora. Nuestra

organización ofrece a sus usuarios un servicio de asistencia técnica de 24 horas, disponible en numerosos idiomas, capaz de adaptarse a su clientela internacional.

B.1. Otros productos Kaspersky Lab

Kaspersky Lab News Agent

El agente de noticias está diseñado para entregar de forma periódica noticias publicadas por Kaspersky Lab, con notificaciones acerca de la actividad vírica actual y noticias recientes. El programa lee las cabeceras y contenidos de noticias disponibles desde el servidor de noticias de Kaspersky Lab con una frecuencia determinada.

El agente de noticias permite a los usuarios:

- Ver el indicador antivirus actualizado en la barra del sistema
- Suscribirse o cancelar su suscripción a las noticias
- Descargar las cabeceras de noticias a intervalo especificado y recibir notificaciones acerca de noticias recientes
- Examinar las noticias de los hilos seleccionados
- Revisar la lista y estado de las cabeceras
- Abrir el artículo completo en su navegador

El agente de noticias es una aplicación Microsoft Windows independiente, que puede usarse por sí sola o integrada en varias soluciones ofrecidas por Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

El programa es un servicio gratuito ofrecido a los visitantes del sitio Web corporativo de Kaspersky Lab. El servicio ofrece en línea un análisis antivirus eficiente de su equipo. Kaspersky OnLine Scanner se ejecuta directamente en su navegador. De este modo, el usuario obtiene rápidamente respuestas a cuestiones relacionadas con la posible infección de su equipo. Con este servicio, los visitantes pueden:

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

Kaspersky® OnLine Scanner Pro

Se trata de un servicio por suscripción ofrecido a los visitantes del sitio Web corporativo de Kaspersky Lab. El servicio ofrece en línea un análisis antivirus

eficiente de su equipo y la neutralización de los archivos peligrosos. Kaspersky OnLine Scanner Pro se ejecuta directamente en su navegador. Con este servicio, los visitantes pueden:

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

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 está diseñado para proteger los equipos personales contra software dañino y es una combinación óptima de métodos convencionales de protección antivirus y de nuevas tecnologías proactivas.

El programa ofrece medios de análisis avanzados que incluyen:

- Análisis antivirus del tráfico de correo a nivel del protocolo de transmisión de datos (POP3, IMAP y NNTP para correo entrante y SMTP para mensajes salientes) sin tener en cuenta el cliente de correo utilizado, así como la desinfección de las bases de correo.
- Análisis antivirus en tiempo real del tráfico Internet que transita por HTTP.
- Análisis antivirus de archivos, directorios o unidades individuales. Además, es posible utilizar una tarea de análisis predeterminada para iniciar el análisis antivirus exclusivamente de zonas críticas y de objetos de inicio del sistema operativo Microsoft Windows.

La protección proactiva ofrece las características siguientes:

Control de cambios dentro del sistema de archivos. El programa permite a los usuarios crear una lista de aplicaciones, para controlarlas de acuerdo con sus componentes. Ayuda a proteger la integridad de la aplicación contra los efectos de software dañino.

Supervisión de procesos en memoria viva (RAM). Kaspersky Anti-Virus 7.0 informa a tiempo a los usuarios cuando detecta procesos peligrosos, sospechosos u ocultos, o cuando ocurren cambios no autorizados en los procesos activos.

Control de cambios en el Registro del sistema gracias al control interno del Registro del sistema.

Control de procesos ocultos, que ayuda a proteger contra el código dañino disimulado en el sistema operativo por técnicas de ocultación (rootkit).

Analizador heurístico. Cuando analiza un programa, el analizador simula su ejecución y registra cualquier actividad sospechosa, como por ejemplo, la apertura o escritura en un archivo, el desvío de vectores de interrupción, etc. De acuerdo con este comportamiento, el programa toma

una decisión acerca de la posible infección del programa por un virus. La simulación se realiza en un entorno virtual aislado que protege el equipo contra cualquier infección.

Restauración del sistema después de ataques por software dañino, al registrar todos los cambios en el Registro o el sistema de archivos y posibilidad de anular estos cambios a petición del usuario.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 es una solución integral de protección de equipos personales contra las principales amenazas a sus datos (virus, intrusos, correo no solicitado y software espía). Una interfaz única permite a los usuarios configurar y administrar todos los componentes del programa.

