

Kaspersky Anti-Virus 6.0 SOS MP4

GUÍA DEL USUARIO

VERSIÓN DE LA APLICACIÓN: 6.0 PAQUETE DE MANTENIMIENTO 4



KASPERSKY lab

¡Estimado Usuario de Kaspersky Anti-Virus!

Gracias por elegir nuestro producto. Esperamos que esta documentación lo ayude en su trabajo y le proporcione las respuestas que pueda necesitar.

Todo tipo de reproducción o distribución de cualquier material, incluso en forma traducida, está permitido sólo con el permiso escrito de Kaspersky Lab.

Este documento y las imágenes gráficas que contiene pueden ser utilizados exclusivamente para propósitos de información, no comerciales o personales.

Este documento puede ser modificado sin previo aviso. Para obtener la última versión de este documento, por favor diríjase al sitio web de Kaspersky Lab en <http://latam.kaspersky.com/soporte/support-docs.php>.

Kaspersky Lab no se responsabiliza por el contenido, calidad, importancia o exactitud de los materiales utilizados en este documento, ya que son derechos de terceros, o por los daños potenciales asociados con el uso de tales documentos.

Este documento involucra las marcas registradas y las marcas de servicio que son propiedad de sus respectivos dueños.

Fecha de revisión: 07.09.2009

© 1997-2009 Kaspersky Lab ZAO. Todos los derechos reservados.

<http://latam.kaspersky.com>
<http://usa.kaspersky.com/support/corporate/>

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN.....	7
Contrato de Licencia para usuario final (EULA).....	7
Servicios proporcionados para usuarios registrados.....	7
Requisitos de sistema de hardware y software.....	7
KASPERSKY ANTI-VIRUS 6.0 SOS MP4.....	9
Obtener información acerca de la aplicación.....	9
Fuentes de información para investigar por su cuenta.....	9
Contactar al Departamento de Ventas.....	10
Contactar al servicio de Soporte Técnico.....	10
Tratar las aplicaciones Kaspersky Lab en el foro web.....	11
Qué hay de nuevo en Kaspersky Anti-Virus 6.0 SOS MP4.....	11
Kaspersky Anti-Virus 6.0 SOS MP4.....	13
Tareas de análisis antivirus.....	13
Actualización.....	13
Características de soporte de la aplicación.....	14
INSTALACIÓN DE KASPERSKY ANTI-VIRUS.....	15
Instalación utilizando el Asistente de Instalación.....	15
Paso 1. Verificar que el sistema cumpla con los requisitos de instalación.....	16
Paso 2. Ventana de inicio de la instalación.....	16
Paso 3. Ver el Acuerdo de Licencia.....	16
Paso 4. Seleccionar la carpeta de instalación.....	16
Paso 5. Utilizar la configuración guardada de la instalación anterior.....	17
Paso 6. Seleccionar el tipo de instalación.....	17
Paso 7. Seleccionar los componentes de la aplicación para la instalación.....	17
Paso 8. Buscar otros programas de antivirus.....	18
Paso 9. Completar la instalación.....	18
Instalación de la aplicación de la línea de comando.....	18
Instalación del editor de Objeto de la Política de Grupo.....	19
Instalar la aplicación.....	19
Descripción de las configuraciones del archivo setup.ini.....	19
Actualizar la versión de la aplicación.....	20
Quitar la aplicación.....	20
INTRODUCCIÓN.....	21
Asistente de Configuración Inicial.....	21
Activar la aplicación.....	22
Actualizar los parámetros de configuración.....	23
Configurar el cronograma de análisis de virus.....	24
Restricción de acceso a la aplicación.....	24
Finalizar el Asistente de Configuración.....	25
Analizar equipo en busca de virus.....	25
Actualizar la aplicación.....	25
Administrar licencias.....	26
Administración de la seguridad.....	26
Eliminar problemas. Soporte técnico al usuario.....	27

Crear archivo de rastreo	28
Configurar los parámetros de la aplicación.....	28
Aplicación de reportes de operación. Archivos de datos	29
INTERFAZ DE LA APLICACIÓN	30
Icono del área de notificación de la barra de tareas	30
Menú contextual	31
Ventana Principal de la Aplicación.....	32
Notificaciones	33
Ventana de configuración de la aplicación.....	34
ANALIZAR EQUIPO EN BUSCA DE VIRUS	35
Iniciar el análisis de virus	36
Crear una lista de objetos a analizar	37
Cambiar nivel de seguridad	38
Cambiar acciones a realizar sobre objetos detectados	38
Modificar el tipo de objetos a analizar.....	39
Optimización del análisis	40
Análisis de archivos compuestos	41
Cambiar método de análisis	41
Tecnología de análisis	42
Eficiencia del equipo durante la ejecución de tareas	42
Modo de ejecución: especificar una cuenta	43
Modo de ejecución: crear horario	43
Características de inicio de tareas programadas.....	44
Estadísticas de análisis de virus	44
Asignar parámetros de análisis comunes para todas las tareas	45
Restaurar parámetros de análisis por defecto	45
ACTUALIZACIÓN DE KASPERSKY ANTI-VIRUS	46
Comenzar la actualización.....	47
Reversión a la última actualización.....	48
Selección del origen de actualización	48
Configuración regional.....	49
Utilizar el servidor proxy.....	49
Modo de ejecución: especificar una cuenta	50
Modo de ejecución: crear horario	50
Cambiar modo de ejecución de la tarea de actualización.....	51
Seleccionar objetos para actualizar	51
Actualizar desde una carpeta local	52
Estadísticas de actualización	53
Posibles problemas durante la actualización	53
CONFIGURAR LOS PARÁMETROS DE LA APLICACIÓN	57
Protección.....	58
Lanzar la aplicación en el inicio del sistema operativo de la aplicación	58
Selección de las categorías de amenazas detectables.....	59
Crear una zona de confianza	59
Exportar / importar parámetros de Kaspersky Anti-Virus.	62
Restauración de la configuración predeterminada	63
Análisis	63

Actualización.....	64
Opciones.....	64
Auto-defensa de la aplicación	65
Restricción de acceso a la aplicación	65
Notificaciones acerca de eventos de Kaspersky Anti-Virus.....	66
Elementos activos de la interfaz.....	68
Reportes y Almacenamientos	68
Principios de manejo de reportes	69
Configurar reportes	69
Cuarentena para objetos potencialmente infectados	70
Acciones sobre objetos en cuarentena	71
Copias de resguardo de objetos peligrosos	71
Trabajo con copias de resguardo	71
Configurar cuarentena y resguardo.....	72
VALIDAR PARÁMETROS DE KASPERSKY ANTI-VIRUS	73
Verificar "virus" EICAR y sus modificaciones.....	73
Validar parámetros de análisis antivirus	74
TIPOS DE NOTIFICACIONES	75
Objeto nocivo detectado	75
El objeto no se puede desinfectar.....	76
Objeto sospechoso detectado	76
CÓMO TRABAJAR CON LA APLICACIÓN DESDE LA LÍNEA DE COMANDOS.....	78
Visualizar la Ayuda	79
Análisis antivirus	79
Actualizar la aplicación	81
Reversión a la última actualización.....	82
Inicia / detiene la ejecución de tareas	82
Estadísticas sobre el funcionamiento de una tarea o componente.....	83
Exportar parámetros de protección.....	83
Importar parámetros de protección.....	84
Activar la aplicación	84
Restaurar un archivo de la cuarentena.....	85
Cerrar la aplicación.....	85
Obtener un archivo de rastreo	85
Devuelve códigos de la línea de comandos.....	86
MODIFICAR, REPARAR O QUITAR LA APLICACIÓN.....	87
Modificar, reparar y quitar la aplicación utilizando el Asistente de Instalación.....	87
Paso 1. Ventana de Bienvenida a la Instalación	87
Paso 2. Seleccionar una operación.....	88
Paso 3. Completar la modificación, reparación o eliminación de la aplicación.....	88
Quitar la aplicación desde el prompt del comando	88
ADMINISTRAR LA APLICACIÓN A TRAVÉS DE KASPERSKY ADMINISTRATION KIT	90
Administrar la aplicación	92
Iniciar y detener la aplicación	93
Configurar los parámetros de la aplicación	95
Configurar parámetros específicos	96
Administrar tareas.....	98

Inicio y detención de tareas.....	99
Crear tareas	99
Asistente de Tareas Local.....	100
Configurar tareas	101
Administrar políticas.....	103
Crear políticas	103
Asistente de Creación de Política	104
Configurar la política	106
UTILIZAR CÓDIGO DE UN TERCERO	108
Biblioteca Boost 1.30	109
Biblioteca LZMA SDK 4.40, 4.43	109
Biblioteca Windows Template Library (WTL 7.5)	109
Biblioteca Windows Installer XML (WiX-2.0).....	110
Biblioteca ZIP-2.31	113
Biblioteca ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3	114
Biblioteca UNZIP-5.51	114
Biblioteca LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12.....	115
Biblioteca LIBJPEG-6B.....	117
Biblioteca LIBUNGIF-4.1.4.....	118
Biblioteca MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.....	118
Biblioteca MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.....	118
Biblioteca INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999	119
Biblioteca CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004	119
Biblioteca COOL OWNER DRAWN MENUS-V. 2.4, 2.63 Por Brent Corkum	119
Biblioteca PLATFORM INDEPENDENT IMAGE CLASS	120
Biblioteca FLEX PARSER (FLEXLEXER)-V. 1993	120
Biblioteca ENSURECLEANUP, SWMRG, LAYOUT-V. 2000.....	120
Biblioteca STDSTRING- V. 1999	121
T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006	121
Biblioteca NTSERVICE- V. 1997	122
Biblioteca SHA-1-1.2.....	122
Biblioteca COCOA SAMPLE CODE- V. 18.07.2007.....	122
Otra información	123
GLOSARIO.....	124
KASPERSKY LAB.....	131
ACUERDO DE LICENCIA.....	132
INDEX	138

INTRODUCCIÓN

EN ESTA SECCIÓN

Servicios proporcionados para usuarios registrados	7
Requisitos de sistema de hardware y software	7

CONTRATO DE LICENCIA PARA USUARIO FINAL (EULA)

El Contrato de Licencia para usuario final es un acuerdo legal entre usted y Kaspersky Lab que especifica los términos y condiciones bajo los cuales podrá utilizar el software que ha adquirido.

¡Lea atentamente el Contrato de Licencia para usuario final!

Si usted no está de acuerdo con los términos y condiciones del Contrato de Licencia para usuario final, puede devolver el producto en su caja al revendedor a quien se lo adquirió, y se le devolverá el dinero que pagó por la solicitud, siempre que el sobre que contenga el disco de instalación esté aún sellado.

Al abrir el sobre sellado con el CD de instalación, usted acepta todos los términos y condiciones del Contrato de Licencia para usuario final.

SERVICIOS PROPORCIONADOS PARA USUARIOS REGISTRADOS

Kaspersky Lab ofrece un extenso paquete de servicios para todos los usuarios registrados legalmente, permitiéndoles así obtener mayores resultados de la aplicación.

Luego de adquirir la licencia, usted se convertirá en un usuario registrado y, durante el período de su licencia, podrá utilizar los siguientes servicios:

- actualizaciones cada hora de las bases de datos de aplicaciones y actualizaciones de los paquetes de software;
- soporte en temas relacionados con la instalación, configuración y la utilización del producto de software que ha adquirido. Los servicios se brindarán de manera telefónica o por correo electrónico;
- notificaciones acerca de los nuevos producto de Kaspersky Lab y de los nuevos virus que aparecen a nivel mundial. Este servicio se encuentra disponible para los usuarios que están suscriptos a las noticias por correo de Kaspersky Lab en el sitio web del Servicio de Soporte Técnico (<http://latam.kaspersky.com/soporte/>).

No se brindará soporte técnico en temas relacionados con el rendimiento y el uso de sistemas operativos, software de terceros, u otras tecnologías.

REQUISITOS DE SISTEMA DE HARDWARE Y SOFTWARE

Para un correcto funcionamiento de Kaspersky Anti-Virus 6.0, el equipo deberá cumplir con los siguientes requisitos mínimos:

Requisitos generales:

- 300 MB libres en el disco duro.
- Microsoft Internet Explorer 6.0, o superior (para las aplicaciones de actualización de bases de datos y módulos de programa por Internet).
- Microsoft Windows Installer 2.0, o superior.

Microsoft Windows 2000 Professional (Service Pack 4 Rollup1), Microsoft Windows XP Professional (Service Pack 2, o superior), Microsoft Windows XP Professional x64 (Service Pack 2, o superior):

- procesador Intel Pentium 300 MHz 32-bit (x86) / 64-bit (x64), o superior (o uno equivalente compatible).
- 256 MB libres de memoria RAM.

Microsoft Windows Vista Business / Enterprise / Ultimate (Service Pack 1, o superior), Microsoft Windows Vista Business / Enterprise / Ultimate x64 (Service Pack 1, o superior), Microsoft Windows 7 Professional / Enterprise / Ultimate, Microsoft Windows 7 Professional / Enterprise / Ultimate x64:

- procesador Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64), o superior (o uno equivalente compatible).
- 512 MB libres de memoria RAM.

KASPERSKY ANTI-VIRUS 6.0 SOS MP4

Kaspersky Anti-Virus 6.0 SOS MP4 es una nueva generación de productos para seguridad de la información.

La principal diferencia entre Kaspersky Anti-Virus 6.0 SOS MP4 y los productos existentes es que la aplicación es una herramienta de protección anti-virus complementaria diseñada para el análisis de virus. Al mismo tiempo, Kaspersky Anti-Virus 6.0 SOS MP4 es capaz de cooperar con otras soluciones anti-virus sin crear ningún conflicto.

EN ESTA SECCIÓN

Obtener información acerca de la aplicación.....	9
Qué hay de nuevo en Kaspersky Anti-Virus 6.0 SOS MP4	11
Kaspersky Anti-Virus 6.0 SOS MP4	13

OBTENER INFORMACIÓN ACERCA DE LA APLICACIÓN

Si tiene preguntas respecto de la adquisición, instalación, o utilización de Kaspersky Anti-Virus, ya hay respuestas disponibles para su lectura.

Kaspersky Lab brinda varias fuentes de información sobre la aplicación. Puede elegir la más adecuada de ellas, de acuerdo con la gravedad y urgencia de su pregunta.

EN ESTA SECCIÓN

Fuentes de información para investigar por su cuenta	9
Contactar al Departamento de Ventas	10
Contactar al servicio de Soporte Técnico	10
Tratar las aplicaciones Kaspersky Lab en el foro web.....	11

FUENTES DE INFORMACIÓN PARA INVESTIGAR POR SU CUENTA

Puede dirigirse a las siguientes fuentes de información sobre la aplicación:

- página de la aplicación en el sitio web de Kaspersky Lab;
- página de la aplicación en el sitio web del Servicio de Soporte Técnico (en la Base de Conocimientos);
- sistema de ayuda;
- documentación.

Página de la aplicación en el sitio web de Kaspersky Lab

<http://usa.kaspersky.com/support/corporate/workstation/windows/>

Esta página le brindará información general acerca de la aplicación, sus características y opciones.

Página de la aplicación en el sitio web del Servicio de Soporte Técnico (en la Base de Conocimientos)

<http://usa.kaspersky.com/support/corporate/workstation/windows/>

En esta página, encontrará artículos creados por los especialistas del Servicio de Soporte Técnico.

Estos artículos contienen información útil, recomendaciones y Preguntas de Uso Frecuente (PUF) sobre la adquisición, instalación y utilización de la aplicación. Están clasificados por asunto, como por ejemplo Administrar archivos llave, Configurar actualización de bases de datos, o Eliminar fallos de funcionamiento. Los artículos pueden brindar respuesta a las preguntas referidas no sólo a esta aplicación sino también a otros productos de Kaspersky Lab; también pueden contener novedades del Servicio de Soporte Técnico.

Sistema de Ayuda

El paquete de instalación de la aplicación incluye el archivo de ayuda completa y contextual que contiene información acerca de cómo administrar la protección del equipo (ver estado de protección, analizar distintas áreas del equipo en busca de virus, ejecutar otras tareas), e información sobre cada ventana de la aplicación tal como sus parámetros adecuados y su descripción, y la lista de tareas a ejecutar.

Para abrir el archivo de ayuda, haga click el botón **Ayuda** en la ventana requerida, o presione la tecla <F1>.

Documentación.

El paquete de instalación Kaspersky Anti-Virus incluye la **Guía del Usuario** (en formato PDF). Este documento contiene descripciones de las características y opciones de la aplicación, como así también los algoritmos principales de funcionamiento.

CONTACTAR AL DEPARTAMENTO DE VENTAS

Si tiene preguntas acerca de la elección o adquisición de la aplicación, extensión de la licencia, por favor llame a uno de nuestros distribuidores autorizados o uno de los teléfonos indicados en esta liga:

<http://latam.kaspersky.com/contactenos/>

Tiene la opción de enviar preguntas al Departamento de Ventas llenando la forma en esta liga:

http://latam.kaspersky.com/productos/sales_info_request.php

CONTACTAR AL SERVICIO DE SOPORTE TÉCNICO

Si ya ha adquirido Kaspersky Anti-Virus, puede obtener información al respecto en el Servicio de Soporte Técnico, ya sea en forma telefónica o por Internet.

Los especialistas del Servicio de Soporte Técnico responderán sus preguntas acerca de la instalación y utilización de la aplicación. También lo ayudarán a eliminar las consecuencias de las actividades de software nocivo si su equipo ha sido infectado.

Antes de contactar al Servicio de Soporte Técnico, por favor lea los Términos y Condiciones de Soporte Técnico (<http://support.kaspersky.com/support/rules>).

Petición por correo electrónico al Servicio de Soporte Técnico

Usted puede enviar sus preguntas a los especialistas del Servicio de Soporte Técnico completando el formulario en el sitio web de la Mesa de Ayuda (<http://support.kaspersky.com/helpdesk.html>).

Puede realizar su pregunta en ruso, inglés, alemán, francés o español.

Para enviar una petición por correo electrónico, debe indicar el **ID de cliente** obtenido durante su registro en el sitio web del Servicio de Soporte Técnico junto con la **contraseña**.

Si usted aún no es un usuario registrado de las aplicaciones de Kaspersky Lab, puede llenar un formulario de registro en <https://support.kaspersky.com/en/personalcabinet/registration/form/>. Al registrarse, tendrá que ingresar el *código de activación* o el *nombre de su archivo de clave de licencia*.

El Servicio de Soporte Técnico responderá a su petición en la forma a seguir: <http://usa.kaspersky.com/support/corporate-support-case.php> y mediante el correo electrónico que ha especificado en su petición.

Describa su problema en el formulario de petición brindando el mayor nivel de detalle posible. Especifique los siguientes campos obligatorios:

- **Tipo de petición.** Seleccione la opción que refleje con mayor exactitud su problema, por ejemplo: Problema con la instalación/desinstalación del producto, o Problema con la búsqueda/eliminación de virus. Si no encuentra un ítem adecuado, seleccione "Pregunta General".
- **Nombre de la aplicación y número de versión.**
- **Texto de la petición.** Describa su problema brindando tantos detalles como le sea posible.
- **ID de cliente y contraseña.** Ingrese el número de cliente y la contraseña que ha recibido al registrarse en el sitio web del Servicio de Soporte Técnico.
- **Dirección de correo.** El Servicio de Soporte Técnico le enviará una respuesta a su pregunta a esta dirección de correo.

Soporte técnico por teléfono

Si se produce un problema urgente, siempre puede llamar al Servicio de soporte al número de soporte corporativo basado en los Estados Unidos, horario de la Costa Este: 8am-9pm ET, excepto feriados: 1-866-323-4801.

TRATAR LAS APLICACIONES KASPERSKY LAB EN EL FORO WEB

Si su pregunta no requiere de una respuesta urgente, puede tratarla con los especialistas de Kaspersky Lab y otros usuarios en nuestro foro en <http://forum.kaspersky.com>.

En este foro puede ver temas ya existentes, dejar comentarios, crear temas nuevos y utilizar el motor de búsqueda.

QUÉ HAY DE NUEVO EN KASPERSKY ANTI-VIRUS 6.0 SOS MP4

Kaspersky Anti-Virus 6.0 es una herramienta comprensiva de protección de datos. La aplicación permite realizar un análisis centralizado de estaciones de trabajo en una LAN corporativa sin ningún problema de compatibilidad con otros software anti-virus.

Echemos un vistazo a las innovaciones de Kaspersky Anti-Virus 6.0.

Novidades en protección:

- El nuevo núcleo antivirus que Kaspersky Anti-Virus utiliza detecta programas nocivos de manera más efectiva. Asimismo, el nuevo núcleo antivirus es significativamente más rápido en el escaneo de virus del sistema. Este es el resultado de un procesamiento del objeto mejorado y del uso optimizado de los recursos del equipo (particularmente para procesadores de doble o cuádruple núcleo).
- Se ha implementado un nuevo analizador heurístico que brinda una detección más precisa y un bloqueo de programas maliciosos anteriormente desconocidos. Si no se ha encontrado la firma de un programa en las bases de datos de antivirus, el analizador heurístico simula el lanzamiento del programa en un entorno virtual

aislado. El método es seguro y permite analizar todos los efectos de un programa antes de ejecutarlo en un entorno real.

- Se ha mejorado el proceso de actualización de la aplicación. Ahora, rara vez necesita reiniciar el equipo.

Nuevas características de interfaz:

- La interfaz hace que las características del programa sean simples y fáciles de acceder.
- La interfaz ha sido rediseñada considerando las necesidades de los administradores de redes pequeñas a medianas así como también de administradores de redes de grandes compañías.

Nuevas características en el Kaspersky Administration Kit:

- Se ha agregado una característica que permite la instalación remota de la aplicación con la última versión de las bases de datos de la aplicación.
- Se ha mejorado la administración de la aplicación cuando está instalada en un equipo remoto (se ha rediseñado la política de estructura).
- Se ha sumado una característica que, al crear una política, permite utilizar un archivo de configuración de la aplicación ya existente.
- Otra característica importante se observa en la opción de crear parámetros específicos para los usuarios móviles cuando configuran tareas de actualización de grupo.

KASPERSKY ANTI-VIRUS 6.0 SOS MP4

Kaspersky Anti-Virus incluye:

- Tareas de análisis de virus con las que el equipo o los archivos separados, carpetas, discos, o áreas se analizan ante virus.
- La actualización, asegura el estado actualizado de los módulos de aplicación internos, y las bases de datos utilizadas para analizar en busca de programas nocivos.
- Características del Soporte que brinda información de soporte para trabajar con el programa y expandir sus posibilidades.

EN ESTA SECCIÓN

Tareas de análisis antivirus	13
Actualización	13
Características de soporte de la aplicación	14

TAREAS DE ANÁLISIS ANTIVIRUS

Es muy importante que analice su equipo contra virus de manera periódica. Para este propósito, las siguientes tareas antivirus están incluidas en Kaspersky Anti-Virus:

Escanear

Analiza objetos seleccionados por el usuario. Ud. puede analizar cualquier objeto en el sistema de archivos del equipo.

Escaneo completo

Consiste en un análisis en detalle de todo el sistema. Los siguientes objetos son analizados por defecto: memoria del sistema, programas cargados al iniciar, resguardo del sistema, bases de datos de correo, discos duros, unidades extraíbles de almacenamiento y unidades de red.

Escaneo rápido

Análisis en busca de virus en los objetos de inicio del sistema operativo.

ACTUALIZACIÓN

Para bloquear un ataque por red, eliminar un virus u otro programa nocivo, Kaspersky Anti-Virus debe ser actualizado regularmente. El componente **Actualización** está designado para este propósito. Este maneja la actualización de los módulos y bases de datos utilizados por la aplicación.

El servicio de distribución de actualización permite guardar actualizaciones de bases de datos y módulos de programas bajados de los servidores de Kaspersky Lab a una carpeta local y darles acceso a otros equipos de la red para proteger el tráfico de la red.

CARACTERÍSTICAS DE SOPORTE DE LA APLICACIÓN

Kaspersky Anti-Virus incluye una cantidad de características de soporte. Están designadas para mantener la aplicación al día, ampliar sus posibilidades y asistirlo en el uso de la aplicación.

Archivos de datos

Al utilizar la aplicación se crea un reporte de cada tarea de análisis y actualización de la aplicación. Contiene información acerca de las actividades realizadas y los resultados; con ellos, usted podrá aprender acerca de los detalles de cómo funcionan todas las tareas. En caso que surjan problemas, puede enviar los reportes a Kaspersky Lab para que nuestros especialistas puedan estudiar la situación en profundidad y ayudarlo tan pronto como sea posible.

Kaspersky Anti-Virus mueve todos los archivos potencialmente peligrosos a un área especial de almacenamiento llamada *Cuarentena*. Allí son almacenados en forma cifrada para evitar infectar el equipo. Usted puede analizar estos objetos de virus, restaurarlos a sus ubicaciones anteriores, borrarlos, o poner los archivos en cuarentena por su cuenta. Todos los archivos que resultan no infectados luego de la finalización del análisis de virus, se restauran automáticamente a sus ubicaciones anteriores.

El *Resguardo* mantiene copias de archivos desinfectados y eliminados por Kaspersky Anti-Virus. Estas copias se crean para que pueda restaurar los archivos o una foto de su infección, de ser necesario. Las copias de resguardo de los archivos también son almacenadas en forma cifrada para evitar futuras infecciones.

Puede restaurar un archivo de una copia de resguardo a su ubicación original y eliminar la copia.

Licencia

Al adquirir Kaspersky Anti-Virus, usted contrae con Kaspersky Lab un acuerdo de licencia que rige el uso de la aplicación, su acceso a las actualizaciones de las bases de datos, y Soporte Técnico por un período de tiempo especificado. El término de uso y otra información requerida para el funcionamiento de la aplicación con todas sus características están provistos en una licencia.

Utilizando la función **Licencia** puede obtener información detallada sobre la licencia actual, adquirir una nueva licencia, o renovar la ya existente.

Soporte

Todos los usuarios registrados de Kaspersky Anti-Virus pueden obtener los beneficios de nuestro Servicio de Soporte Técnico. Para ver información de donde puede recibir soporte técnico, utilice la función **Soporte**.

Al utilizar los enlaces provistos, usted puede ir al foro de usuarios de productos Kaspersky Lab y visitar una lista de preguntas realizadas frecuentemente, que pueden darle una solución a su problema. Asimismo, puede llenar el formulario especial en el sitio y enviar un mensaje al Soporte Técnico relacionado con un error o un comentario acerca del funcionamiento del programa.

También tiene acceso al Soporte Técnico en línea, y por supuesto, nuestro personal está siempre listo a brindarle asistencia telefónica sobre Kaspersky Anti-Virus.

INSTALACIÓN DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus 6.0 SOS MP4 puede instalarse junto a cualquier otra aplicación anti-virus por distribuidores de terceros o de Kaspersky Lab, salvo por:

- Kaspersky Anti-Virus 2009;
- Kaspersky Internet Security 2009;
- Kaspersky Anti-Virus 6.0 para Windows Workstations;
- Kaspersky Anti-Virus 6.0 para Windows Servers.

Kaspersky Anti-Virus 6.0 SOS MP4 no puede asegurar la protección del equipo en tiempo real, ¡es un programa anti-virus complementario!

Kaspersky Anti-Virus 6.0 SOS MP4 puede instalarse en un equipo de diferentes maneras:

- instalación local – instalación de la aplicación en un único equipo. Se requiere acceso directo a ese equipo para ejecutar y completar la instalación. La instalación local puede llevarse a cabo de alguna de las siguientes maneras:
 - El modo interactivo, utilizando el asistente de instalación de la aplicación, este modo requiere la participación del usuario para la instalación;
 - El modo no interactivo en que la instalación de la aplicación se abrirá de la línea de comando y no requiere la participación del usuario para la instalación.
- instalación remota – la instalación de la aplicación en equipos en red administrados remotamente desde la terminal de un administrador utilizando lo siguiente:
 - set de software de Kaspersky Administration Kit (ver Guía de Implementación de Kaspersky Administration Kit);
 - políticas de dominio de grupo de Microsoft Windows Server 2000/2003.

Antes de comenzar la instalación de Kaspersky Anti-Virus (incluyendo el remoto), se recomienda cerrar todas las aplicaciones activas.

EN ESTA SECCIÓN

Instalación utilizando el Asistente de Instalación.....	15
Instalación de la aplicación de la línea de comando	18
Instalación del editor de Objeto de la Política de Grupo.....	19

INSTALACIÓN UTILIZANDO EL ASISTENTE DE INSTALACIÓN

Para instalar Kaspersky Anti-Virus en su equipo, ejecutar el archivo de instalación en el CD del producto.

Instalar la aplicación del archivo de instalación descargado a través de Internet, es igual a instalar la aplicación del CD.

El programa de instalación está implementado como un asistente estándar de Windows. Cada ventana contiene un conjunto de botones para controlar el proceso de instalación. Abajo brindamos una breve descripción de su propósito:

- **Siguiente** – acepte la acción y vaya al paso siguiente en el proceso de instalación.
- **Atrás** – vuelve al paso anterior en el proceso de instalación.
- **Cancelar** – cancela la instalación.
- **Terminar** – completa el proceso de instalación de la aplicación.

Abajo encontrará una discusión detallada de cada paso de la instalación del paquete.

PASO 1. VERIFICAR QUE EL SISTEMA CUMPLA CON LOS REQUISITOS DE INSTALACIÓN

Antes de instalar Kaspersky Anti-Virus en el equipo, el asistente verificará que su equipo cumpla con los requisitos mínimos. También verificará que usted tenga los derechos necesarios para instalar el software.

Si no cumple con alguno de los requisitos, se mostrará el aviso correspondiente en la pantalla. Recomendamos que instale toda actualización requerida utilizando el servicio de **Actualización de Windows**, y los programas requeridos, antes de intentar volver a instalar Kaspersky Anti-Virus.

PASO 2. VENTANA DE INICIO DE LA INSTALACIÓN

Si su sistema cumple en su totalidad con los requisitos implícitos, inmediatamente luego del lanzamiento del archivo de instalación, se abrirá la ventana de inicio en la pantalla y mostrará la información en el inicio de la instalación de Kaspersky Anti-Virus.

Para continuar con la instalación, haga click en el botón **Siguiente**. Para cancelar la instalación, haga click en el botón **Cancelar**.

PASO 3. VER EL ACUERDO DE LICENCIA

El cuadro de diálogo de la aplicación contiene el acuerdo de licencia entre usted y Kaspersky Lab. Léalo cuidadosamente, y si está de acuerdo con todos los términos y condiciones del acuerdo, seleccione la opción **Acepto los términos y condiciones del Acuerdo de Licencia** y haga click en el botón **Siguiente**. La instalación continuará.

Para cancelar la instalación, haga click en el botón **Cancelar**.

PASO 4. SELECCIONAR LA CARPETA DE INSTALACIÓN

El siguiente paso de la instalación de Kaspersky Anti-Virus define la carpeta para instalar la aplicación. La ruta por defecto es la siguiente:

- **<Unidad>** → **Archivos de Programa** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 SOS MP4** – para sistemas de 32-bit.
- **<Unidad>** → **Archivos de Programa (x86)** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 SOS MP4** – para sistemas de 64-bit.

Usted puede especificar una carpeta diferente haciendo click en el botón **Examinar** y seleccionar una carpeta en la ventana de selección de carpeta estándar, o ingresar la ruta de la carpeta en el campo de entrada proporcionado.

Por favor note que si ingresa manualmente la ruta completa en la carpeta de instalación, su longitud no deberá exceder los 200 caracteres, y la ruta no deberá contener caracteres especiales.

Para continuar con la instalación, haga click en el botón **Siguiente**.

PASO 5. UTILIZAR LA CONFIGURACIÓN GUARDADA DE LA INSTALACIÓN ANTERIOR

En este paso, se le ofrecerá especificar si usted desea utilizar las configuraciones de protección y las bases de datos en el funcionamiento de la aplicación si estos objetos han sido guardados en su equipo después que una versión previa de Kaspersky Anti-Virus 6.0 haya sido eliminada (si, por ejemplo, usted está instalando la versión comercial luego de haber quitado la versión beta).

Veamos más atentamente cómo habilitar las características descritas anteriormente.

Si una versión anterior (build) de Kaspersky Anti-Virus ha sido instalada en su equipo, y ha guardado las bases de datos de la aplicación luego de haberla eliminado, entonces podrá integrarlas en la versión que está instalando. Para hacerlo, active la casilla **Bases de datos de la aplicación**. Las bases de datos de la aplicación incluidas en el paquete de instalación no se copiarán en su equipo.

Para utilizar las configuraciones de protección que ha modificado en una versión previa y guardado en su equipo, active la casilla **Configuración de la aplicación**.

Haga click en el botón **Siguiente** para continuar.

PASO 6. SELECCIONAR EL TIPO DE INSTALACIÓN

En este paso, deberá definir la finalización de la instalación de la aplicación. Hay dos opciones de instalación:

Completa. En este caso, todos los componentes de Kaspersky Anti-Virus se instalarán en su equipo. Para conocer más sobre los pasos para la instalación, refiérase al Paso 8.

Personalizada. En este caso, se le ofrecerá elegir qué componentes de la aplicación desea instalar. Para más detalles ver Paso 7.

Para seleccionar el modo de instalación, haga click en el botón correspondiente.

PASO 7. SELECCIONAR LOS COMPONENTES DE LA APLICACIÓN PARA LA INSTALACIÓN

Este paso se realizará sólo si eligió la opción de instalación **Personalizada**.

Antes de comenzar con la instalación personalizada, deberá seleccionar qué componentes de Kaspersky Anti-Virus desea instalar. Por defecto, el componente análisis de virus y el conector Agente de Red para administrar la aplicación remotamente vía Kaspersky Administration Kit, se eligen para la instalación.

Para seleccionar un componente para la siguiente instalación, debe abrir el menú haciendo click izquierdo sobre el icono siguiente al nombre del componente y elegir el ítem **Esta característica se instalará en su disco duro local**. Para más detalles acerca de la funcionalidad del componente que ha seleccionado y sobre el espacio de disco requerido para la instalación, por favor vea la parte inferior de esta ventana del programa de instalación.

Para una información más detallada sobre el espacio disponible en el disco de su equipo, haga click en el botón **Volumen**. Se mostrará la información en la ventana que se abrirá.

Para cancelar el componente de instalación, elija la opción **Esta característica no estará disponible** del menú contextual. Tenga en cuenta que al cancelar la instalación de algún componente, no estará protegido contra una cantidad de programas peligrosos.

Cuando haya terminado de seleccionar los componentes a instalar haga click en el botón **Siguiente**. Para volver a la lista de componentes predeterminados a instalarse, haga click en el botón **Restablecer**.

PASO 8. BUSCAR OTROS PROGRAMAS DE ANTIVIRUS

En este paso, el asistente busca otros programas anti-virus instalados en su equipo.

Si se detecta algún software anti-virus de terceros, Kaspersky Anti-Virus 6.0 SOS MP4 continuará su instalación. Se mostrará una notificación para advertirle que la aplicación que se está instalando no puede asegurar una protección completa del equipo.

Para continuar con la instalación, haga click en el botón **Siguiente**.

PASO 9. COMPLETAR LA INSTALACIÓN

La ventana **Instalación completa** contiene información sobre la finalización de la instalación de Kaspersky Anti-Virus en su equipo.

Para ejecutar el Asistente de Configuración Inicial, haga click en el botón **Siguiente**.

Si se requiere que se reinicie la instalación para una finalización exitosa, se mostrará una notificación especial en pantalla.

INSTALACIÓN DE LA APLICACIÓN DE LA LÍNEA DE COMANDO

➤ Para instalar Kaspersky Anti-Virus 6.0 SOS MP4, ingrese lo siguiente en la línea de comandos:

```
msiexec /i <nombre_del_paquete>
```

El asistente de instalación se ejecutará (ver sección "Instalación utilizando el Asistente de Instalación" en página [15](#)).

➤ Para instalar la aplicación en un modo no interactivo (sin abrir el asistente de instalación), escriba lo siguiente:

```
msiexec /i <nombre_del_paquete> /qn
```

➤ Para instalar la aplicación con una contraseña, que confirma el derecho de eliminar la aplicación, escriba lo siguiente:

```
msiexec /i <nombre_del_paquete> KLUNINSTPASSWD=***** – cuando instale la aplicación en modo interactivo;
```

```
msiexec /i <nombre_del_paquete> KLUNINSTPASSWD=***** /qn – cuando instale la aplicación en modo no interactivo sin reiniciar el equipo;
```

Cuando instale Kaspersky Anti-Virus en modo no interactivo, se soporta la lectura del archivo setup.ini; el archivo contiene la configuración general para la instalación de la aplicación, el archivo de configuración *install.cfg* (ver sección Importar la configuración de la protección en página [84](#)), y archivo llave de licencia. Tenga en cuenta que esos archivos deben ubicarse en la misma carpeta que el paquete de instalación de Kaspersky Anti-Virus.

INSTALACIÓN DEL EDITOR DE OBJETO DE LA POLÍTICA DE GRUPO

Al utilizar el **Editor del Objeto de la Política de Grupo** puede instalar, actualizar y eliminar Kaspersky Anti-Virus en estaciones de trabajo de la empresa que forman parte del dominio, sin utilizar el Kaspersky Administration Kit.

INSTALAR LA APLICACIÓN

➔ *Para instalar Kaspersky Anti-Virus, haga lo siguiente:*

1. Crear una carpeta de red compartida en el equipo que funciona como controlador de dominio, y colocar en él el paquete de instalación Kaspersky Anti-Virus en formato *.msi*.

Adicionalmente, en este directorio puede colocar el archivo *setup.ini*, que contiene la lista de configuraciones para la instalación de Kaspersky Anti-Virus, el archivo de configuración *install.cfg* (ver sección Importar las configuraciones de protección en página [84](#)), y un archivo llave de licencia.

2. Abrir el **Editor del Objeto de la Política de Grupo** de la consola estándar MMC (para una información detallada de cómo trabajar con este editor ver el sistema de ayuda de Microsoft Windows Server).
3. Cree un nuevo paquete. Para hacerlo, seleccione **Objeto de la Política de Grupo / Configuración del equipo/ Configuración del programa / Instalación del software** del árbol de consola, y utilice el comando **Crear / Paquete** del menú contextual.

En la ventana que se abrirá, especifique la ruta de la carpeta compartida que almacena el paquete de instalación Kaspersky Anti-Virus. En la casilla de diálogo **despliegue del Programa**, seleccione la configuración **Asignada**, y haga click en el botón **OK**.

La política de grupo será aplicada a cada estación de trabajo cuando se realice el próximo registro de los equipos del dominio. Como resultado, Kaspersky Anti-Virus se instalará en todos los equipos.