Las características de protección antivirus incluyen:

Análisis antivirus del tráfico de correo a nivel del protocolo de transmisión de datos (POP3, IMAP y NNTP para correo entrante y SMTP para mensajes salientes) sin tener en cuenta el cliente de correo utilizado. El programa dispone de complementos para los clientes de correo más difundidos (Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail y The Bat!) y es capaz de desinfectar sus bases de correo.

Análisis antivirus en tiempo real del tráfico Internet que transita por HTTP.

Protección del sistema de archivos: análisis antivirus de archivos, directorios o unidades individuales. Además, la aplicación puede realizar un análisis antivirus exclusivamente de zonas críticas y de los objetos de inicio de Microsoft Windows.

Defensa proactiva: el programa supervisa constantemente la actividad de aplicaciones y procesos que se ejecutan en la memoria de acceso aleatorio, impidiendo cualquier cambio peligroso en el sistema de archivos o el Registro, y restaura el sistema después de una afección dañina.

La protección contra fraudes por Internet está garantizada por la capacidad de identificar intentos de fraude (phishing), y por tanto prevenir la pérdida de datos confidenciales (ante todo, contraseñas, cuenta bancaria y números de tarjetas de crédito), así como bloquear la ejecución de secuencias de comandos peligrosas en páginas Web, ventanas emergentes y banners publicitarios. La característica de **bloqueo de llamadas con sobrecosto** ayuda a identificar cualquier software que intente utilizar su modem para conexiones ocultas no autorizadas a servicios telefónicos de pago, para evitar su actuación. *El componente Control de privacidad* incluye un módulo Protección de datos confidenciales que asegura sus datos confidenciales contra el acceso y transmisión no autorizados. *El componente Control parental* de Kaspersky Internet Security controla el acceso a Internet.

Kaspersky Internet Security 7.0 **registra los intentos de análisis de los puertos de su equipo**, que anuncian con frecuencia ataques desde la red y le defiende con éxito contra los ataques de intrusos. El programa utiliza **reglas definidas como básicas** para controlar todas las transacciones de red, examinando todos los **paquetes de datos entrantes y salientes**. **El modo invisible** (derivado de la tecnología SmartStealth™) **impide la detección de su equipo desde el exterior**. Cuando activa este modo, el sistema bloquea cualquier actividad de la red con la excepción de una pocas transacciones autorizadas por reglas personalizadas.

El programa realiza un tratamiento integral para el filtrado de los mensajes de correo entrantes no solicitados:

- Verificación de remitentes en listas negras y blancas (con direcciones de sitios de fraude)
- Inspección de frases en el cuerpo de los mensajes
- Análisis del texto del mensaje mediante un algoritmo de autoaprendizaje
- Identificación de datos no solicitados enviados en archivos de imagen

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile ofrece protección antivirus para terminales móviles bajo Symbian OS y Microsoft Windows Mobile. El programa ofrece un análisis antivirus completo, incluido:

- **Análisis a petición** de la memoria interna del terminal móvil, de las tarjetas de memoria, de carpetas individuales o de archivos específicos; si se detecta un archivo infectado, se mueve a cuarentena o se elimina
- **Análisis en tiempo real**: analiza automáticamente todos los archivos entrantes y salientes, así como los archivos a los que se intenta tener acceso
- **Protección contra mensajes de texto no solicitados**

Kaspersky Anti-Virus for File Servers

Esta distribución ofrece una protección segura de los sistemas de archivos de servidores con Microsoft Windows, Novell NetWare, Linux y Samba, contra todos los tipos de software dañino. La suite incluye las aplicaciones Kaspersky Lab siguientes:

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Windows Server](#).
- [Kaspersky Anti-Virus for Linux File Server](#).

- [Kaspersky Anti-Virus for Novell Netware.](#)
- [Kaspersky Anti-Virus for Samba Server.](#)

Características y funciones:

- *Protege el sistema de archivos del servidor en tiempo real:* Todos los archivos del servidor son analizados cuando se abren o guardan en el servidor
- *Prevención de epidemias víricas;*
- *Análisis a petición:* del sistema de archivos completo o de archivos o carpetas individuales;
- *Utiliza tecnologías de optimización* cuando analiza objetos en el sistema de archivos del servidor;
- *Anula los cambios en el sistema después de ataques de virus;*
- *Escalabilidad del paquete software* dentro de los límites de disponibilidad de los recursos del sistema;
- *Control del equilibrio de carga del sistema;*
- *Creación de una lista de procesos de confianza* cuya actividad en el servidor no está controlada por el paquete software;
- *Administración remota* del paquete software, incluyendo su instalación, configuración y administración centralizadas;
- *Copias de respaldo de los objetos infectados y eliminados* en caso de necesitar restaurarlos;
- *Cuarentena de los objetos sospechosos;*
- *Envío de notificaciones de eventos* sobre la actividad del programa al administrador del sistema;
- *Registro en informes detallados;*
- *Actualización automática* de las bases del programa.