DESCRIPCIÓN DE LAS CONFIGURACIONES DEL ARCHIVO SETUP.INI

El archivo *setup.ini* ubicado en el directorio del paquete de instalación de Kaspersky Anti-Virus, es utilizado cuando se instala la aplicación en modo no-interactivo de la línea de comando o del editor del Objeto de la Política de Grupo. Este archivo incluye las siguientes configuraciones:

[Configuración] – configuraciones generales para la instalación de la aplicación.

- **InstallDir**=<ruta a la carpeta de instalación de la aplicación>.
- **Reiniciar=sí|no** – define si su equipo debe reiniciarse cuando la instalación de la aplicación finalice o no (el reinicio no se ejecuta de manera predeterminada).

[Tareas] – habilitar tareas de Kaspersky Anti-Virus. Si no se especifica una tarea, todas las tareas estarán disponibles luego de la instalación. Si se especifica al menos una tarea, las tareas que no han sido listadas serán deshabilitadas.

- **AnalizarMiEquipo=sí|no** – tarea de análisis completo.
- **AnalizarInicio=sí|no** – tarea de análisis rápido.
- **Analizar=sí|no** – tarea de análisis.
- **Actualizador=sí|no** – tarea de actualización para bases de datos de aplicación y módulos de programas.

El 1, encendido, permitir, valores permitidos pueden ser utilizados en lugar del valor **sí**; el 0, apagado, deshabilitado, valores deshabilitados pueden ser utilizados en lugar del valor **no** .

ACTUALIZAR LA VERSIÓN DE LA APLICACIÓN

➤ *Para actualizar la versión de Kaspersky Anti-Virus, haga lo siguiente:*

1. Coloque el paquete de instalación que contiene las actualizaciones de Kaspersky Anti-Virus en formato msi en una carpeta de red compartida.
2. Abra el **Editor de Objeto de la Política de Grupo** y crear un nuevo paquete utilizando el proceso descrito anteriormente.
3. Seleccione el nuevo paquete de la lista y utilice el comando **Propiedades** en el menú contextual. Seleccione la pestaña **Actualizaciones** en la ventana de propiedades del paquete, y especifique el paquete, que contiene el paquete de instalación de la versión anterior de Kaspersky Anti-Virus. Para instalar una versión actualizada de Kaspersky Anti-Virus guardando la configuración de protección, seleccione la opción de instalación por encima del paquete existente.

La política de grupo será aplicada a cada estación de trabajo cuando se realice el próximo registro de los equipos del dominio.

QUITAR LA APLICACIÓN

➤ *Para quitar Kaspersky Anti-Virus, haga lo siguiente:*

1. Abra **Editor de Objeto de la Política de Grupo**.
2. Seleccionar **Objeto_Política_Grupo / Configuración del equipo/ Configuración del programa/ Instalación del software** en el árbol de consola.

Seleccione el paquete Kaspersky Anti-Virus de la lista de paquetes, abra el menú contextual, y ejecute el comando **Todas las tareas/ Eliminar**.

En el cuadro de diálogo **Eliminar aplicaciones**, seleccione **Eliminar inmediatamente esta aplicación de los equipos de todos los usuarios** para que Kaspersky Anti-Virus sea eliminado en el próximo reinicio.

INTRODUCCIÓN

Una de las mayores metas de Kaspersky Lab al crear Kaspersky Anti-Virus era encontrar la configuración óptima de la aplicación. Esto permite a los usuarios con cualquier nivel de conocimientos informáticos reforzar la protección de su equipo inmediatamente después de la instalación sin perder tiempo configurando parámetros.

Sin embargo, los detalles de configuración para su equipo o para las tareas que realice con él pueden ser específicos. Por eso recomendamos realizar una configuración preliminar para lograr un enfoque más flexible y personalizado para proteger su equipo.

Para la conveniencia del usuario, hemos incorporado etapas preliminares de configuración junto con una interfaz unificada del Asistente de Configuración Inicial que comienza al finalizar el proceso de instalación de la aplicación. Siguiendo las instrucciones del Asistente, puede activar la aplicación, configurar los parámetros para las actualizaciones y lanzamiento de tareas de análisis de virus, acceso protegido con contraseña a la aplicación, etc.

Luego de finalizada la instalación y comenzar el programa, recomendamos tomar los siguientes pasos:

- Actualización de la aplicación (a menos que haya sido hecha utilizando el asistente de instalación, o inmediatamente de forma automática luego de que la aplicación haya sido instalada).
- Analizar el equipo en busca de virus.

EN ESTA SECCIÓN

Asistente de Configuración Inicial	21
Analizar equipo en busca de virus.....	25
Actualizar la aplicación	25
Administrar licencias.....	26
Administración de la seguridad	26
Eliminar problemas. Soporte técnico al usuario	27
Crear archivo de rastreo.....	28
Configurar los parámetros de la aplicación	28
Aplicación de reportes de operación. Archivos de datos.....	29

ASISTENTE DE CONFIGURACIÓN INICIAL

El Asistente de Configuración Kaspersky Anti-Virus se inicia cuando finaliza la instalación de la aplicación. Está diseñado para ayudarlo a configurar los parámetros iniciales de la aplicación, sobre la base de las características y tareas de su equipo.

La Interfaz del Asistente de Configuración está diseñada como un Asistente estándar de Microsoft Windows y consiste en una serie de pasos que puede examinar utilizando los botones **Atrás** y **Siguiente**, o completar utilizando el botón **Finalizar**. Para detener la operación del asistente en cualquier momento, pulse el botón **Cancelar**.

Para completar la instalación de la aplicación en el equipo, debe realizar todos los pasos del procedimiento del asistente. Si la operación del asistente ha sido interrumpida por alguna razón, no se guardarán los valores de configuración que ya se hayan especificado. En el próximo intento de ejecutar la aplicación, el Asistente de Configuración Inicial se ejecuta nuevamente requiriendo así editar las configuraciones.

ACTIVAR LA APLICACIÓN

El procedimiento de activación de la aplicación consiste en registrar una licencia instalando un archivo llave. De acuerdo con la licencia, la aplicación determinará los privilegios existentes y calculará el término de uso.

El archivo llave contiene información del sistema requerida por Kaspersky Anti-Virus para ser completamente operativo y como dato adicionales:

- información de soporte (quién provee el soporte, y dónde puede obtenerse);
- nombre llave y número así como también fecha de caducidad de la licencia.

Dependiendo de si ya tiene el archivo llave, o si recibirá uno del servidor de Kaspersky Lab, tendrá las siguientes opciones para activar Kaspersky Anti-Virus:

- Activación en línea (ver página [23](#)). Seleccione este tipo de activación si ha adquirido una versión comercial de la aplicación, y si se le brindado un código de activación. Puede utilizar este código para obtener un archivo llave para brindar acceso al funcionamiento total de la aplicación mediante el período efectivo de la licencia.
- Activar la versión de prueba (ver página [23](#)). Utilice este tipo de activación si desea instalar la versión de evaluación de la aplicación antes de tomar la decisión de adquirir una versión comercial. Se le proveerá un archivo llave gratuito válido por un término especificado en el acuerdo de licencia de la versión de evaluación.
- Activación con una licencia llave obtenida anteriormente (ver sección "Activación utilizando un archivo llave" en página [23](#)). Activar la aplicación utilizando un archivo llave Kaspersky Anti-Virus 6.0 obtenido previamente.
- Activar más tarde. Si elige esta opción, omite el paso de activación. La aplicación se instalará en su equipo, y tendrá acceso a todas las características de la aplicación, salvo por las actualizaciones (sólo una actualización de la aplicación estará disponible, inmediatamente luego de la instalación). La opción **Activar más tarde** no estará disponible la primera vez que inicia el Asistente de Activación. Las próximas veces que inicie el asistente, si la aplicación ya está activada, la opción **Eliminar archivo llave** estará disponible para realizar la eliminación.

Si elige alguna de las primeras dos aplicaciones de activación, la aplicación se activará mediante el servidor web de Kaspersky Lab, que requiere conexión a Internet para utilizar el enlace. Antes de comenzar con la activación, verifique y edite las configuraciones de conexión de red como se requiere en la ventana que se abrirá cuando haga click en el botón **Configuraciones LAN**. Para más detalles acerca de las configuraciones de red, contacte a su administrador de red o a su proveedor de Internet.

Si al momento de la instalación no hay una conexión de Internet disponible, puede realizar la activación más tarde, utilizando la interfaz de la aplicación o conectándose a Internet desde un equipo diferente para obtener una llave, utilizando un código de activación recibido al registrarse en el sitio web del Servicio de Soporte Técnico de Kaspersky Lab.

También puede activar la aplicación utilizando el Kaspersky Administration Kit. Para hacerlo, debe crear una tarea de instalación del archivo llave (ver página [99](#)) (para más detalles refiérase a la guía de ayuda de Kaspersky Administration Kit).

VER TAMBIÉN

Activación en línea	23
Obtener un archivo llave.....	23
Activar utilizando un archivo llave	23
Completar la activación	23

ACTIVACIÓN EN LÍNEA

La activación en línea se realiza ingresando un código de activación que recibirá por correo electrónico cuando compre Kaspersky Anti-Virus por Internet. Si adquiere la aplicación en caja (versión al por menor), el código de activación estará impreso en el sobre que contiene el disco de instalación.

INGRESAR UN CÓDIGO DE ACTIVACIÓN

En este paso, debe ingresar el código de activación. El código de activación es una secuencia de números y letras divididos por guiones en grupos de cuatro o cinco símbolos sin espacios. Por ejemplo, 11111-11111-11111-11111. Tenga en cuenta que el código sólo deberá ingresarse en caracteres latinos.

Ingrese su información personal 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 un usuario registrado si, por ejemplo, la información de su licencia se ha perdido o ha sido robada. En este caso, puede obtener otro código de activación utilizando su información personal.

OBTENER UN ARCHIVO LLAVE

El Asistente de Configuración se conecta a los servidores de Internet de Kaspersky Lab y envía su información de registro, incluyendo el código de activación y su información de contacto. Una vez que se establece la conexión, se verificará el código de activación y su información de contacto. Si el código de activación ha superado la verificación exitosamente, el Asistente recibe un archivo llave que será instalado automáticamente. Al finalizar la activación, se abrirá una ventana con información detallada de la licencia obtenida.

Si el código de activación no ha superado la verificación, la notificación correspondiente aparecerá en la pantalla. Si esto sucede, contacte al distribuidor del software de quien adquirió la aplicación para mayor información.

Si ha excedido la cantidad de activaciones con el código de activación, la notificación correspondiente aparecerá en la pantalla. Se interrumpirá el proceso de activación y la aplicación le ofrecerá contactarse con el servicio de Soporte Técnico de Kaspersky Lab.

ACTIVAR LA VERSIÓN DE EVALUACIÓN

Utilice esta opción si desea instalar una versión de evaluación de Kaspersky Anti-Virus antes de decidir la adquisición de una versión comercial. Se le dará una licencia gratuita, que será válida por el término especificado en el acuerdo de licencia en la versión de prueba. Una vez que la licencia vence, no podrá activar nuevamente la versión de prueba.

ACTIVAR UTILIZANDO UN ARCHIVO LLAVE

Si tiene un archivo llave, puede utilizarlo para activar Kaspersky Anti-Virus. Para realizarlo, utilice el botón **Examinar** y elija la ruta del archivo para el archivo con extensión *.key*.

Luego de haber instalado exitosamente la llave, verá la información sobre la licencia en la parte inferior de la ventana: número de la licencia, tipo de licencia (comercial, beta, de prueba, etc.), fecha de caducidad de la licencia, y cantidad de servidores.

COMPLETAR LA ACTIVACIÓN

El Asistente de Configuración le informará que Kaspersky Anti-Virus ha sido exitosamente activado. Asimismo, se le dará información acerca de la licencia: número de la licencia, tipo de licencia (comercial, beta, de prueba, etc.), fecha de caducidad de la licencia, y cantidad de servidores.

ACTUALIZAR LOS PARÁMETROS DE CONFIGURACIÓN

La calidad del análisis de virus en su equipo depende directamente de recibir de manera oportuna la firma de amenaza y actualización del módulo de la aplicación. En esta ventana, el Asistente de Configuración le pide seleccionar el modo de actualización de la aplicación y editar los parámetros de programación:

-  **Automático.** Kaspersky Anti-Virus verifica la fuente de actualización para paquetes de actualización a intervalos especificados. La frecuencia de análisis puede aumentar durante epidemias de virus y disminuir cuando finalizan. Si se encuentran nuevas actualizaciones, Kaspersky Anti-Virus las descarga e instala en su equipo. Este es el modo por defecto.
-  **Cada 2 hora(s)** (frecuencia que puede variar dependiendo de los parámetros del cronograma). Las actualizaciones se ejecutan de manera automática según el horario creado. Puede modificar los parámetros del cronograma en otra ventana haciendo click en el botón **Cambiar**.
-  **Manual.** Si selecciona esta opción, Ud. ejecutará las actualizaciones de la aplicación por su cuenta.

Tenga en cuenta que las bases de datos de la aplicación y los módulos incluidos dentro del paquete de instalación pueden resultar anticuados al momento que instala la aplicación. Por eso recomendamos que obtenga las últimas actualizaciones de la aplicación. Para realizarlo, haga click en el botón **Actualizar ahora**. Luego Kaspersky Anti-Virus descargará las actualizaciones necesarias desde el sitio de actualizaciones y las instalará en su equipo.

Si desea cambiar la configuración de las actualizaciones (especificar las configuraciones de red, elegir una fuente de actualización, ejecutar una actualización desde una cuenta de usuario específica, o habilitar descargas a una fuente local), haga click en el botón **Configuración**.

CONFIGURAR EL CRONOGRAMA DE ANÁLISIS DE VIRUS

Analizar las áreas elegidas para detectar objetos nocivos es una de las tareas clave que protegen su equipo.

Cuando instala Kaspersky Anti-Virus, se pueden crear tres tipos de tareas de análisis de virus. En esta ventana, el Asistente de Configuración le solicitará que elija un modo de ejecutar la tarea de análisis:

Escaneo completo

Consiste en un análisis en detalle de todo el sistema. Los siguientes objetos son analizados por defecto: memoria del sistema, programas cargados al iniciar, resguardo del sistema, bases de datos de correo, discos duros, unidades extraíbles de almacenamiento y unidades de red. Puede cambiar los parámetros de cronograma en la ventana que se abrirá cuando haga click en el botón **Cambiar**.

Escaneo rápido

Análisis en busca de virus en los objetos de inicio del sistema operativo. Puede cambiar los parámetros de cronograma en la ventana que se abrirá cuando haga click en el botón **Cambiar**.

RESTRICCIÓN DE ACCESO A LA APLICACIÓN

Dado que una computadora personal puede ser utilizada por varias personas con distintos niveles de conocimientos informáticos y que los programas maliciosos pueden desactivar la protección, Ud. tiene la opción de proteger con contraseña el acceso a Kaspersky Anti-Virus. El uso de una contraseña puede proteger la aplicación de intentos de desactivar la protección sin autorización o cambiar los parámetros de configuración de la aplicación.

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

Debajo, especifique el área que desea proteger con una contraseña:

-  **Todas las operaciones (excepto notificaciones de eventos peligrosos).** La contraseña será requerida si el usuario intenta realizar cualquier acción sobre la aplicación, además de responder a las notificaciones acerca de objetos peligrosos.
-  **Operaciones seleccionadas:**
 - **Configurar los parámetros de la aplicación** – solicita una contraseña si un usuario intenta modificar los parámetros de la aplicación.
 - **Cerrar la aplicación** – la contraseña será requerida cuando el usuario intente cerrar la aplicación.

- **Detener tareas de análisis** – requiere contraseña si un usuario intenta detener una tarea de análisis antivirus.
- **Al desinstalar la aplicación** – requiere contraseña si el usuario intenta eliminar la aplicación del equipo.

FINALIZAR EL ASISTENTE DE CONFIGURACIÓN

Si es necesario, verifique la casilla del **Inicio de la aplicación** en la última ventana y presione el botón **Finalizar** para completar al Asistente de Configuración Inicial.

ANALIZAR EQUIPO EN BUSCA DE VIRUS

Los creadores de programas nocivos se esfuerzan por ocultar sus acciones, y por lo tanto puede que no note la presencia de programas nocivos en su equipo.

Una vez que Kaspersky Anti-Virus esté instalado en su equipo, automáticamente realizará la tarea de **Escaneo Rápido**. Esta tarea busca y neutraliza programas dañinos en objetos cargados al iniciar el sistema operativo.

Los especialistas de Kaspersky Lab también recomiendan que lleve a cabo la tarea de **Escaneo Completo**.

➔ *Para iniciar / detener una tarea de análisis de virus, haga lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Haga click en el botón **Iniciar Escaneo** para comenzar el análisis. Si desea detener la ejecución de la tarea, haga click en el botón **Detener Escaneo** mientras la tarea está en progreso.

ACTUALIZAR LA APLICACIÓN

Necesitará estar conectado a Internet para actualizar Kaspersky Anti-Virus.

El paquete de instalación Kaspersky Anti-Virus incluye las bases de datos que contienen las firmas de las amenazas. En el momento que instala la aplicación, estas bases de datos pueden tornarse obsoletas, ya que las actualizaciones de Kaspersky Lab tanto para las bases de datos como para los módulos de aplicaciones se realizan regularmente.

Cuando el Asistente de Configuración Inicial está activo, puede elegir el modo de ejecución de la actualización. Por defecto, Kaspersky Anti-Virus verifica automáticamente si existen actualizaciones en los servidores de Kaspersky Lab. Si el servidor contiene nuevas actualizaciones, Kaspersky Anti-Virus las descargará e instalará en modo silencioso.

Para mantener la protección de su equipo al día, se recomienda actualizar Kaspersky Anti-Virus inmediatamente después de la instalación.

➔ *Para actualizar Kaspersky Anti-Virus por su cuenta, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Pulse el botón **Iniciar la actualización**.

ADMINISTRAR LICENCIAS

Kaspersky Anti-Virus requiere una licencia para funcionar. Al adquirir el producto, recibirá una licencia. Le da derecho a utilizar el producto tan pronto como lo active.

Sin una licencia, si no se ha activado la versión de prueba de la aplicación, Kaspersky Anti-Virus se ejecutará en modo de una actualización. La aplicación no descargará ninguna nueva actualización.

Si se ha activado la versión de prueba de la aplicación, Kaspersky Anti-Virus no se ejecutará luego de que la licencia gratuita expire.

Cuando expira una licencia comercial el programa seguirá funcionando, con la salvedad que no podrá actualizar las bases de datos de la aplicación. Como anteriormente, podrá analizar su equipo en busca de virus y utilizar los componentes de protección, pero sólo utilizando las bases de datos que tenía al expirar la licencia. No podemos garantizar que Ud. estará protegido contra virus que puedan aparecer después de la expiración de su licencia.

Para evitar infectar su equipo con nuevos virus, recomendamos renovar su licencia para Kaspersky Anti-Virus. Dos semanas antes de que la licencia expire, la aplicación le notificará al respecto. Durante determinado período, se mostrará un mensaje correspondiente cada vez que se inicie la aplicación.

Se mostrará información general sobre la licencia actualmente en uso (licencias activas y adicionales si estas últimas han sido instaladas) en la sección **Licencia** de la ventana principal de Kaspersky Anti-Virus: tipo de licencia (completa, de prueba, beta), cantidad máxima de servidores, fecha de caducidad de la licencia, y cantidad de días restantes hasta la fecha de caducidad de la licencia. Para obtener más detalles acerca de la licencia, haga click en el enlace que contiene el tipo de licencia que actualmente tiene en uso.

Para ver las condiciones del acuerdo de licencia de la aplicación, haga click en el botón **Ver el Acuerdo de Licencia de Usuario Final**.

Para quitar la licencia, haga click en el botón **Agregar / Eliminar** y siga las instrucciones del asistente que se abrirá.

Kaspersky Lab tiene ofertas especiales para la renovación de la licencia de nuestros productos. Verificar ofertas especiales en el sitio web de Kaspersky Lab.

➔ *Para adquirir o renovar una licencia, haga lo siguiente:*

1. Adquiera un nuevo archivo llave o un código de activación. Para hacerlo, utilice la **licencia de Compra** (si la aplicación no ha sido activada) o los botones para la **renovación de la Licencia**. En el sitio web que se abrirá encontrará información detallada sobre los términos para adquirir la llave de la eStore de Kaspersky Lab o de distribuidores autorizados. Si realiza la compra en línea, recibirá un archivo llave o un código de activación por correo a la dirección especificada en el formulario de la orden una vez que se haya realizado el pago.
2. Activar la aplicación. Utilice el botón **Agregar / Eliminar** en la sección **Licencia** de la aplicación principal de la ventana, o utilice el comando **Activar** desde el menú contextual de la aplicación. Esto iniciará el Asistente de Activación.

ADMINISTRACIÓN DE LA SEGURIDAD

Los problemas de protección en su equipo se indican en el estado de protección en su equipo, por medio de los cambios en el color del ícono de estado de protección, y del panel en que el ícono está ubicado. Cuando aparezcan problemas en la protección, se le aconseja que los solucione.



Figura 1. Estado actual de protección del equipo

Puede ver la lista de problemas ocurridos, su descripción y posibles maneras de solucionarlos, mediante el Asistente de Seguridad (ver la figura a continuación) que puede activarse haciendo click en el enlace **Reparar** (ver la figura anterior).



Figura 2. Solucionar problemas de seguridad

Puede visualizar la lista de problemas actuales. Los problemas son ordenados de acuerdo con su calidad crítica: primero, los más críticos (con el ícono en color rojo), luego los menos críticos –con ícono de estado en color amarillo-, y por último, mensajes de información. Se provee una información detallada para cada problema y las siguientes acciones están disponibles:

- **Eliminar inmediatamente.** Al utilizar los enlaces adecuados, puede i a solucionar el problema, que es la acción recomendada.
- **Posponer la eliminación.** Si, por cualquier razón, la eliminación inmediata del problema no fuera posible, puede posponer esta acción y volver a ella más tarde. Active la casilla **Ignorar esta amenaza al determinar el estado de seguridad** para que la amenaza no afecte el estado de protección actual.

Tenga en cuenta que esta acción no está disponible para problemas serios. Tales problemas incluyen, por ejemplo, objetos nocivos que no fueron desinfectados, fallas de uno o varios componentes, o corrupción de los archivos de la aplicación. Problemas como estos deben eliminarse tan rápido como sea posible.

ELIMINAR PROBLEMAS. SOPORTE TÉCNICO AL USUARIO

Si ocurren problemas con el funcionamiento de Kaspersky Anti-Virus, el primer lugar para verificar para ayudar a solucionar el problema es el sistema de Ayuda. El segundo lugar es la Base de Conocimiento de Kaspersky Lab (<http://usa.kaspersky.com/support/corporate/>). La *Base de conocimientos* es una sección aparte del sitio web del soporte técnico, y contiene recomendaciones para los productos de Kaspersky Lab y respuestas a las preguntas más frecuentes. Intente encontrar una respuesta a su pregunta o una solución a su problema con este recurso.

➤ *Para utilizar la Base de Conocimientos, haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte inferior de la pestaña, haga click en el enlace **Soporte**.
3. En la ventana de **Soporte** que se abrirá, haga click en el enlace **Servicio de Soporte Técnico**.

Otro recurso que puede utilizar para obtener información sobre cómo trabajar con la aplicación es el Foro de usuarios de Kaspersky Lab. Es otra sección aparte del sitio web del soporte técnico y contiene preguntas de usuarios, comentarios y peticiones. Puede ver los tópicos principales del foro, dejar un comentario o encontrar la respuesta a una pregunta.

➤ *Para abrir el foro de usuarios, haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte inferior de la pestaña, haga click en el enlace **Soporte**.
3. En la **ventana** Soporte que se abrirá, haga click en el enlace **Foro de usuarios**.

Si no encuentra una solución a su problema en Ayuda, en la Base de Conocimiento, o en el Foro de Usuarios, recomendamos que contacte al Soporte Técnico de Kaspersky Lab.

CREAR ARCHIVO DE RASTREO

Después de instalar Kaspersky Anti-Virus, pueden ocurrir algunos fallos en el sistema operativo o en el funcionamiento de algunas aplicaciones en particular. La causa más probable es un conflicto entre la aplicación y el software instalado en su equipo, o con los controladores de los componentes de su equipo. Se le ofrecerá crear un archivo de rastreo para que los especialistas de Kaspersky Lab resuelvan exitosamente su problema.

➤ *Para crear una archivo de rastreo:*

1. Abra la ventana principal del programa.
2. En la parte inferior de la pestaña, haga click en el enlace **Soporte**.
3. En la ventana **Soporte** que se abrirá, haga click en el enlace **Rastreos**.
4. En la ventana **Información del Servicio de soporte técnico** que se abrirá, utilice la lista desplegable de la sección **Rastreos** para seleccionar el nivel de rastreo. El nivel de rastreo debería establecerse de acuerdo con la recomendación del especialista del soporte técnico. Si no se dispone de instrucciones del soporte técnico, se le recomienda establecer el nivel de rastreo en **500**.
5. Para iniciar el proceso de rastreo, haga click en el botón **Activar**.
6. Recrear la situación que ocasionó el problema.
7. Para detener el proceso de rastreo, haga click el botón **Desactivar**.

CONFIGURAR LOS PARÁMETROS DE LA APLICACIÓN

La ventana de configuración de la aplicación (ver página [57](#)) que puede accederse desde la ventana principal haciendo click en el botón **Configuración**, está diseñada para acceder rápidamente a los parámetros de Kaspersky Anti-Virus 6.0.

APLICACIÓN DE REPORTE DE OPERACIÓN. ARCHIVOS DE DATOS

Cada análisis o tarea de actualización está registrado en un reporte (ver página [69](#)). Para ver los reportes, utilice el botón **Reportes** en la esquina inferior derecha de la ventana principal.

Los objetos que han estado en cuarentena (ver página [70](#)) o colocados en resguardo (ver página [71](#)) por Kaspersky Anti-Virus, se denominan *archivos de aplicación de datos*. Al presionar el botón **Detectado**, puede abrir la ventana **Almacenamiento**, en el que puede procesar estos objetos según sea necesario.

INTERFAZ DE LA APLICACIÓN

Kaspersky Anti-Virus posee una interfaz sencilla y fácil de utilizar. Este capítulo destaca sus características básicas:

- ícono de la bandeja del sistema;
- menú contextual;
- ventana principal;
- notificaciones;
- ventana de parámetros de Kaspersky Anti-Virus.

Además de la interfaz principal, la aplicación tiene un complemento para Microsoft Windows Explorer. El complemento extiende la funcionalidad de Microsoft Windows Explorer brindando la posibilidad de utilizar su interfaz para administrar Kaspersky Anti-Virus 6.0 SOS MP4.

EN ESTA SECCIÓN

Icono del área de notificación de la barra de tareas	30
Menú contextual	31
Ventana Principal de la Aplicación	32
Notificaciones	33
Ventana de configuración de la aplicación	34

ICONO DEL ÁREA DE NOTIFICACIÓN DE LA BARRA DE TAREAS

Inmediatamente luego de instalar Kaspersky Anti-Virus, sus íconos aparecerán en la bandeja del sistema.

El ícono es una especie de indicador de las funciones de Kaspersky Anti-Virus. También refleja el estado de protección y muestra un número de operaciones básicas realizadas por la aplicación.

Si el ícono  está presente en la bandeja del sistema, Kaspersky Anti-Virus está activado.

El ícono de Kaspersky Anti-Virus cambia según la operación que se esté realizando:

 el análisis del archivo está en progreso.

 La base de datos de Kaspersky Anti-Virus y el módulo de actualización están en progreso.

 ha ocurrido un error en la operación de algún componente de Kaspersky Anti-Virus.

El ícono también brinda acceso a los componentes básicos de la interfaz de la aplicación: menú contextual y ventana principal.

Para abrir el menú contextual, haga click derecho en el ícono de la aplicación.

Para abrir la ventana principal de Kaspersky Anti-Virus, haga click sobre ícono de la aplicación.

MENÚ CONTEXTUAL

Puede ejecutar las tareas de protección básicas del menú contextual, que contienen los siguientes elementos:

- **Escaneo Completo** – inicia un análisis completo de su equipo en busca de objetos de programas nocivos. Se analizarán objetos ubicados en todas las unidades, incluyendo las extraíbles.
- **Análisis** – selecciona objetos e inicia un análisis antivirus. Por defecto, la lista contiene una cantidad de archivos, como la carpeta **Mis Documentos**, objetos del Inicio, bases de datos de correo electrónico, todas las unidades de disco de su equipo, etc. Puede ampliar la lista, seleccionar otros objetos para análisis y comenzar el análisis en busca de virus.
- **Actualizar** - inicia la actualización del módulo y las firmas de amenazas de Kaspersky Anti-Virus y las instala en su equipo.
- **Activar** – activa la aplicación. Para ser un usuario registrado con acceso a toda la funcionalidad de las aplicaciones y el Soporte Técnico, debe activar su versión de Kaspersky Anti-Virus. Este ítem del menú sólo está disponible si la aplicación no ha sido activada.
- **Configuración** – ve y configura los parámetros de la aplicación Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus** – abre la ventana principal de la aplicación.
- **Acerca de** – mostrar ventana con información acerca de la aplicación.
- **Salir** – cierra Kaspersky Anti-Virus (cuando se seleccione esta función, la aplicación será descargada de la RAM del equipo).



Figura 3. Menú contextual

Si se está ejecutando la tarea de análisis de virus, se indicará el nombre en el menú contextual con la indicación del porcentaje en progreso. Luego de seleccionar una tarea, puede ir a la ventana del reporte para visualizar el resultado actual del rendimiento.

VENTANA PRINCIPAL DE LA APLICACIÓN

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

- La parte superior de la ventana indica el estado actual de protección de su equipo.



Figura 4. Estado actual de protección del equipo

Existen tres valores posibles del estado de protección: cada uno de ellos se indica con un determinado color, parecido a un semáforo. El verde indica que la protección de su equipo está en el nivel correcto, mientras que el amarillo y el rojo indican que hay amenazas de seguridad en la configuración del sistema o en el funcionamiento de Kaspersky Anti-Virus. Además de los programas nocivos, las amenazas incluyen, por ejemplo, bases de datos obsoletas de la aplicación.

Las amenazas a la seguridad deben eliminarse tan pronto como aparecen. Para obtener una información detallada acerca de ellos y para eliminarlos rápidamente, utilice el enlace **Reparar** (ver figura anterior).

- La parte izquierda de la ventana brinda un acceso rápido a las tareas de análisis de virus, actualizaciones, etc.



Figura 5. Parte izquierda de la ventana principal

- La parte derecha de la ventana brinda herramientas para realizar tareas de análisis de virus, descarga de actualizaciones, etc.

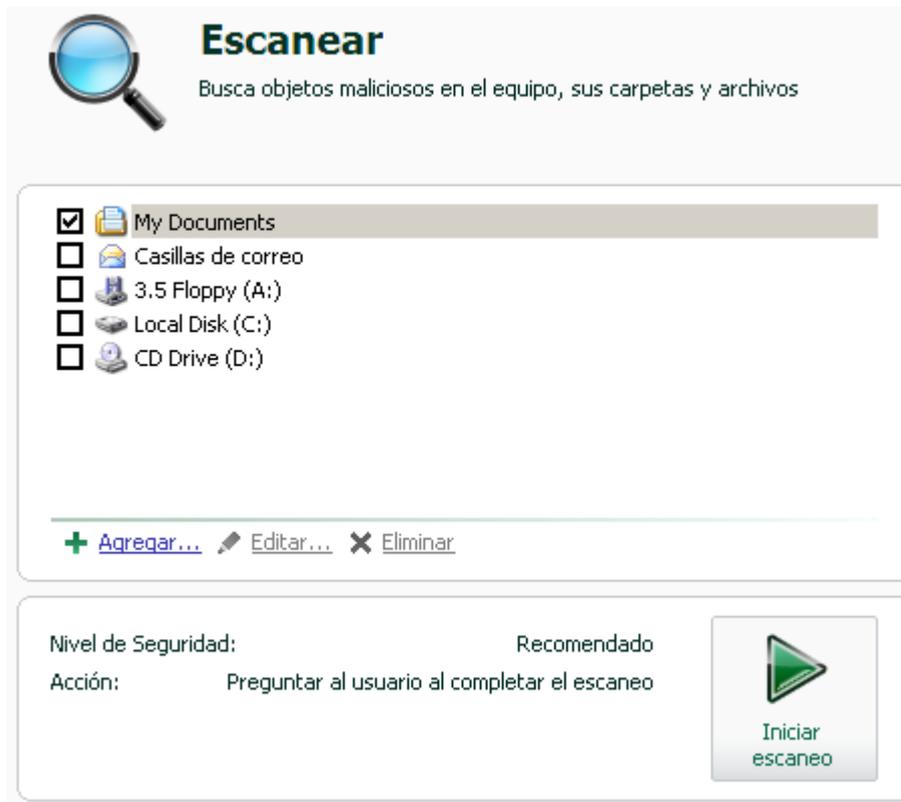


Figura 6. Parte derecha de la ventana principal

También puede utilizar:

- El botón **Configuración** – para abrir la ventana de configuración de la aplicación (ver página [57](#)).
- El enlace **Ayuda** – para abrir la Ayuda de Kaspersky Anti-Virus.
- El botón **Detectado** – para trabajar con archivos de datos de la aplicación (ver página [68](#)).
- El botón **Reportes** – para abrir los reportes en el funcionamiento de los componentes de la aplicación (ver página [69](#)).
- El enlace **Soporte** – para abrir la ventana que contiene la información sobre el sistema y los enlaces a los recursos informativos de Kaspersky Lab (ver página [27](#)) (sitio web del servicio de Soporte Técnico, foro).

NOTIFICACIONES

Si ocurren eventos durante el funcionamiento de Kaspersky Anti-Virus, se mostrarán notificaciones especiales en pantalla, como mensajes emergentes sobre el icono de la aplicación en la barra de tareas de Microsoft Windows.

Dependiendo de la criticidad del evento para su equipo, usted podría recibir los siguientes tipos de notificación:

- **Alarma.** Ha ocurrido un evento de importancia crítica, como un virus que ha sido detectado. Ud. deberá decidir inmediatamente qué hacer con esta amenaza. Este tipo de información está codificada en color rojo.
- **Advertencia.** Ha ocurrido un evento potencialmente peligroso, como un objeto potencialmente peligroso que ha sido detectado. Deberá decidir cuán peligroso cree que sea este evento. Este tipo de información está codificada en color amarillo.

- **Info.** Esta notificación brinda información sobre eventos no críticos. Las notificaciones menores están codificadas en color verde.

VER TAMBIÉN

Tipos de notificaciones [75](#)

VENTANA DE CONFIGURACIÓN DE LA APLICACIÓN

La ventana de configuración de Kaspersky Anti-Virus puede abrirse desde la ventana principal o utilizando el menú contextual. Para hacerlo, haga click en el botón **Configuración** en la parte superior de la ventana principal, o seleccione la opción apropiada en el menú contextual de la aplicación.

La ventana de configuración de la aplicación tiene de dos partes:

- la parte izquierda de la ventana le brinda acceso a los componentes de Kaspersky Anti-Virus, tareas de análisis de virus, tareas de actualización, etc.;
- la parte derecha de la ventana contiene la lista de parámetros del ítem (componente, tarea, etc.) seleccionado en la izquierda de la ventana.

VER TAMBIÉN

Configurar los parámetros de la aplicación [57](#)

ANALIZAR EQUIPO EN BUSCA DE VIRUS

Kaspersky Anti-Virus 6.0 SOS MP4 puede analizar los elementos en forma separada (archivos, carpetas, discos, medios removibles) o todo el equipo en busca de virus.

Kaspersky Anti-Virus 6.0 SOS MP4 comprende las siguientes tareas predeterminadas de análisis antivirus:

Escanear

Analiza objetos seleccionados por el usuario. Ud. puede analizar cualquier objeto en el sistema de archivos del equipo.

Escaneo completo

Consiste en un análisis en detalle de todo el sistema. Los siguientes objetos son analizados por defecto: memoria del sistema, programas cargados al iniciar, resguardo del sistema, bases de datos de correo, discos duros, unidades extraíbles de almacenamiento y unidades de red.

Escaneo rápido

Análisis en busca de virus en los objetos de inicio del sistema operativo.

Por defecto, aquellas tareas se ejecutan con parámetros recomendados. Estos parámetros pueden ser modificados, y las tareas pueden ser programadas para ejecutarse.

Asimismo, todo objeto puede ser analizado (como un disco duro que almacena software y juegos, bases de datos de correo traídas de la oficina a la casa, un archivo comprimido recibido por correo, etc.) sin crear una tarea de análisis dedicada. Un objeto a analizar puede ser seleccionado utilizando la interfaz de Kaspersky Anti-Virus o las herramientas estándar de Microsoft Windows (por ejemplo, **Windows Explorer** o **Escritorio**, etc.). Colocar el cursor en el nombre del objeto deseado, hacer click derecho para abrir el menú contextual, y seleccionar la opción **Buscar virus**.

Colocar el cursor en el nombre del objeto deseado, hacer click derecho para abrir el menú contextual, y seleccionar la opción **Buscar virus**.

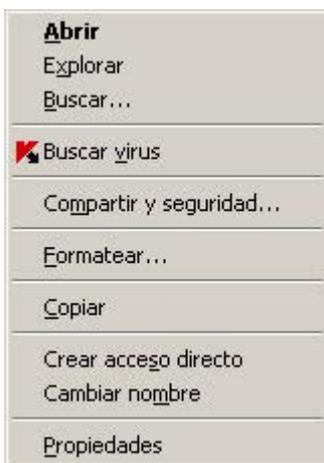


Figura 7. Menú contextual de Microsoft Windows

Adicionalmente, luego de un análisis usted puede ver el reporte del análisis que contiene información completa sobre los eventos ocurridos durante la ejecución de las tareas.

► Para cambiar los parámetros de toda tarea de análisis de virus, por favor haga lo siguiente:

1. Abrir la ventana principal del programa.

2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, realice los cambios necesarios en los parámetros de la tarea que ha seleccionado.

➔ *Para cambiar al reporte del análisis del virus, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Haga click en el botón **Reportes**.