Kaspersky Open Space Security

Kaspersky Open Space Security es un paquete a software con un acercamiento novedoso a la seguridad de las redes corporativas actuales, de cualquier tamaño, que ofrece sistemas de protección centralizados de la información y soporte para oficinas remotas y usuarios móviles.

La suite incluye cuatro programas:

- Kaspersky Work Space Security

- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Las particularidades de cada programa se indican a continuación.

Kaspersky WorkSpace Security es un programa de protección centralizada de estaciones de trabajo, tanto dentro como fuera de las redes corporativas, contra todas las amenazas modernas de Internet (virus, software espía, intrusiones y correo no solicitado).

Características y funciones:

- *Protección integral contra virus, software espía, intrusiones de piratas y correo no solicitado;*
- *Defensa proactiva contra nuevos programas malintencionados cuyas firmas no han sido todavía incluidas en la base de datos;*
- *Personal Firewall con sistema detector de intrusiones y tentativas de ataque por red;*
- *Anulación de los cambios malintencionados en el sistema;*
- *Protección contra tentativas de fraude y correo no solicitado;*
- *Redistribución dinámica de recursos durante los análisis del sistema completo;*
- *Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;*
- *Soporte para Cisco® NAC (Network Admission Control);*
- *Análisis del correo y tráfico Internet en tiempo real;*
- *Bloqueo de ventanas emergentes y banners publicitarios cuando navega en Internet;*
- *Funcionamiento seguro en cualquier tipo de red, incluso inalámbrica (Wi-Fi);*
- *Herramientas para crear discos de emergencia que permiten recuperar el sistema después de un ataque vírico;*
- *Amplio sistema de generación de informes sobre el estado de la protección;*
- *Actualizaciones automáticas de bases de datos;*
- *Soporte completo para sistemas operativos de 64 bits;*

- *Optimización del rendimiento de programas en portátiles (tecnología Intel® Centrino® Duo);*
- *Posibilidades de desinfección remota (Intel® Active Management, Intel® vPro™).*

Kaspersky Business Space Security ofrece una protección óptima de los datos de su organización contra las amenazas actuales de Internet. Kaspersky Business Space Security protege la estaciones de trabajo y los servidores de archivos contra cualquier tipo de virus, troyanos y gusanos, evita epidemias víricas y asegura su información mientras los usuarios se benefician de un acceso instantáneo a los recursos de la red.

Características y funciones:

- *Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;*
- *Soporte para Cisco® NAC (Network Admission Control);*
- *Protección de estaciones de trabajo y servidores de archivos contra cualquier tipo de amenaza Internet;*
- *Tecnología iSwift para no repetir el análisis de archivos dentro de la red;*
- *Distribución de la carga entre los procesadores del servidor;*
- *Cuarentena de los objetos sospechosos en estaciones de trabajo;*
- *Anulación de los cambios malintencionados en el sistema;*
- *Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;*
- *Defensa proactiva para estaciones de trabajo contra nuevos programas malintencionados cuyas firmas no han sido todavía incluidas en la base de datos;*
- *Análisis del correo y tráfico Internet en tiempo real;*
- *Personal Firewall con sistema detector de intrusiones y tentativas de ataque por red;*
- *Protección del uso de redes inalámbricas (Wi-Fi);*
- *Autoprotección contra programas malintencionados;*
- *Cuarentena de los objetos sospechosos;*
- *Actualizaciones automáticas de bases de datos.*

Kaspersky Enterprise Space Security

Este programa incluye componentes de protección de estaciones de trabajo y servidores vinculados contra cualquier tipo de amenaza Internet contemporánea. Elimina los virus del correo, mantiene segura la información mientras ofrece a los usuarios acceso seguro a los recursos de la red.