EN ESTA SECCIÓN

Iniciar el análisis de virus.....	36
Crear una lista de objetos a analizar	37
Cambiar nivel de seguridad.....	38
Cambiar acciones a realizar sobre objetos detectados	38
Modificar el tipo de objetos a analizar	39
Optimización del análisis	40
Análisis de archivos compuestos	41
Cambiar método de análisis	41
Tecnología de análisis.....	42
Eficiencia del equipo durante la ejecución de tareas.....	42
Modo de ejecución: especificar una cuenta.....	43
Modo de ejecución: crear horario	43
Características de inicio de tareas programadas	44
Estadísticas de análisis de virus.....	44
Asignar parámetros de análisis comunes para todas las tareas	45
Restaurar parámetros de análisis por defecto.....	45

INICIAR EL ANÁLISIS DE VIRUS

Usted puede comenzar una tarea de análisis de virus en una de las siguientes formas:

- desde el menú contextual de Kaspersky Anti-Virus;
- desde la ventana principal de Kaspersky Anti-Virus.

Se mostrará información sobre la ejecución de la tarea en la ventana principal de Kaspersky Anti-Virus.

Además, puede seleccionar un objeto para analizarlo con las herramientas estándar del sistema operativo Microsoft Windows, por ejemplo, en la ventana del **Explorador** o en su **Escritorio**, etc.).

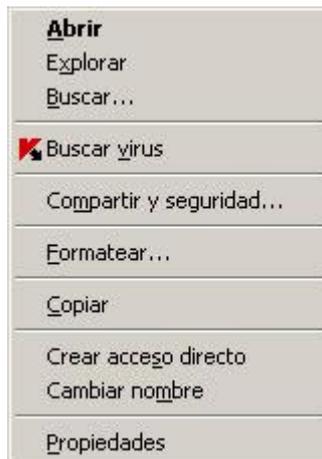


Figura 8. Menú contextual de Microsoft Windows

➔ Para comenzar una tarea de análisis de virus del menú contextual, por favor haga lo siguiente:

1. Pulse con el botón derecho el ícono de la aplicación en el área de notificaciones de la barra de tareas.
2. Seleccione el ítem **Escanear** del menú desplegable. En la ventana principal de la aplicación que se abrirá, seleccione la tarea requerida de **Escanear (Escaneo Completo, Escaneo rápido)**. Si se requiere, configurar la tarea seleccionada y haga click en el botón **Iniciar análisis**.
3. Alternativamente, puede seleccionar el ítem **Escaneo Completo** del menú contextual. Esto iniciará un análisis completo del equipo. Se mostrará el progreso de la tarea en la ventana principal de Kaspersky Anti-Virus.

➔ Para iniciar el análisis en busca de virus desde la ventana principal de la aplicación:

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Haga click en el botón **Iniciar análisis** para la sección seleccionada. El progreso de ejecución de la tarea se mostrará en la ventana principal de la aplicación.

➔ Para iniciar desde el menú contextual de Microsoft Windows una tarea de análisis en busca de virus sobre un objeto seleccionado:

1. Haga click-derecho en el nombre del objeto seleccionado.
2. Seleccione el ítem **Analizar en busca de virus** en el menú contextual que se abrirá. El progreso y los resultados de la ejecución de la tarea se mostrará en la ventana estadísticas.

CREAR UNA LISTA DE OBJETOS A ANALIZAR

Cada tarea de análisis en busca de virus posee su propia lista de objetos por defecto. Para ver una lista de objetos, seleccione el nombre de la tarea (tal como **Escaneo Completo**) en la sección **Escanear** de la ventana principal de la aplicación. La lista de objetos se mostrará en la parte derecha de la ventana.

Las listas de objetos a analizar ya están generadas para las tareas por defecto creadas en la instalación de la aplicación.

Según la conveniencia del usuario, puede agregar categorías al alcance del análisis, tales como casillas de correo del usuario, memoria RAM, objetos de inicio, respaldo del sistema operativo, y archivos en la carpeta de Cuarentena de Kaspersky Anti-Virus.

Asimismo, cuando agrega una carpeta que contiene objetos incrustados para el alcance del análisis, puede editar la recursión. Para hacerlo, seleccione el objeto requerido de la lista de objetos a analizar, abra el menú contextual, y utilice la opción **Incluir subcarpetas**.

➔ *Para crear una lista de objetos a analizar, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Haga click en el enlace **Agregar** para la sección seleccionada.
4. En la ventana **Seleccionar el objeto a analizar** que se abrirá, seleccione el objeto y haga click en el botón **Agregar**. Presione el botón **OK** después agregar todos los objetos que necesitaba. Para excluir cualquier objeto de la lista de objetos a analizar, desactive las casillas próximas a éste. Para quitar un objeto de la lista, selecciónelo y haga click en el enlace **Eliminar**.

CAMBIAR NIVEL DE SEGURIDAD

El nivel de seguridad es un conjunto predeterminado de parámetros de análisis. Los especialistas de Kaspersky Lab distinguen tres niveles de seguridad. Usted deberá tomar la decisión sobre el nivel a seleccionar en base a sus preferencias:

- Si sospecha que su equipo tiene una alta posibilidad de infectarse, seleccione el nivel de seguridad Alto.
- El nivel recomendado es adecuado en la mayoría de los casos, y es el aconsejado para su uso por los especialistas de Kaspersky Lab.
- Si Ud está utilizando programas que consumen considerables recursos RAM, seleccione el nivel de seguridad bajo, porque así la aplicación disminuye su demanda de recursos del sistema.

Si ninguno de estos niveles predeterminados se ajusta a sus necesidades, entonces configure Ud. mismo los parámetros del análisis. En este caso, el nombre del nivel de seguridad cambiará a **Personalizado**. Para restaurar la configuración predeterminada del análisis, seleccione uno de los niveles de seguridad. Por defecto, el análisis está establecido en el nivel **Recomendado**.

➔ *Para modificar el nivel de seguridad determinado:*

1. Abrir la ventana Principal de la Aplicación.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, ajustar el control deslizante en la escala. Al ajustar el nivel de seguridad, usted define el cociente de velocidad de análisis y la cantidad total de archivos analizados: cuanto menor es la cantidad archivos a analizar en busca de virus, mayor es la velocidad de análisis. También puede hacer click en el botón **Personalizar** y modificar los parámetros requeridos en la ventana que se abrirá. El nivel de seguridad cambiará a **Personalizado**.

CAMBIAR ACCIONES A REALIZAR SOBRE OBJETOS DETECTADOS

Si un análisis de virus identifica un objeto como infectado o sospechado de estarlo, el proceso posterior por la aplicación depende del estado del objeto y de la acción seleccionada.

En base a los resultados analizados, a un objeto se le puede asignar uno de los siguientes estados:

- el estado del programa nocivo (tales como *virus*, *Troyano*);
- el estado *potencialmente infectado* cuando el análisis no puede determinar si el objeto está infectado. Esto ocurre cuando la aplicación detecta en el archivo una secuencia de código de un virus desconocido, o el código modificado de un virus conocido.

Por defecto, todos los objetos infectados son sometidos a desinfección, y todos los objetos potencialmente infectados son colocados en cuarentena.

SI LA ACCIÓN SELECCIONADA ERA	CUANDO SE DETECTA UN OBJETO INFECTADO POTENCIALMENTE / NOCIVO
<input checked="" type="radio"/> Preguntar al usuario al completar el análisis	La aplicación postergará el procesamiento de objetos hasta la finalización del análisis. Al completar el análisis, emergerá la ventana de estadísticas con una lista de objetos detectados, y se le preguntará si desea procesar los objetos.
<input checked="" type="radio"/> Preguntar al usuario durante el análisis	La aplicación mostrará un mensaje de advertencia sobre el tipo de código nocivo que ha infectado al objeto, y ofrecerá varias opciones de acciones posteriores.
<input checked="" type="radio"/> No preguntar al usuario	La aplicación crea un informe con información acerca de los objetos detectados sin procesarlos ni notificar al usuario. Este modo de la aplicación no es el recomendado porque mantiene objetos infectados o potencialmente infectados en su equipo, haciendo que la infección sea virtualmente inevitable.
<input checked="" type="radio"/> No preguntar al usuario <input checked="" type="checkbox"/> Desinfectar	La aplicación intenta desinfectar el objeto sin solicitar ninguna confirmación del usuario. Si falla el intento de desinfectar el objeto, este será bloqueado (si el objeto no puede ser desinfectado), o se le asignará el estado de <i>potencialmente infectado</i> (si el objeto es considerado sospechoso) y será movido a Cuarentena. Información relevante registrada en el reporte. Ud. puede tratar de desinfectar el objeto después.
<input checked="" type="radio"/> No preguntar al usuario <input checked="" type="checkbox"/> Desinfectar <input checked="" type="checkbox"/> Eliminar si falla la desinfección	La aplicación intenta desinfectar el objeto sin solicitar ninguna confirmación del usuario. Si no es posible desinfectar el objeto, se lo eliminará.
<input checked="" type="radio"/> No preguntar al usuario <input type="checkbox"/> Desinfectar <input checked="" type="checkbox"/> Eliminar	La aplicación elimina el objeto automáticamente.

Antes de intentar desinfectar o eliminar un objeto infectado, Kaspersky Anti-Virus crea una copia de respaldo del objeto y la almacena en el Respaldo para permitir una posterior restauración o eliminación.

➡ Para modificar la acción especificada que se realizará en los objetos detectados, por favor haga lo siguiente:

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la sección **Acción**, ingrese los cambios requeridos en la ventana que se abrirá.

MODIFICAR EL TIPO DE OBJETOS A ANALIZAR

Cuando especifica el tipo de objetos a analizar, establece qué formatos de archivos y tamaños serán analizados en busca de virus cuando se ejecuta el análisis de virus seleccionado.

Recuerde esto cuando seleccione los tipos de archivos:

- Ciertos formatos de archivos (tales como *.txt*) apenas tienen un bajo riesgo de tener código nocivo infiltrado en ellos y posteriormente activado. A la vez existen formatos que contienen o pueden tener un código ejecutable (como *exe*, *dll*, *doc*). El riesgo de inyección y activación de códigos nocivos en estos archivos y su posterior activación, es bastante alto.
- Recuerde que un intruso puede enviar un virus a su equipo en un archivo con extensión *.txt* que en realidad sea un archivo ejecutable renombrado como un archivo *.txt*. Si Ud. selecciona la opción  **Analizar archivos por extensión**, el análisis ignorará estos archivos. Si la opción  **Analizar archivos por formato** ha sido seleccionada, la protección de archivos analizará el encabezado del archivo y podrá determinar que el mismo es un archivo *.exe*. Un archivo como ese sería minuciosamente analizado en busca de virus.

➡ *Para modificar el tipo de objetos analizados:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Alcance**, en la sección **Tipos de archivos**, seleccione los parámetros requeridos.

OPTIMIZACIÓN DEL ANÁLISIS

Usted puede acortar el tiempo de análisis y aumentar la velocidad de Kaspersky Anti-Virus. Esto se puede lograr analizando sólo los archivos nuevos y modificados desde el último análisis. Aplica tanto a archivos simples como compuestos.

Adicionalmente, usted puede imponer una restricción en la longitud del análisis. El análisis se detendrá al alcanzar el periodo de tiempo especificado. También puede limitar el tamaño del archivo que está siendo analizado. El archivo será omitido si su tamaño excede el valor que usted ha establecido.

➡ *Para analizar sólo los archivos nuevos y modificados, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Cobertura**, en la sección **Optimización del análisis**, active la casilla **Analizar solamente archivos nuevos y modificados**.

➡ *Para limitar el tiempo de la duración del análisis:*

1. Abrir la ventana Principal de la Aplicación.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Cobertura**, en la sección **Optimización del análisis**, active la casilla **Detener el análisis si tarda más de** e indique la duración del análisis en el campo provisto.

➤ *Para limitar el tamaño del archivo a analizar, por favor haga lo siguiente:*

1. Abrir la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Cobertura**, haga click en el botón **Adicional**.
6. En la ventana **Archivos compuestos** que se abrirá, active la casilla **No descomprimir archivos compuestos grandes** y especifique el tamaño del archivo en el campo contiguo.

ANÁLISIS DE ARCHIVOS COMPUESTOS

Un método habitual de esconder virus es insertarlos dentro de archivos compuestos: archivadores, bases de datos, etc. Para detectar virus escondidos con este método se debe descomprimir el archivo compuesto, lo cual puede disminuir considerablemente la velocidad de análisis.

Para cada tipo de archivo compuesto, puede seleccionar o analizar todos los archivos o sólo los más recientes. Para ello, use el enlace que se encuentra al lado del nombre del objeto. Cambia de valor cuando pulsa en él. Si selecciona analizar archivos nuevos y modificados sólo en modo análisis, no podrá seleccionar qué tipos de archivos compuestos serán analizados.

➤ *Para modificar la lista de archivos compuestos analizados:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Cobertura**, en la sección **Análisis de archivos compuestos**, seleccione el tipo requerido de archivos compuestos a analizar.

CAMBIAR MÉTODO DE ANÁLISIS

Usted puede utilizar el *análisis heurístico* como un método de análisis. Éste analiza las acciones que puede realizar un objeto en el sistema. Si estas acciones corresponden a las de los objetos nocivos, entonces es probable que se identifique al objeto como nocivo o sospechoso.

Adicionalmente, usted puede fijar el nivel de detalle para el análisis heurístico moviendo la barra deslizante hacia una de las siguientes posiciones: **superficial**, **medio**, o **avanzado**.

Además de este método de análisis, puede utilizar el Análisis Rootkit. *Rootkit* es un conjunto de herramientas que puede ocultar aplicaciones nocivas en su sistema operativo. Estas utilidades se infiltran en el sistema, ocultando su presencia y también la de procesos, carpetas y claves de registro de otros programas maliciosos instalados con el rootkit. Si el análisis está activado, puede especificar el nivel de detalle (análisis avanzado) para detectar rootkits. Éste buscará atentamente tales programas analizando un gran número de variados objetos.

➤ *Para especificar qué método de análisis utilizar:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.

3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Adicional**, en la sección **Métodos de Análisis**, seleccione las tecnologías de análisis requeridas.

TECNOLOGÍA DE ANÁLISIS

Adicionalmente, Ud. puede especificar la tecnología *iChecker* que se usará durante el análisis.

La **tecnología iChecker** excluye algunos objetos del análisis para incrementar la rapidez del análisis. Un objeto es excluido del análisis utilizando un algoritmo especial que toma en cuenta la fecha de lanzamiento de la base de datos de la aplicación, la fecha en que el objeto fue analizado por última vez, y cualquier modificación en los parámetros del análisis.

Por ejemplo, usted tiene un archivo que ha sido analizado por Kaspersky Anti-Virus y asignado el estado *no infectado*. La próxima vez la aplicación omitirá analizar este archivo a menos que haya sido modificado o que hayan sido modificados los parámetros de análisis. Si la estructura del archivo ha cambiado al agregarle un nuevo objeto, o si los parámetros de análisis han cambiado, o si las bases de datos de la aplicación han sido actualizadas, el archivo se volverá a analizar.

Existen limitaciones a la tecnología iChecker: no trabaja con archivos grandes y aplica sólo a los objetos con una estructura que la aplicación reconoce (por ejemplo, .exe, .dll, .lnk, .tff, .inf, .sys, .com, .chm, .zip, .rar).

► *Para analizar objetos utilizando la tecnología iChecker, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Adicional**, en la sección **Parámetros Adicionales**, active la casilla **Tecnología iChecker**.

EFICIENCIA DEL EQUIPO DURANTE LA EJECUCIÓN DE TAREAS

Las tareas de análisis antivirus pueden postergarse con el fin de limitar la carga en la unidad central del procesador (CPU) y en los subsistemas de almacenamiento.

La ejecución de tareas de análisis incrementa la carga en el CPU y en los subsistemas de disco, ralentizando otras aplicaciones. Por defecto, de darse esa situación, Kaspersky Anti-Virus pausará las tareas de análisis y liberará recursos del sistema para las aplicaciones del usuario.

Sin embargo, existe una cantidad de aplicaciones que se iniciarán tan pronto como se liberen recursos del CPU y se ejecutarán en segundo plano. Para que el análisis no dependa del rendimiento de esas aplicaciones, no deberían concederse recursos del sistema a las mismas.

Note que este parámetro puede ser configurado en forma individual para cada tarea de análisis de virus. En este caso, la configuración para una tarea específica tiene mayor prioridad.

► *Para posponer la ejecución de tareas de análisis si ralentizan otras aplicaciones, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.

2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Adicional**, en la sección **Métodos de análisis**, active la casilla **Conceder recursos a otras aplicaciones**.

MODO DE EJECUCIÓN: ESPECIFICAR UNA CUENTA

Ud. puede especificar una cuenta utilizada por la aplicación al realizar un análisis en busca de virus.

➤ *Para iniciar la tarea con los privilegios de una cuenta de usuario diferente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Nivel de Seguridad**, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Modo de ejecución**, en la sección **Usuario**, active la casilla **Ejecutar tarea como**. Especificar usuario y contraseña.

MODO DE EJECUCIÓN: CREAR HORARIO

Todas las tareas de análisis de virus pueden ser iniciadas en forma manual, o según un cronograma.

El ajuste predeterminado de la programación para las tareas creadas cuando el programa está instalado está desactivado. La excepción es la tarea de análisis rápido, que se ejecuta cada vez que inicia su equipo.

Cuando crea una programación en el lanzamiento de tareas, es necesario establecer el intervalo de los análisis.

Si no es posible iniciar la tarea por alguna razón (por ejemplo, el equipo no estaba encendido en el tiempo especificado), puede configurar la tarea para iniciar automáticamente tan pronto como sea posible.

➤ *Para editar una planificación de tareas de análisis:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, presione el botón **Modificar** en la sección **Modo de ejecución**.
5. Realizar los cambios requeridos en la ventana **Programación** que se abrirá.

➤ *Para configurar ejecuciones automáticas de tareas ignoradas:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.

4. En la ventana que se abrirá, presione el botón **Modificar** en la sección **Modo de ejecución**.
5. En la ventana **Programación** que se abrirá, en la sección **Programar parámetros**, active la casilla **Ejecutar tarea si es omitida**.

CARACTERÍSTICAS DE INICIO DE TAREAS PROGRAMADAS

Todas las tareas de análisis de virus pueden ser iniciadas en forma manual, o según un cronograma.

Las tareas planificadas poseen una funcionalidad adicional, por ejemplo, usted puede *suspender el análisis planificado cuando el protector de pantalla está inactivo o el equipo está desbloqueado*. Esta funcionalidad pospone el inicio de la tarea hasta que el usuario haya finalizado su trabajo con el equipo. Así, el análisis no utilizará recursos del sistema durante el trabajo.

➔ *Para iniciar tareas únicamente cuando el equipo ya no está en uso, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escaneo Completo, Escaneo Rápido**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, en la sección **Modo de ejecución**, active la casilla **Pausar el análisis programado cuando el protector de pantalla esté inactivo o el equipo no esté bloqueado**.

ESTADÍSTICAS DE ANÁLISIS DE VIRUS

La información general sobre cada tarea de análisis de virus se muestra en la ventana de estadísticas. Aquí podrá verificar cuántos objetos han sido analizados y cuántos objetos peligrosos o sospechosos sujetos de procesamiento han sido detectados. En forma adicional, aquí podrá encontrar información sobre el inicio y tiempo en que se completará la última ejecución de tareas y sobre la longitud del análisis.

La información general sobre los resultados del análisis se agrupa en las siguientes pestañas:

- La pestaña *Detectado* lista todos los objetos peligrosos cuando se ejecuta una tarea.
- La pestaña *Eventos* lista todos los eventos ocurridos cuando se ejecuta una tarea.
- La pestaña *Estadísticas* proporciona información estadística de los objetos analizados.
- La pestaña *Configuración* proporciona la configuración que determina el modo de ejecutar una tarea.