Características y funciones:

- *Protección de estaciones de trabajo y servidores de archivos contra cualquier tipo de virus, troyanos y gusanos;*
- *Protección de servidores de correo Sendmail, Qmail, Postfix y Exim;*
- *Análisis de todos los correos en Microsoft Exchange Server, incluyendo carpetas compartidas;*
- *Procesado de correos, bases de datos y otros objetos de servidores Lotus Domino;*
- *Protección contra tentativas de fraude y correo no solicitado;*
- *Prevención contra el envío masivo de correo y epidemias víricas;*
- *Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;*
- *Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;*
- *Soporte para Cisco® NAC (Network Admission Control);*
- *Defensa proactiva para estaciones de trabajo contra nuevos programas malintencionados cuyas firmas no han sido todavía incluidas en la base de datos;*
- *Personal Firewall con sistema detector de intrusiones y tentativas de ataque por red;*
- *Protección del uso de redes inalámbricas (Wi-Fi);*
- *Análisis del tráfico Internet en tiempo real;*
- *Anulación de los cambios malintencionados en el sistema;*
- *Redistribución dinámica de recursos durante los análisis del sistema completo;*
- *Cuarentena de los objetos sospechosos;*

- *Amplio sistema de generación de informes sobre el estado de la protección;*
- *Actualizaciones automáticas de bases de datos.*

Kaspersky Total Space Security

Esta solución supervisa todos los flujos de datos entrantes y salientes (correo, Internet y todas las comunicaciones de red). Incluye componentes de protección para estaciones de trabajo y equipo móviles, ofrece a los usuarios acceso seguro a la información de la organización y a Internet y garantiza comunicaciones seguras por correo.

Características y funciones:

- *Protección integral contra virus, software espía, intrusiones de piratas y correo no solicitado en todos los niveles de la red corporativa, desde las estaciones de trabajo a las pasarelas Internet;*
- *Defensa proactiva para estaciones de trabajo contra nuevos programas malintencionados cuyas firmas no han sido todavía incluidas en la base de datos;*
- *Protección de servidores de correo y servidores vinculados;*
- *Análisis del tráfico Internet (HTTP/FTP) que entra en la red local, en tiempo real;*
- *Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;*
- *Prohibición de acceso a estaciones de trabajo infectadas;*
- *Prevención de epidemias víricas;*
- *Sistema de generación de informes centralizado sobre el estado de la protección;*
- *Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;*
- *Soporte para Cisco® NAC (Network Admission Control);*
- *Soporte para servidores proxy hardware;*
- *Filtra el tráfico Internet mediante una lista de servidores de confianza, tipos de objetos y grupos de usuarios;*
- *Tecnología iSwift para no repetir el análisis de archivos dentro de la red;*

- *Redistribución dinámica de recursos durante los análisis del sistema completo;*
- *Personal Firewall con sistema detector de intrusiones y tentativas de ataque por red;*
- *Seguridad para los usuarios de cualquier tipo de red, incluso inalámbrica (Wi-Fi);*
- *Protección contra tentativas de fraude y correo no solicitado;*
- *Posibilidades de desinfección remota (Intel® Active Management, Intel® vPro™);*
- *Anulación de los cambios malintencionados en el sistema;*
- *Autoprotección contra programas malintencionados;*
- *soporte completo para sistemas operativos de 64 bits;*
- *actualizaciones automáticas de bases de datos.*

Kaspersky Security for Mail Servers

Este programa protege los servidores de correo y los servidores vinculados contra los programas malintencionados y el correo no solicitado. El programa incluye aplicaciones para la protección de todos los servidores de correo estándar (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix y Exim) y también le permite configurar una pasarela de correo dedicada. Esta solución incluye:

- [Kaspersky Administration Kit.](#)
- [Kaspersky Mail Gateway.](#)
- [Kaspersky Anti-Virus for Lotus Notes/Domino.](#)
- [Kaspersky Anti-Virus for Microsoft Exchange.](#)
- [Kaspersky Anti-Virus for Linux Mail Server.](#)

Sus características incluyen:

- *Protección segura contra programas malintencionados o potencialmente peligrosos;*
- *Filtrado de correo no solicitado;*
- *Análisis de correos entrantes y salientes, incluyendo los adjuntos;*
- *Análisis antivirus de todos los correos en Microsoft Exchange Server, incluyendo carpetas compartidas;*

- *Procesado de correos, bases de datos y otros objetos de servidores Lotus Notes/Domino;*
- *Filtrado del correo por el tipo de adjunto;*
- *Cuarentena de los objetos sospechosos;*
- *Sencillo sistema administrador del programa;*
- *Prevención de epidemias víricas;*
- *Supervisión del estado del sistema de protección mediante notificaciones;*
- *Generación de informes de actividad del programa;*
- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;
- *actualizaciones automáticas de bases de datos.*

Kaspersky Security for Internet Gateways

Este programa ofrece a todos los empleados de una organización acceso seguro a Internet, y la eliminación automática del software dañino o de riesgo en los datos entrantes por HTTP/FTP. Esta solución incluye:

- [Kaspersky Administration Kit.](#)
- [Kaspersky Anti-Virus for Proxy Server.](#)
- [Kaspersky Anti-Virus for Microsoft ISA Server.](#)
- [Kaspersky Anti-Virus for Check Point FireWall-1.](#)

Sus características incluyen:

- *Protección segura contra programas malintencionados o potencialmente peligrosos;*
- *Análisis del tráfico Internet (HTTP/FTP) en tiempo real;*
- *Filtra el tráfico Internet mediante una lista de servidores de confianza, tipos de objetos y grupos de usuarios;*
- *Cuarentena de los objetos sospechosos;*
- *Sencillo sistema administrador;*
- *Generación de informes de actividad del programa;*
- *Soporte para servidores proxy hardware;*
- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;

- *Actualizaciones automáticas de bases de datos.*

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam es una suite de software avanzado diseñada para ayudar a las organizaciones con redes de tamaño pequeño o mediano a luchar contra la invasión de correos no solicitados (spam). El producto combina una tecnología revolucionaria de análisis lingüístico con todos los métodos modernos de filtrado del correo (incluyendo listas negras de DNS 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 no solicitado. La aplicación es compatible con cualquier sistema de mensajería existente en las instalaciones del cliente, en un servidor de correo existente o dedicado.

Kaspersky® Anti-Spam obtiene sus altas prestaciones gracias a actualizaciones diarias de la base de contenidos filtrados, a partir de las muestras proporcionadas por los especialistas del laboratorio lingüístico. Las bases se actualizan cada 20 minutos.

Kaspersky Anti-Virus® for MIMESweeper

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

El programa es un complemento software que actúa como antivirus y procesa el tráfico de correo entrante y saliente en tiempo real.

B.2. Cómo encontrarnos

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.

Soporte técnico	Encontrará información de asistencia técnica en la dirección http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
-----------------	--

Información	WWW: http://www.kaspersky.com http://www.viruslist.com Correo: info@kaspersky.com
-------------	---

ANEXO C. CONTRATO DE LICENCIA

Contrato estándar de licencia de usuario final

NOTA A TODOS LOS USUARIOS: LEA ATENTAMENTE EL SIGUIENTE CONTRATO DE LICENCIA ("CONTRATO"), PARA EL SOFTWARE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS ("SOFTWARE") FABRICADO POR KASPERSKY LAB ("KASPERSKY LAB").

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

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

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

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

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

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

1.1 *Uso*. El número de equipos que el Usuario puede proteger con el Software viene especificado en el Archivo de llave de licencia y se indica en la ventana "Servicio". El Software no puede utilizarse para proteger redes con un número de equipos superior a éste.

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

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

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

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

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

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

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

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

1.1.9 Eliminación de productos potencialmente dañinos. Usted reconoce y acepta que, además de detectar software dañino y malintencionado, el Producto puede también identificar, eliminar o desactivar productos potencialmente peligrosos, incluso aquellos que han sido clasificados como publicitarios (Adware), de riesgo (Riskware), pornográficos (Pornware), etc.

2. Soporte.

- (i) Kaspersky Lab le proporcionará los servicios de soporte ("Servicios de soporte") definidos para el periodo especificado en el archivo llave de licencia, e indicado en la ventana "Servicio", a partir de la fecha de su adquisición, en los siguientes supuestos:
 - (a) Pago de la cuota vigente de soporte, y;
 - (b) El servicio de soporte técnico de Kaspersky Lab está también habilitado para solicitar al Usuario final datos de registro adicionales para identificarle con derecho a asistencia.
 - (c) Hasta la activación del Software, o la obtención del identificador de Usuario final (Id. de cliente), el soporte técnico tan sólo facilita ayuda para la activación del software y el registro del Usuario final.
- (ii) Al completar el formulario de Suscripción de los Servicios de Soporte, acepta los términos de la Política de privacidad de Kaspersky Lab disponible en la dirección www.kaspersky.com/privacy, y acepta explícitamente que sus datos sean transmitidos a otros países que el suyo, tal y como se describe en la Política de privacidad.
- (iii) 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.
- (iv) "Servicio de soporte" significa:
 - (a) Actualizaciones horarias de la base antivirus;
 - (b) Actualizaciones gratuitas del software, incluidas actualizaciones de la versión de antivirus;
 - (c) Soporte técnico por Internet y teléfono proporcionados por el Fabricante o el Distribuidor;
 - (d) Detección de virus y actualizaciones para su desinfección en un plazo de 24 horas.
- (v) El Servicio de soporte se proporciona sólo cuando la última versión del Software (incluyendo los paquetes de mantenimiento) disponible en el

sitio Internet oficial de Kaspersky Lab (www.kaspersky.com) está instalada en su equipo.