Si se ha producido un error durante el análisis, intente volver a ejecutarlo. Si el próximo intento devuelve un error, recomendamos que guarde el reporte en los resultados de las tareas en un archivo utilizando el botón **Guardar como**. Luego contacte al Servicio de Soporte Técnico, y envíe el archivo del reporte. Los especialistas de Kaspersky Lab lo ayudarán.

➔ *Para ver las estadísticas de una tarea de análisis de virus, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Escanear (Escaneo Completo, Escaneo Rápido)**, cree una tarea de análisis, y láncela. El progreso de la tarea se mostrará en la ventana principal. Haga click en el enlace **Detalles** para cambiar a la ventana de estadísticas.

ASIGNAR PARÁMETROS DE ANÁLISIS COMUNES PARA TODAS LAS TAREAS

Cada tarea de análisis se ejecuta de acuerdo con sus propios parámetros. Por defecto, las tareas creadas en la instalación de la aplicación se ejecutan con los parámetros recomendados por los expertos de Kaspersky Lab.

Usted puede configurar los parámetros de análisis universales para todas las tareas. Utilizará un grupo de propiedades para analizar un objeto individual en busca de virus en el punto de inicio.

➤ *Para asignar parámetros de análisis universal a todas las tareas, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Analizar**.
3. En la parte derecha de la ventana, en la sección **Otros parámetros de tareas**, haga click en el botón **Aplicar**. Confirmar los parámetros universales que ha seleccionado en la casilla de diálogo emergente.

RESTAURAR PARÁMETROS DE ANÁLISIS POR DEFECTO

Cuando edita los parámetros para tareas, siempre puede restaurarlos a los recomendados. Son considerados óptimos, recomendados por Kaspersky Lab, y agrupados en el nivel de seguridad **Recomendado**.

➤ *Para restaurar los parámetros de análisis del archivo predeterminado, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, elija la sección **Escanear (Escaneo Completo, Escaneo Rápido)**.
3. Para la sección seleccionada, haga click en el enlace con el nivel de seguridad preestablecido.
4. En la ventana que se abrirá, presione el botón **Nivel Predeterminado** en la sección **Nivel de Seguridad**.

ACTUALIZACIÓN DE KASPERSKY ANTI-VIRUS

Diariamente se crean en todo el mundo nuevos virus, troyanos, y otros programas nocivos; por lo tanto, es extremadamente importante asegurarse de utilizar la última versión de la base de datos de la aplicación.

La actualización de la aplicación se descarga e instala en su equipo:

- **Bases de datos de Aplicaciones**

La protección de la información se basa en bases de datos que contienen firmas de amenazas. A las bases de datos se les agrega cada hora los registros de nuevas amenazas y métodos utilizados para combatirlos. Por esta razón, le recomendamos actualizarlas con regularidad.

- **Módulos de la aplicación**

Además de las bases de datos de la aplicación, puede actualizar los módulos de la aplicación. Los paquetes de actualización reparan las vulnerabilidades de la aplicación y agregan nuevas funcionalidades o mejoran las existentes.

Los servidores de actualización de Kaspersky Lab son las fuentes primarias de actualizaciones de Kaspersky Anti-Virus.

Para la descarga exitosa de actualizaciones desde los servidores, su equipo debe estar conectado a Internet. Por defecto, los parámetros de la conexión a Internet se determinan de manera automática. Si la configuración del servidor proxy no está configurada apropiadamente, los parámetros de conexión pueden establecerse manualmente.

Durante una actualización, los módulos de aplicación y bases de datos en su equipo se comparan con aquellos en la fuente de actualización. Si su equipo cuenta con la última versión de las bases de datos y los módulos de la aplicación, aparecerá una ventana de notificación confirmando que su equipo está actualizado. Si las bases de datos y los módulos en su equipo no coinciden con los del servidor de actualización, la aplicación descargará sólo la parte incremental de las actualizaciones. El hecho de que no todas las bases de datos o los módulos se descarguen, aumenta de forma significativa la velocidad del copiado de archivos y reduce el tráfico Internet.

Antes de actualizar las bases de datos, Kaspersky Anti-Virus crea copias de respaldo de ellas, para que pueda volver a utilizarlas en el futuro.

Usted podría necesitar la opción de reversión si, por ejemplo, las bases de datos se han vuelto corruptas durante el proceso de actualización. Es fácil revertir a las bases de datos previas e intentar la actualización después.

Usted puede copiar las actualizaciones recuperadas a una fuente local mientras actualiza la aplicación. Este servicio permite la actualización de las bases de datos y módulos de la aplicación en equipos en red para ahorrar el tráfico de Internet.

También puede configurar el inicio automático de actualización.

La sección de **Actualización** muestra el estado actual de las bases de datos de la aplicación.

Puede ver el reporte de actualización, que contiene información completa de todos los eventos ocurridos durante la actualización. También puede ver la información general sobre la actividad viral en www.kaspersky.com haciendo click en el enlace **Información sobre la actividad viral**.

► *Para editar los parámetros de toda tarea de actualización, por favor haga lo siguiente:*

1. Abra la ventana principal de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.

4. En la ventana que se abrirá, realice los cambios necesarios en los parámetros de la tarea que ha seleccionado.

➤ *Para cambiar al reporte de actualización, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Haga click en el botón **Reportes**.

EN ESTA SECCIÓN

Comenzar la actualización	47
Reversión a la última actualización	48
Selección del origen de actualización.....	48
Configuración regional.....	49
Utilizar el servidor proxy.	49
Modo de ejecución: especificar una cuenta.....	50
Modo de ejecución: crear horario	50
Cambiar modo de ejecución de la tarea de actualización	51
Seleccionar objetos para actualizar.....	51
Actualizar desde una carpeta local.....	52
Estadísticas de actualización	53
Posibles problemas durante la actualización.....	53

COMENZAR LA ACTUALIZACIÓN

Usted puede iniciar la actualización de la aplicación en cualquier momento. Las actualizaciones se descargan de la fuente de actualización seleccionada.

Puede actualizar Kaspersky Anti-Virus utilizando uno de los dos métodos soportados:

- En el menú contextual.
- En la ventana principal de la aplicación.

Actualizar información se mostrará en la ventana principal de la aplicación.

Note que las actualizaciones son distribuidas a una fuente local durante el proceso de actualización, siempre que este servicio esté habilitado.

➤ *Para iniciar la actualización de Kaspersky Anti-Virus desde el menú contextual:*

1. Pulse con el botón derecho el ícono de la aplicación en el área de notificaciones de la barra de tareas.
2. Seleccione el ítem **Actualizar** del menú desplegable.

➤ *Para iniciar la actualización de Kaspersky Anti-Virus desde la ventana principal de la aplicación:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Pulse el botón **Iniciar la actualización**. El progreso de ejecución de la tarea se mostrará en la ventana principal de la aplicación.

REVERSIÓN A LA ÚLTIMA ACTUALIZACIÓN

Al iniciar el proceso de actualización, Kaspersky Anti-Virus crea una copia de resguardo de la actual base de datos y de los módulos de las aplicaciones. Esto permite que la aplicación continúe funcionando, usando las bases de datos anteriores, si la actualización falla.

La opción de reversión puede resultar muy útil si, por ejemplo, se daña una parte de las bases de datos. Las bases de datos locales pueden estar corruptas por el usuario o por un programa nocivo, que sólo es posible si está desactivada la auto-defensa de la aplicación. Es fácil revertir a las bases de datos previas e intentar la actualización después.

➤ *Para revertir a la versión previa de las bases de datos:*

1. Abra la ventana principal de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Haga click en el enlace **Revertir a las bases de datos anteriores**.

SELECCIÓN DEL ORIGEN DE ACTUALIZACIÓN

La *fente de actualización* es un recurso que contiene actualizaciones para bases de datos y módulos de aplicaciones de Kaspersky Anti-Virus.

Puede utilizar los siguientes orígenes de actualización:

- *Servidor de Administración* es un repositorio de actualización centralizado ubicado en el Servidor de administración de Kaspersky Administration Kit (para más detalles vea la Guía del Administrador de Kaspersky Administration Kit).
- *Servidores de actualización de Kaspersky Lab* son sitios web especiales que contienen actualizaciones para las bases de datos y módulos de la aplicación para todos los productos de Kaspersky Lab.
- *Servidores FTP o HTTP, carpetas locales o de red* son servidores locales o carpetas que contienen las últimas actualizaciones.

Si no tiene acceso a los servidores de actualización de Kaspersky Lab (por ejemplo, su equipo no está conectado a Internet), puede llamar a la casa central de Kaspersky Lab al +7 (495) 797-87-00 o +7 (495) 645-79-39 para solicitar información de contacto de asociados a Kaspersky Lab que puedan proveerle actualizaciones en disquetes o discos ZIP.

Puede copiar las actualizaciones de un disco removible y cargarlas en un sitio web FTP o HTTP, o guardarlas en una carpeta local o de red.

Al solicitar las actualizaciones en un medio removible, por favor especifique si también desea tener las actualizaciones para los módulos de la aplicación.

Debe disponer de una conexión a Internet si selecciona un recurso ubicado fuera de la red local como el origen de la actualización.

Si varios recursos son seleccionados como orígenes de actualización, la aplicación intentará conectarse a ellos por turno, comenzando con el primero de la lista y recolectando las actualizaciones del primer origen disponible.

➤ *Para elegir un origen de actualización:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, en la sección **Parámetros de actualización**, haga click en el botón **Configuración**.
5. En la ventana que se abrirá, en la pestaña **Origen de actualización**, haga click en el botón **Agregar**.
6. Seleccione un sitio FTP o HTTP, o ingrese su dirección IP, el nombre simbólico, o dirección URL en la ventana **Seleccionar origen de actualización** que se abrirá.

CONFIGURACIÓN REGIONAL

Si como fuente de actualización utiliza los servidores de Kaspersky Lab, puede seleccionar la ubicación del servidor al descargar las actualizaciones. Kaspersky Lab tiene servidores en varios países. Si escoge el servidor de actualización de Kaspersky Lab más cercano a Ud., ahorrará tiempo y las descargas de actualizaciones serán más rápidas.

➤ *Para seleccionar el servidor más cercano:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, en la sección **Parámetros de actualización**, haga click en el botón **Configuración**.
5. En la ventana que se abrirá, en la pestaña **Actualizar origen**, en la sección **Configuración regional**, seleccione la opción  **Seleccionar de la lista** y luego seleccione el país más cercano a su ubicación actual de la lista desplegable.

Si selecciona la opción  **Autodetectar**, la información de su ubicación se copiará de su registro del sistema operativo al actualizar.

UTILIZAR EL SERVIDOR PROXY

Si se conecta a Internet mediante un servidor proxy, también debe configurar sus parámetros.

➤ *Para configurar el servidor proxy, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, en la sección **Parámetros de actualización**, haga click en el botón **Configuración**.
5. En la ventana que se abrirá, editar los parámetros del servidor proxy en la pestaña **Parámetros proxy**.

MODO DE EJECUCIÓN: ESPECIFICAR UNA CUENTA

Kaspersky Anti-Virus cuenta con una función que inicia actualizaciones del programa desde otro perfil. Por defecto, este servicio se encuentra deshabilitado, y las tareas se inician usando la cuenta registrada en el sistema.

Debido a que la aplicación puede ser actualizada de una fuente a la cual usted no tiene acceso (como el directorio de actualizaciones de la red) o derechos de usuario autorizado al servidor proxy, puede utilizar esta característica para ejecutar las actualizaciones de la aplicación usando el inicio de sesión de un usuario que tenga tales privilegios.

Note que si no ejecuta la tarea con privilegios, la actualización programada se ejecutará con los privilegios de la cuenta del usuario actual. Si no hay usuarios registrados actualmente en el equipo, la ejecución de actualizaciones bajo otra cuenta de usuario no está configurada, y las actualizaciones se ejecutan automáticamente, se ejecutarán con los privilegios del SISTEMA.

➔ *Para iniciar la tarea con los privilegios de una cuenta de usuario diferente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, en la sección **Parámetros de actualización**, haga click en el botón **Configuración**.
5. En la ventana que se abrirá, en la pestaña **Adicional**, en la sección **Modo de ejecución**, active la casilla **Ejecutar tarea como**. A continuación ingrese los datos para la sesión que desea iniciar la tarea: nombre de usuario y contraseña.

MODO DE EJECUCIÓN: CREAR HORARIO

Todas las tareas de análisis de virus pueden ser iniciadas en forma manual, o según un cronograma.

Cuando crea una programación en el lanzamiento de tareas, es necesario establecer el intervalo de las tareas de actualización.

Si no es posible iniciar la tarea por alguna razón (por ejemplo, el equipo no estaba encendido en el tiempo especificado), puede configurar la tarea para iniciar automáticamente tan pronto como sea posible.

➔ *Para editar una planificación de tareas de análisis:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, presione el botón **Modificar** en la sección **Modo de ejecución**.
5. Realizar los cambios requeridos en la ventana **Programación** que se abrirá.

➔ *Para configurar ejecuciones automáticas de tareas ignoradas:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.

3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, presione el botón **Modificar** en la sección **Modo de ejecución**.
5. En la ventana **Programación** que se abrirá, en la sección **Programar parámetros**, active la casilla **Ejecutar tarea si es omitida**.

CAMBIAR MODO DE EJECUCIÓN DE LA TAREA DE ACTUALIZACIÓN

El modo de inicio de la tarea de actualización de Kaspersky Anti-Virus se selecciona en el Asistente de Configuración de la Aplicación. Puede cambiar el modo de ejecución que ha seleccionado.

La tarea de actualización puede iniciarse mediante uno de los siguientes modos:

-  **Automático**. Kaspersky Anti-Virus verifica la fuente de actualización para paquetes de actualización a intervalos especificados. Si se encuentran nuevas actualizaciones, Kaspersky Anti-Virus las descarga e instala en su equipo. Este es el modo por defecto.

Kaspersky Anti-Virus intentará realizar actualizaciones en intervalos especificados en el paquete de actualización anterior. Esta opción permite que Kaspersky Lab regule la frecuencia de actualización en caso de brotes de virus y otras situaciones potencialmente peligrosas. Su aplicación recibirá las últimas actualizaciones para las bases de datos, ataques de red, y módulos de software de manera oportuna, excluyendo la posibilidad de que el malware penetre su equipo.

-  **Según planificación** (cambios en el intervalo de tiempo que dependen de los parámetros). Las actualizaciones se ejecutan de manera automática según el horario creado.
-  **Manual**. Si selecciona esta opción, Ud. ejecutará las actualizaciones de la aplicación por su cuenta. Kaspersky Anti-Virus lo notificará cuando se requieran actualizaciones sin falla.

➔ *Para configurar el horario de inicio de la tarea de actualización:*

1. Abra la ventana principal de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, seleccione el modo de lanzamiento de la tarea de actualización en la sección **Modo de ejecución**. Si se selecciona la opción de la actualización programada, crear el cronograma.

SELECCIONAR OBJETOS PARA ACTUALIZAR

Objetos para actualizar son los componentes que serán actualizados:

- bases de datos de aplicaciones;
- módulos de la aplicación.

Las bases de datos de la aplicación son actualizadas siempre, mientras que los módulos de la aplicación sólo son actualizados si es seleccionado el modo adecuado.

Si al instalar hay un grupo de módulos de la aplicación en la fuente de actualización, Kaspersky Anti-Virus lo descargará y lo instalará cuando se reinicie el equipo. Las actualizaciones de los módulos descargadas no serán instaladas hasta que el equipo sea reiniciado.

Si la próxima actualización de la aplicación ocurriese antes de que el equipo sea reiniciado y por consiguiente antes de que las actualizaciones de los módulos de la aplicación descargados anteriormente sean instalados, sólo se actualizarán las firmas de amenazas.

➤ *Si desea descargar e instalar actualizaciones para módulos de aplicaciones, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, en la sección **Parámetros de actualización**, active la casilla **Actualizar módulos de la aplicación**.

ACTUALIZAR DESDE UNA CARPETA LOCAL

El procedimiento para la recuperación de actualizaciones desde carpetas locales es como sigue:

1. Uno de los equipos de la red obtiene el paquete de actualización de Kaspersky Anti-Virus del servidor de Kaspersky Lab, o de un servidor espejo que contiene el conjunto actual de actualizaciones. Las actualizaciones recuperadas se ubican en la Carpeta compartida.
2. Otros equipos de la red acceden a la carpeta compartida para recolectar las actualizaciones.

Kaspersky Anti-Virus 6.0 sólo recupera sus paquetes de actualización de servidores de Kaspersky Lab. Recomendamos distribuir actualizaciones de otras aplicaciones de Kaspersky Lab a través de Kaspersky Administration Kit.

➤ *Para permitir actualizar el módulo de distribución, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Adicional**, en la sección **Actualizar distribución**, active la casilla **Copiar actualizaciones a la carpeta** y en el campo de abajo especifique la ruta a una carpeta pública en la cual se copiarán las actualizaciones descargadas. Asimismo, puede seleccionar la ruta en la ventana que se abrirá al hacer click en el botón **Examinar**.

➤ *Si desea que las actualizaciones de la aplicación se realicen de la carpeta compartida seleccionada, por favor haga lo siguiente en todos los equipos de la red:*

1. Abra la ventana principal.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Para la sección seleccionada, haga click en el enlace con el modo de ejecución preestablecido.
4. En la ventana que se abrirá, haga click en el botón **Personalizar**.
5. En la ventana que se abrirá, en la pestaña **Origen de actualización**, haga click en el botón **Agregar**.
6. En la ventana **Seleccionar origen de actualización** que se abrirá, seleccione una carpeta o ingrese la ruta completa en el campo **Origen**.

7. Desactive la casilla **Servidores de actualización de Kaspersky Lab** en la pestaña **Origen de actualización**.

ESTADÍSTICAS DE ACTUALIZACIÓN

Encontrará información general sobre tareas de actualización en la ventana estadísticas. En esta ventana, también puede ver los eventos ocurridos al ejecutar una tarea (la pestaña *Eventos*) y ver la lista de parámetros que determinan la ejecución de la tarea (la pestaña *Parámetros*).

Si se ha producido un error durante el análisis, intente volver a ejecutarlo. Si el próximo intento devuelve un error, recomendamos que guarde el reporte en los resultados de las tareas en un archivo utilizando el botón **Guardar como**. Luego contacte al Servicio de Soporte Técnico, y envíe el archivo del reporte. Los especialistas de Kaspersky Lab lo ayudarán.

Las breves estadísticas de actualización se muestran en la parte superior de la ventana de estadísticas. Incluye el tamaño de las actualizaciones descargadas e instaladas, la velocidad y duración actualizadas, y otra información.

➔ *Para ver las estadísticas de una tarea de análisis de virus, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**, crear una tarea de actualización, y lanzarla. El progreso de la tarea se mostrará en la ventana principal. Puede cambiar la ventana de estadísticas haciendo click en el enlace **Detalles**.

POSIBLES PROBLEMAS DURANTE LA ACTUALIZACIÓN

Cuando actualiza los módulos de la aplicación de Kaspersky Anti-Virus o las firmas de amenazas, pueden ocurrir errores, que se asocian con la configuración incorrecta de la actualización, problemas de conexión, etc. Esta sección de Ayuda cubre la mayor parte de los errores y brinda consejos para eliminarlos. Si encuentra errores que no están cubiertos en la Ayuda o desea recomendaciones detalladas para eliminarlos, trate de encontrar información en la Base de Conocimiento en el portal del Soporte Técnico en la sección "Si un programa generó un error...". Si las recomendaciones brindadas en esta sección no fueron útiles para solucionar el problema o si no hay información sobre el error en la Base de Conocimiento, envíe una solicitud al Equipo de Soporte Técnico.