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

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

5. *Garantía limitada.*

- (i) Kaspersky Lab le garantiza que durante seis (6) meses desde la primera descarga o instalación del Software adquirido en un soporte físico, su funcionamiento responderá esencialmente a lo descrito por la Documentación, si se ejecuta de forma apropiada y de la manera especificada en la Documentación.
- (ii) Al seleccionar este software, usted acepta toda la responsabilidad derivada de la satisfacción de sus necesidades. Kaspersky Lab no garantiza que el Software y/o la Documentación son adecuados para sus necesidades, funcionarán de forma ininterrumpida ni que estén libres de errores;
- (iii) Kaspersky Lab no garantiza que este Software identifique todos los virus conocidos, ni que ocasionalmente no detecte por error un virus en un archivo que no está infectado por ese virus.
- (iv) Kaspersky Lab no garantiza que este Software ofrezca protección después de su fecha de caducidad (ver sección.2 (i))
- (v) Su único recurso y la entera responsabilidad de Kaspersky Lab por la ruptura de la garantía mencionada en el párrafo (i) será, según la decisión de Kaspersky Lab, reparación, reemplazo o reembolso del Software si ha informado de esto a Kaspersky Lab o sus proveedores durante el período de la garantía. Debe proporcionar toda la información que pueda ser necesaria para ayudar al Proveedor a determinar el elemento defectuoso;
- (vi) La garantía mencionada en (i) no se aplicará si usted (a) realiza o causa cualquier modificación a este Software sin autorización de Kaspersky Lab,

(b) utiliza el Software de una manera no aplicable (c) no permitida por este Contrato.

- (vii) Las garantías y condiciones especificadas en este Contrato sustituyen todas las otras condiciones, garantías u otros términos acerca de las prestaciones o prestación prevista, ausencia o tardanza en las prestaciones del Software o la Documentación que puedan tener efecto entre Kaspersky Lab y usted, excepto en los casos especificados en este párrafo (vi), o estuvieren implícitas o incorporadas a este Contrato o cualquier contrato colateral, por normativa legal, derecho común o cualquier otra razón, que quedan todas excluidas (incluidas, sin limitación alguna, a condiciones implícitas, garantías u otros términos relativos a niveles razonables de calidad, conveniencia, capacidad y cuidados necesarios).

6. Limitación de responsabilidad.

- (i) Nada en este Contrato excluirá o limitará la responsabilidad de Kaspersky Lab por (a) acto delictuoso de engaño, (b) muerte o daños personales debidos al incumplimiento de obligaciones relativas a la salud o por violación negligente de este Contrato o (c) cualquier responsabilidad que no quede excluida por ley.
- (ii) De acuerdo con el párrafo (i) anterior, el Proveedor no será responsable (por contrato, daño, restitución o cualquier otra forma) por las siguientes pérdidas o daños (si tales pérdidas o daños estaban previstas, eran previsibles, o conocidas de cualquier otra forma):
- (a) Pérdida de ingresos;
 - (b) Pérdida de beneficios reales o anticipados (incluyendo la pérdida de beneficios en contratos);
 - (c) Pérdida del uso de dinero;
 - (d) Pérdida de ahorros anticipados;
 - (e) Pérdida de negocios;
 - (f) Pérdida de oportunidad;
 - (g) Pérdida de buena fe;
 - (h) Pérdida de reputación;
 - (i) Pérdida, daños o corrupción de datos, o:
 - (j) Cualquier otra pérdida o daño incidental o consecuente causado de cualquier forma (incluyendo, para eliminar cualquier duda, pérdida o daño del tipo especificado en los párrafos (ii), (a) - (ii), (i).
- (iii) De acuerdo con el párrafo (i), la responsabilidad de Kaspersky Lab (por contrato, daño, restitución o cualquier otra forma) que es resultado de o está conectada con la entrega del Software, estará en cualquier

circunstancias limitada a una cantidad no mayor que la pagada por el Software.

7. Este contrato contiene el pleno conocimiento de las partes en cuanto a su contenido y reemplaza todos y cualquier declaración, acuerdo o compromiso entre Usted y Kaspersky Lab, tanto oral o como por escrito o formulado en negociaciones 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.

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

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