ERRORES DE CONFIGURACIÓN

Los errores de este grupo ocurren en gran parte debido a una instalación incorrecta de la aplicación, o debido a modificaciones de la configuración de la aplicación, que resultaron en una pérdida de funcionalidad.

Recomendaciones generales:

Si se generaron errores en este grupo, recomendamos reiniciar las actualizaciones. Si el error persiste, contacte al Soporte Técnico.

Si el problema está conectado con la aplicación que ha sido instalada en forma incorrecta, recomendamos reinstalarla.

Ninguna fuente de actualización especificada

Ninguna de las fuentes contiene archivos de actualización. Es posible que no se haya especificado una fuente de actualización en los parámetros de actualización. Por favor asegúrese que los parámetros de actualización estén correctamente configurados y vuelva a intentarlo.

Error al verificar la licencia

Este error es generado si la llave de licencia utilizada por la aplicación está bloqueada y colocada en la lista negra de licencia.

Error al recuperar los parámetros de actualización

Error interno al recuperar los parámetros de la tarea de actualización. Por favor asegúrese que los parámetros de actualización estén correctamente configurados y vuelva a intentarlo.

<p><i>Privilegios insuficientes para actualizar</i></p> <p>Este error ocurre generalmente cuando la cuenta de usuario utilizada para iniciar la actualización, no tiene privilegios de acceso a la fuente de actualización. Recomendamos asegurarse que la cuenta de usuario tenga los privilegios necesarios.</p> <p>Este error también podría generarse cuando el intento de copiar los archivos de actualización a una carpeta que no puede ser creada.</p>
<p><i>Error interno</i></p> <p>Error lógico interno en la tarea de actualización. Por favor asegúrese que los parámetros de actualización estén correctamente configurados y vuelva a intentarlo.</p>
<p><i>Error al verificar actualizaciones</i></p> <p>Este error es generado si los archivos descargados de la fuente de actualización no pasan la verificación interna. Por favor intente actualizar más tarde.</p>
<p>ERRORES QUE OCURREN CUANDO SE TRABAJA CON ARCHIVOS Y CARPETAS</p> <p>Este tipo de error ocurre cuando la cuenta de usuario que está siendo utilizada para ejecutar las actualizaciones tiene derechos restringidos o no tiene derechos para acceder a la fuente de actualización o la carpeta donde están ubicadas las actualizaciones.</p> <p><u>Recomendaciones generales:</u></p> <p>Si ocurren errores de este tipo, recomendamos verificar que la cuenta de usuario tenga los derechos de acceso suficiente para aquellos archivos o carpetas.</p>
<p><i>No puede crear carpeta</i></p> <p>Este error se genera si una carpeta no puede ser creada durante el proceso de actualización.</p>
<p><i>Privilegios insuficientes para ejecutar la operación de archivo</i></p> <p>Este error ocurre si la cuenta de usuario utilizada para ejecutar la actualización no tiene los privilegios suficientes para ejecutar operaciones con los archivos.</p>
<p><i>Archivo o carpeta no encontrada</i></p> <p>Este error ocurre si falta un archivo o carpeta necesarios en actualizaciones. Recomendamos verificar que el archivo o carpeta especificados existe y está disponible.</p>
<p><i>Error de operación del archivo</i></p> <p>Este error es un error lógico interno del módulo de actualización cuando se ejecutan operaciones con archivos.</p>
<p>ERRORES DE RED</p> <p>Los errores de este grupo ocurren cuando hay problemas de conexión o cuando la conexión a la red no está configurada correctamente.</p> <p><u>Recomendaciones generales:</u></p> <p>Si ocurren errores en este grupo, recomendamos asegurarse que su equipo esté conectado a Internet, los parámetros de conexión estén correctamente configurados, y la fuente de actualización esté disponible. Luengo vuelva a intentar la actualización. Si el problema persiste, contacte al Soporte Técnico.</p>
<p><i>Error de red</i></p> <p>Se generó un error al recuperar archivos de actualización. Si encuentra este error, verifique su conexión de red al equipo.</p>
<p><i>Conexión interrumpida</i></p> <p>Este error ocurre cuando la conexión con la fuente de actualización esté terminada por alguna razón por el servidor de actualización.</p>

<p><i>Tiempo de espera de la operación de red</i></p> <p>Tiempo de espera de la conexión de la fuente de actualización. Al configurar los parámetros de actualización del programa, puede haber establecido un valor de tiempo de espera para la conexión con la fuente de actualización. Si su equipo no se puede conectar al servidor o a la carpeta actualizada dentro de ese tiempo, el programa devuelve este error. En ese caso, recomendamos verificar que los parámetros para el Actualizador sean correctos y que la fuente de actualización esté disponible.</p>
<p><i>Error de autorización en el servidor FTP</i></p> <p>Este error ocurre si los parámetros de autorización para el servidor FTP utilizado como la fuente de actualización están ingresados en forma incorrecta. Por favor asegúrese que los parámetros reales del servidor FTP permiten este tipo de cuenta de usuario para descargar archivos.</p>
<p><i>Error de autorización en el servidor proxy</i></p> <p>Este error se genera si los parámetros para actualización a través de un servidor proxy indican en forma incorrecta el nombre y contraseña, o si la cuenta de usuario bajo la cual se ejecutan las actualizaciones no tiene privilegios de acceso a la fuente de actualización. Por favor, editar los parámetros de autorización y vuelva a intentar la actualización.</p>
<p><i>Error al resolver el nombre DNS</i></p> <p>Este error se genera si no se detecta la fuente de actualización. Es posible que la dirección de la fuente de actualización esté indicada en forma incorrecta, los parámetros de red sean incorrectos, o el servidor DNS no esté disponible. Recomendamos verificar sus parámetros de actualización y disponibilidad de fuentes de actualización, luego vuelva a intentar.</p>
<p><i>No se pudo establecer la conexión a la fuente de actualización</i></p> <p>Este error ocurre si no hay conexión con la fuente de actualización. Por favor asegúrese que los parámetros de la fuente de actualización estén correctamente configurados y vuelva a intentarlo.</p>
<p><i>No se pudo establecer la conexión al servidor proxy</i></p> <p>Este error se genera si los parámetros de las conexiones del servidor proxy están indicados en forma incorrecta. Para solucionar el problema, recomendamos asegurarse que estén correctamente configuradas, el servidor de proxy esté disponible, y que Internet esté disponible, y trate de volver a actualizar.</p>
<p><i>Error al resolver el nombre DNS del servidor proxy</i></p> <p>Este error se genera si no se detecta el servidor proxy. Recomendamos asegurarse que los parámetros del servidor proxy sean correctos y que el servidor DNS esté disponible.</p>
<p>ERRORES RELACIONADOS CON BASES DE DATOS CORRUPTAS</p> <p>Estos errores están relacionados con archivos corruptos en la fuente de actualización.</p> <p><u>Recomendaciones generales:</u></p> <p>Si está actualizando desde servidores web de Kaspersky Lab, intente volver a actualizarlos. Si el problema persiste, contacte al Soporte Técnico.</p> <p>Si está actualizando desde una fuente diferente, como una carpeta local, recomendamos actualizarla desde los servidores web de Kaspersky Lab. Si vuelve a ocurrir el error, contacte al Soporte Técnico de Kaspersky Lab.</p>
<p><i>El archivo no está en la fuente de actualización</i></p> <p>Todos los archivos descargados e instalados en su equipo durante el proceso de actualización están listados en un archivo especial incluido en la actualización. Este error ocurre si hay archivos en la lista de actualización que no están en la fuente de actualización.</p>
<p><i>Error al verificar la firma</i></p> <p>Este error puede ser devuelto por la aplicación si la firma digital electrónica del paquete de actualización que está siendo descargado es corrupta o no concuerda con la firma de Kaspersky Lab.</p>
<p><i>Archivo índice corrupto o faltante</i></p> <p>Este error se genera si falta de la fuente de actualización el archivo índice de formato .xml que es utilizado para actualizar o si está corrupto.</p>

<p>ERRORES RELACIONADOS CON LA ACTUALIZACIÓN QUE UTILIZAN EL SERVIDOR DE ADMINISTRACIÓN DE KASPERSKY ADMINISTRATION KIT</p> <p>Estos errores se generan en relación con problemas para actualizar la aplicación a través del Servidor de Administración Kaspersky Administration Kit.</p> <p><u>Recomendaciones generales:</u></p> <p>Primero, asegúrese de que Kaspersky Administration Kit y sus componentes (Servidor de Administración y Agente de Red) estén instalados y ejecutándose. Intente volver a actualizar. Si esto falla, reinicie el Agente de Red y el Servidor de Administración, luego intente volver a actualizar. Si esto no resuelve la cuestión, contacte al Soporte Técnico.</p>
<p><i>Error al conectar al Servidor de Administración</i></p> <p>Este error se genera si el Servidor de Administración de Kaspersky Administration Kit no puede ser conectado. Recomendamos que se asegure que el AgenteR esté instalado y ejecutándose.</p>
<p><i>Error de registro en AgenteR</i></p> <p>Si ocurre este error, siga las recomendaciones generales para solucionar este tipo de errores. Si vuelve a ocurrir este error, envíe el archivo de reporte detallado para la actualización y el Agente de Red en ese equipo al Servicio de Soporte Técnico utilizando el formulario en línea. Describa la situación en detalle.</p>
<p><i>No se puede establecer la conexión. El Servidor de Administración está ocupado y no puede procesar el pedido</i></p> <p>En este caso, se deberá intentar la actualización más tarde.</p>
<p><i>No se puede establecer la conexión con el Servidor de Administración / Servidor de Administración Principal / AgenteR, error físico / error desconocido</i></p> <p>Si encuentra estos errores, recomendamos que vuelva a intentarlo más tarde. Si el problema persiste, contacte al Soporte Técnico.</p>
<p><i>Error al recuperar el archivo del Servidor de Administración, argumento de transporte inválido</i></p> <p>Si el error persiste, contacte al Soporte Técnico.</p>
<p><i>Error al recuperar el archivo del Servidor de Administración</i></p> <p>Si encuentra estos errores, recomendamos que vuelva a intentarlo más tarde. Si el problema persiste, contacte al Soporte Técnico.</p>
<p>CÓDIGOS VARIOS</p> <p>Este grupo incluye errores que no pueden ser incluidos en ninguno de los grupos listados anteriormente.</p>
<p><i>Archivos para operación de reversión faltantes</i></p> <p>Este error se genera si se ha hecho otro intento de reversión luego de completar la reversión de actualizaciones, pero no se han realizado actualizaciones entre ellos. El procedimiento de reversión no puede repetirse hasta que se realice una actualización exitosa que restaure un grupo de archivos de resguardo.</p>

CONFIGURAR LOS PARÁMETROS DE LA APLICACIÓN

La ventana de los parámetros de la aplicación se utiliza para un acceso rápido a los parámetros principales de Kaspersky Anti-Virus 6.0.

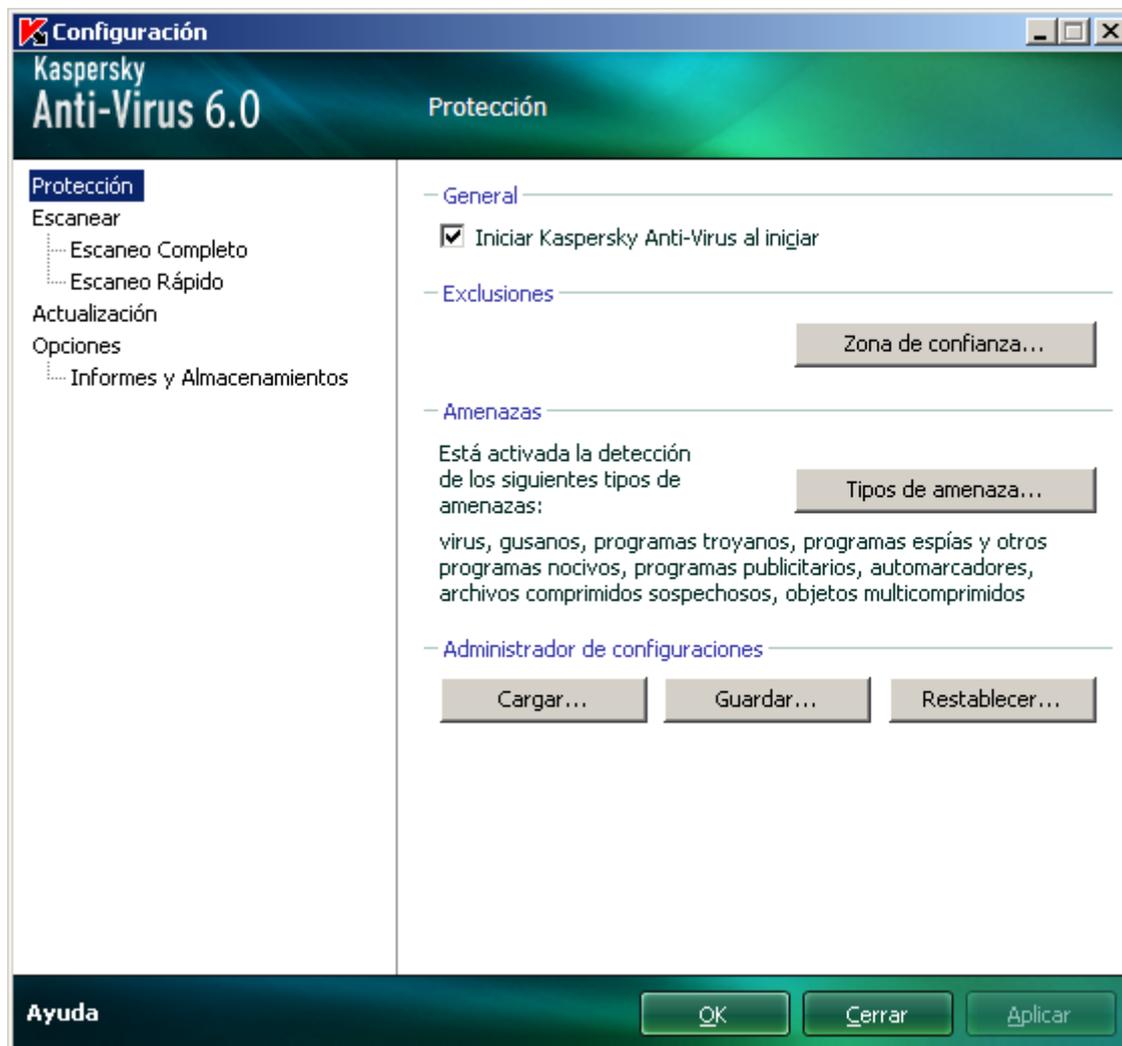


Figura 9. Ventana de configuración de parámetros de la aplicación

La ventana está compuesta por dos partes:

- la parte izquierda de la ventana le brinda acceso a los componentes de Kaspersky Anti-Virus, tareas de análisis de virus, tareas de actualización, etc.;
- la parte derecha de la ventana contiene una lista de parámetros para la tarea, etc., seleccionada en la parte izquierda de la ventana.

Puede abrir esta ventana:

- En la ventana principal de la aplicación. Para hacerlo, haga click en el botón **Configuración** en la parte superior de la ventana principal.

- En el menú contextual. Para ello, seleccione el ítem **Configuración** en el menú contextual de la aplicación.



Figura 10. Menú contextual

EN ESTA SECCIÓN

Protección	58
Análisis	63
Actualización	64
Configuración	64
Reportes y Almacenamientos.....	68

PROTECCIÓN

En la ventana **Protección** puede utilizar las siguientes funciones avanzadas de Kaspersky Anti-Virus:

- Lanzar la aplicación en el inicio del sistema operativo de la aplicación (ver página [58](#)).
- Seleccionar las categorías de amenazas detectables (ver página [59](#)).
- Crear una zona de confianza (ver página [59](#)):
 - crear una regla de exclusión (ver página [60](#));
 - exportar / importar componentes de la regla de exclusión (ver página [62](#)).
- Exportar / importar los parámetros de la aplicación (ver página [62](#)).
- Restaurar los parámetros predeterminados de la aplicación (ver página [63](#)).

LANZAR LA APLICACIÓN EN EL INICIO DEL SISTEMA OPERATIVO DE LA APLICACIÓN

Si debe cerrar completamente Kaspersky Anti-Virus por alguna razón, seleccione el elemento **Salir** del menú contextual de la aplicación. Luego la aplicación será descartada de la RAM. Eso significa que el equipo se ejecutará sin protección.

Usted puede activar la protección de su equipo iniciando la aplicación desde el menú **Inicio** → **Programas** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**.

También puede reanudar automáticamente la protección reiniciando su sistema operativo.

➤ Para activar el modo de lanzamiento de la aplicación en el inicio del sistema operativo, por favor haga lo siguiente:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. Active la casilla **Lanzar Kaspersky Anti-Virus en el inicio**.

SELECCIÓN DE LAS CATEGORÍAS DE AMENAZAS DETECTABLES

Kaspersky Anti-Virus lo protege contra varios tipos de programas maliciosos. Sin importar los parámetros seleccionados, la aplicación siempre analizará y desinfectará los virus y Troyanos. Estos programas pueden causar daños importantes a su equipo. Para brindarle mayor seguridad a su equipo, Ud. puede agrandar la lista de amenazas a detectar, activando el control de varios programas potencialmente peligrosos.

➤ Para seleccionar las categorías de amenazas detectables, por favor haga lo siguiente:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Amenazas**, haga click en el botón **Tipos de amenazas**.
4. En la ventana **Tipos de amenazas** que se abrirá, active las casillas para las categorías de amenazas que desea proteger de su equipo.

CREAR UNA ZONA DE CONFIANZA

Zona de confianza es una lista de objetos creada por el usuario que no es controlada por Kaspersky Anti-Virus. En otras palabras, es un conjunto de exclusiones del alcance de la protección de la aplicación.

El usuario crea una zona de confianza en base a las características de los objetos con los que trabaja, y a las aplicaciones instaladas en el equipo del usuario. Puede necesitar crear esa lista de exclusión si, por ejemplo, Kaspersky Anti-Virus bloquea el acceso a un objeto o a una aplicación que usted está seguro que es absolutamente segura.

Usted puede excluir del análisis archivos de ciertos formatos, utilizar una máscara de archivo, o excluir cierta área (por ejemplo, una carpeta o una aplicación), procesos de programas, u objetos de acuerdo con la clasificación de la Enciclopedia del Virus (estado asignado por Kaspersky Anti-Virus a objetos durante el análisis).

Un objeto de exclusión se excluye del análisis cuando se analiza el disco o la carpeta donde está ubicado. Sin embargo, si selecciona ese objeto específicamente, la regla de exclusión no se aplicará.

➤ Para crear la lista de exclusiones del análisis, por favor haga lo siguiente:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Exclusiones**, haga click en el botón **Zona de confianza**.
4. En la ventana que se abrirá, configure las reglas de exclusión para objetos (ver página [60](#)).

VER TAMBIÉN:

Crear una regla de exclusión.....	60
Máscaras aceptadas para exclusión de archivos	61
Máscaras de exclusión permitidas de acuerdo con la Enciclopedia de Virus.....	62
Exportar / importar reglas de exclusión	62

CREAR UNA REGLA DE EXCLUSIÓN

Reglas de exclusión son conjuntos de condiciones que Kaspersky Anti-Virus utiliza para verificar si puede ignorar el análisis de un objeto.

Puede excluir del análisis los archivos de ciertos formatos, utilizar una máscara de archivo, o excluir cierta área (por ejemplo, una carpeta o una aplicación), procesos de programa, u objetos de acuerdo con la clasificación de la Enciclopedia de Virus.

Tipo de amenaza es el estado que Kaspersky Anti-Virus asigna a un objeto mientras es analizado. Este estado es asignado en base a la clasificación de malware y riskware encontrado en la Enciclopedia de Virus de Kaspersky Lab.

El software potencialmente peligroso no tiene funciones nocivas pero puede ser utilizado como un componente auxiliar para un código nocivo, ya que contiene agujeros y errores. Esta categoría incluye, por ejemplo, aplicaciones de administración remota, clientes IRC, servidores FTP, utilidades multi-propósito para detener u ocultar procesos, registradores de pulsaciones de teclado (keyloggers), macros de contraseñas, automarcadores, etc. Ese software se clasifica como no-es-virus, pero puede dividirse en varios tipos, por ejemplo: Programas Publicitarios (Adware), Bromas, Programas de Riesgo (Riskware), etc. (para más información sobre software potencialmente peligroso detectado por Kaspersky Anti-Virus, ver la Enciclopedia de Virus en www.viruslist.com (<http://www.viruslist.com/en/viruses/encyclopedia>)). Después del análisis, estos programas pueden bloquearse. Debido a que muchos de ellos son ampliamente explotados por los usuarios, pueden ser excluidos del análisis. Para hacerlo, deberá agregar el nombre de la amenaza o la máscara del nombre de la amenaza (de acuerdo con la clasificación de la Enciclopedia de Virus) en la zona de confianza.

Por ejemplo, quizás Ud. utilice frecuentemente un programa de Administración Remota. Este es un sistema de acceso remoto que le permite operar sus recursos desde un equipo remoto. Kaspersky Anti-Virus ve esta clase de actividad de aplicación como potencialmente peligrosa y puede bloquearla. Para evitar bloquear la aplicación, deberá crear una regla de exclusión que especificaría la Administración Remota como el veredicto.

Cuando se agrega una exclusión, esto resulta en una regla, que luego puede ser utilizada en la ejecución de tareas de análisis de virus.

➤ *Para crear una regla de exclusión, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Exclusiones**, haga click en el botón **Zona de confianza**.
4. En la ventana que se abrirá, en la pestaña **Reglas de exclusión**, haga click en el botón **Agregar**.
5. En la ventana **Máscara de exclusión** que se abrirá, en la sección **Propiedades**, seleccione un tipo de exclusión. Luego, en la sección **Descripción de la regla**, asigne valores a los tipos de exclusión seleccionados y seleccione qué componentes de Kaspersky Anti-Virus deberán ser cubiertos por la regla.

➤ *Para crear una regla de exclusión de la ventana de reporte, por favor haga lo siguiente:*

1. Seleccione el objeto del reporte para agregarlo a las exclusiones.

2. Seleccione el elemento **Agregar a la zona de confianza** del menú contextual para este objeto.
3. Se abrirá la ventana **Máscara de exclusión**. Asegúrese de que está satisfecho con los parámetros de la regla de exclusión. Los campos nombre del objeto y tipo de amenaza relevante se completan en forma automática en el informe. Para crear la regla, haga click en el botón **OK**.

MÁSCARAS ACEPTADAS PARA EXCLUSIÓN DE ARCHIVOS

Veamos algunos ejemplos de máscaras aceptadas que puede utilizar al crear la lista de archivos a excluir del análisis:

1. Máscaras sin rutas de archivos:
 - ***.exe** – todos los archivos con extensión `.exe` ;
 - ***.ex?** – todos los archivos con extensión `ex?` , donde `?` puede representar cualquier carácter individual;
 - **test** – todos los archivos con nombre `test`.

2. Máscaras con rutas de archivos absolutas:

- **C:\dir*.*** o **C:\dir*** o **C:\dir** – todos los archivos en 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`.

Si no desea que la aplicación analice archivos en todas las subcarpetas anidadas de la carpeta especificada, active la casilla **Incluir subcarpetas** al crear la máscara.

3. Máscaras de rutas de archivo:

- **dir*.***, o **dir***, o **dir** – todos los archivos en carpetas `dir\`;
- **dir\test** – todos los archivos `test` en carpetas `dir\`;
- **C:\dir*.exe** – todos los archivos con extensión `.exe` en carpetas `dir\`;
- **dir*.ex?** – todos los archivos con extensión `ex?` en todas las carpetas `dir\`, donde `?` puede representar cualquier carácter.

Si no desea que la aplicación analice archivos en todas las subcarpetas anidadas de la carpeta especificada, active la casilla **Incluir subcarpetas** al crear la máscara.

Las máscaras de exclusión `*.*` y `*` sólo pueden utilizarse si especifica el tipo de clasificación de la amenaza de acuerdo con la Enciclopedia de Virus. En este caso, la amenaza especificada no será detectada en ningún objeto. Utilizar estas máscaras sin especificar el tipo de clasificación básicamente desactiva la vigilancia. Tampoco se recomienda, al seleccionar una exclusión, seleccionar una ruta relacionada a un disco de red creado basándose en una carpeta de sistemas de archivos utilizando el comando `subst`, y tampoco a un disco que copia una carpeta de red. El caso es que distintos recursos pueden recibir el mismo nombre de disco para diferentes usuarios, lo que inevitablemente llevará a una ejecución incorrecta de las reglas de exclusión.

VER TAMBIÉN

Máscaras de exclusión permitidas de acuerdo con la Enciclopedia de Virus.....[62](#)

MÁSCARAS DE EXCLUSIÓN PERMITIDAS DE ACUERDO CON LA ENCICLOPEDIA DE VIRUS

Al agregar máscaras para excluir determinadas amenazas de acuerdo con su clasificación en la Enciclopedia de Virus, puede especificar lo siguiente:

- el nombre completo de la amenaza indicado en la Enciclopedia de Virus en www.viruslist.com (<http://www.viruslist.com>), por ejemplo, **no-es-virus: ProgramadeRiesgo.AdministradorRemoto.RA.311** o **Flooder.Win32.Fuxx**;
- el nombre de la amenaza por máscara, por ejemplo:
 - **no-es-virus*** – excluye del análisis programas legítimos pero potencialmente peligrosos, como programas de broma;
 - ***Programa de riesgo.*** – excluye del análisis programas de riesgo;
 - ***Administrador remoto.*** – excluye del análisis todos los administradores remotos.

VER TAMBIÉN

Máscaras aceptadas para exclusión de archivos [61](#)

EXPORTAR / IMPORTAR REGLAS DE EXCLUSIÓN

Exportar e importar están diseñados para llevar las reglas creadas a otros equipos.

➤ *Para copiar las reglas de exclusión, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Exclusiones**, haga click en el botón **Zona de confianza**.
4. En la ventana que se abrirá, en la pestaña **Reglas de exclusión**, utilice los botones **Exportar** e **Importar** para realizar las acciones requeridas para copiar las reglas.

EXPORTAR / IMPORTAR PARÁMETROS DE KASPERSKY ANTI-VIRUS.

Kaspersky Anti-Virus brinda la opción de importar y exportar sus parámetros.

Esta es una característica de ayuda cuando, por ejemplo, se instala la aplicación en el equipo de su hogar y en su oficina. Usted puede configurar la aplicación en la forma que desee en su hogar, exportar aquellos parámetros como un archivo en un disco, y cargarlos en el equipo de su trabajo utilizando la función importar. Se guardan los parámetros en un archivo de configuración especial.

➤ *Para exportar los parámetros actuales de la aplicación, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Administrador de configuraciones** presione el botón **Guardar**.

4. En la ventana que se abrirá, ingrese el nombre del archivo de configuración y la ruta en la que habrá de guardarse.

➤ *Para importar los parámetros de la aplicación de un archivo de configuración guardado, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Administrador de configuraciones** presione el botón **Cargar**.
4. En la ventana que se abrirá, seleccione el archivo desde el que desea importar la configuración para Kaspersky Anti-Virus.

RESTAURACIÓN DE LA CONFIGURACIÓN PREDETERMINADA

Ud. siempre puede volver a los parámetros por defecto o a los recomendados por Kaspersky Anti-Virus. Son considerados óptimos y recomendados por Kaspersky Lab. El Asistente de Configuración de la Aplicación restaura los valores por defecto.

En la ventana que se abrirá, se le pedirá que determine qué parámetros y qué componentes deberán o no guardarse al restaurar el nivel de seguridad recomendado.

➤ *Para restaurar los parámetros de protección, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Protección**.
3. En la sección **Administrador de parámetros de la aplicación** presione el botón **Restablecer**.
4. En la ventana que se abrirá, active las casillas de los parámetros que desea guardar. Haga click en el botón **Siguiente**. Se lanzará el Asistente de Configuración Inicial; siga sus directivas.

ANÁLISIS

La selección del método a utilizar para analizar objetos en su equipo se determina por un conjunto de propiedades asignadas para cada tarea.

Los especialistas de Kaspersky Lab distinguen varias tareas de análisis de virus. Son los siguientes:

Escanear

Analiza objetos seleccionados por el usuario. Ud. puede analizar cualquier objeto en el sistema de archivos del equipo.

Escaneo completo

Consiste en un análisis en detalle de todo el sistema. Los siguientes objetos son analizados por defecto: memoria del sistema, programas cargados al iniciar, resguardo del sistema, bases de datos de correo, discos duros, unidades extraíbles de almacenamiento y unidades de red.

Escaneo rápido

Análisis en busca de virus en los objetos de inicio del sistema operativo.

La ventana de configuración de cada tarea le permite hacer lo siguiente:

- seleccionar el nivel de seguridad (ver página [38](#)) con los parámetros que utilizará la tarea;

- seleccionar una acción (ver página [38](#)) que la aplicación aplicará cuando detecte un objeto infectado / potencialmente infectado;
- crear un cronograma (ver página [43](#)) para ejecutar tareas en forma automática;
- especificar los tipos de archivos (ver página [39](#)) a analizar en busca de virus;
- especificar la configuración del análisis para archivos compuestos (ver página [41](#));
- seleccionar los métodos y de análisis;
- asignar parámetros de análisis comunes para todas las tareas (ver página [45](#)).

➔ *Para editar los parámetros de tareas, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, elija la sección **Analizar (Escaneo Completo, Escaneo Rápido)**.
3. En la parte derecha de la ventana, seleccione el nivel de seguridad requerido, la reacción ante la amenaza y configure el modo de ejecución. Haga click en el botón **Personalizar** para cambiar a los parámetros de otras configuraciones de tareas. Para restaurar los parámetros predeterminados, haga click en el botón **Nivel predeterminado**.

ACTUALIZACIÓN

La actualización de Kaspersky Anti-Virus se realiza utilizando parámetros que determinan lo siguiente:

- el origen (ver página [48](#)) del cual se descargarán e instalarán las actualizaciones;
- el modo de ejecución de la actualización de la aplicación (ver página [51](#)) y los componentes específicos a ser analizados (ver página);
- la frecuencia con que se lanzará si se configura el lanzamiento programado (ver página [50](#));
- bajo qué cuenta (ver página [50](#)) se lanzará la actualización;
- si las actualizaciones van a ser copiadas a una fuente local (ver página [52](#));
- uso de un servidor proxy (ver página [49](#)).

➔ *Para proceder a actualizar la configuración, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Actualizar**.
3. Seleccione el modo de ejecución requerido en la parte derecha de la ventana. Haga click en el botón **Configurar** para cambiar a configurar otras tareas.

OPCIONES

En la ventana **Opciones** puede utilizar las siguientes funciones avanzadas de Kaspersky Anti-Virus:

- Auto-defensa de la aplicación (ver página [65](#)).
- Restringir el acceso a la aplicación (ver página [65](#)).

- Notificaciones sobre los eventos de Kaspersky Anti-Virus (ver página [66](#)):
 - selección de tipos de eventos y forma de enviar notificaciones (ver página [66](#));
 - configurar notificaciones por correo (ver página [67](#));
 - configurar registro de eventos (ver página [67](#)).
- Activar elementos de interfaz (ver página [68](#)).

AUTO-DEFENSA DE LA APLICACIÓN

Kaspersky Anti-Virus refuerza la seguridad de su equipo contra programas maliciosos y, por esa misma razón, puede ser el blanco de programas maliciosos que intenten bloquearlo o eliminarlo.

Para garantizar la estabilidad del sistema de seguridad de su equipo, la aplicación posee sus propios mecanismos de autodefensa y protección contra accesos remotos.

➤ *Para activar la protección contra acceso remoto, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Opciones**.
3. En la sección **Auto-Defensa**, active la casilla **Desactivar el control externo del servicio del sistema** para bloquear todo intento de administrar remotamente los servicios de la aplicación.

Si se detecta alguna acción nociva, se mostrará un mensaje sobre el icono de la aplicación en el área de notificaciones de la barra de tareas, a no ser que el usuario haya desactivado este servicio.

RESTRICCIÓN DE ACCESO A LA APLICACIÓN

Su equipo personal puede ser utilizado por varias personas con distintos niveles de conocimientos informáticos. Dejar abierto el acceso a Kaspersky Anti-Virus y sus parámetros puede disminuir drásticamente la seguridad del equipo en su conjunto.

Para incrementar el nivel de seguridad de su equipo, utilice una contraseña para acceder a Kaspersky Anti-Virus. Esto puede bloquear todas las operaciones, a excepción de las notificaciones que detectan objetos peligrosos, y evitan que se realicen las siguientes acciones:

- cambiar los parámetros de la aplicación;
- cerrar la aplicación;
- detener tareas de análisis.

Cada una de las acciones listadas arriba lleva a un nivel inferior de protección en su equipo, por ello trate de establecer en cuál de los usuarios de su equipo confía para realizar esas acciones.

➤ *Para proteger con una contraseña el acceso a la aplicación, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Opciones**.
3. En la entrada **Protección con contraseña**, seleccione la casilla **Activar la protección con contraseña** y pulse el botón **Configuración**.

- En la ventana **Protección con contraseña** que se abrirá, ingrese la contraseña y especifique el área a cubrir por la restricción de acceso. Ahora, cada vez que un usuario en su equipo intente realizar esta acción que usted ha seleccionado, la aplicación siempre le pedirá la contraseña.

NOTIFICACIONES ACERCA DE EVENTOS DE KASPERSKY ANTI-VIRUS

Ocurren distintos tipos de eventos durante el funcionamiento de Kaspersky Anti-Virus. Pueden ser de tipo referencia o contener información importante. Por ejemplo, un evento puede informarle de la finalización exitosa de una actualización de la aplicación, o puede registrar un error en el funcionamiento de componente determinado que debe ser inmediatamente eliminado.

Para estar actualizado con los eventos más recientes en funcionamiento de Kaspersky Anti-Virus, utilice la función de notificación.

Las notificaciones pueden enviarse en alguna de las siguientes formas:

- mensajes emergentes que aparecen sobre el ícono de la aplicación en la bandeja del sistema;
- notificación de sonido;
- mensajes de correo;
- registrar información en el registro de eventos.

➔ *Para utilizar el servicio de notificación, por favor haga lo siguiente:*

- Abra la ventana de configuración de la aplicación.
- En la parte izquierda de la ventana, seleccione la sección **Opciones**.
- En la sección **Apariencia**, active la casilla **Permitir notificaciones** y haga click en el botón **Configuración**.
- En la ventana **Configuración de Notificación** que se abrirá, especifique los tipos de eventos de Kaspersky Anti-Virus de los cuales desea ser notificado, así como también los tipos de notificación.

VER TAMBIÉN

Seleccionar el tipo de evento y el modo de envío de notificaciones.....	66
Configurar notificaciones por correo.....	67
Configurar registro de eventos	67

SELECCIONAR EL TIPO DE EVENTO Y EL MODO DE ENVÍO DE NOTIFICACIONES

Durante el funcionamiento de Kaspersky Anti-Virus, surgen los siguientes tipos de eventos:

- **Notificaciones críticas** son eventos de importancia crítica. Es altamente recomendable que sean reportados con notificaciones ya que señalan problemas en el funcionamiento de la aplicación o vacíos en la protección de su equipo. Por ejemplo, las *bases de datos son obsoletas* o el *periodo de validez de la licencia ha expirado*.
- **Notificaciones de error** son eventos que conducen a la falta de operabilidad de la aplicación. Por ejemplo, *faltan las bases de datos o están corruptas*.
- **Notificaciones importantes** son eventos que deben ser atendidos porque reflejan situaciones importantes en el funcionamiento de la aplicación. Por ejemplo, las *bases de datos son obsoletas* o la *licencia vence pronto*.

- **Notificaciones menores** son mensajes de tipo referencia que no contienen información importante, como una regla. Por ejemplo, *objetos en cuarentena*.

➔ *Para especificar de cuáles eventos lo notificará la aplicación y cómo, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Opciones**.
3. En la sección **Apariencia**, active la casilla **Permitir notificaciones** y haga click en el botón **Configuración**.
4. En la ventana **Configuración de notificación** que se abrirá, active las casillas para los eventos y las formas de enviar notificaciones para ellos, de los cuales desea ser notificado.

CONFIGURAR NOTIFICACIONES POR CORREO

Una vez que ha seleccionado los eventos (ver sección "Seleccionar tipo de evento y forma de enviar notificaciones" en página [66](#)) sobre cuál desea recibir notificaciones por correo, deberá establecer notificaciones.

➔ *Para configurar las notificaciones por correo, por favor haga lo siguiente:*

1. Abrir la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Opciones**.
3. En la sección **Apariencia**, active la casilla **Permitir notificaciones** y haga click en el botón **Configuración**.
4. En la ventana **Configuración de notificación** que se abrirá, active las casillas para los eventos requeridos en el campo **Correo** y haga click en el botón **Configuración de Correo**.
5. En la ventana **Configuración de notificación por correo** que se abrirá, especifique los valores requeridos para los parámetros. Si desea que las notificaciones sobre los eventos sean enviadas en los momentos programados, cree un cronograma para envío de mensajes informativos haciendo click en el botón **Modificar**. Realizar los cambios requeridos en la ventana **Programación** que se abrirá.

CONFIGURAR REGISTRO DE EVENTOS

Kaspersky Anti-Virus proporciona la opción de registrar información sobre eventos que ocurren mientras se ejecuta la aplicación, ya sea en el registro general de eventos de Microsoft Windows (**Aplicación**) o en el registro dedicado de eventos de Kaspersky Anti-Virus (**Registro de Eventos de Kaspersky**).

Los registros pueden visualizarse en el **Visor de Eventos** de Microsoft Windows que puede abrir utilizando la opción **Inicio/Configuración/Panel de Control/Administración/Ver Eventos**.

➔ *Para configurar el registro de eventos, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Opciones**.
3. En la sección **Apariencia**, active la casilla **Permitir notificaciones** y haga click en el botón **Configuración**.
4. En la ventana **Configuración de notificación** que se abrirá, active las casillas para los eventos requeridos en el campo **Registro** y haga click en el botón **Configuración de Registro**.
5. En la ventana **Configuración del Registro de Eventos** que se abrirá, seleccione el registro en el cual se registrará la información sobre los eventos.

ELEMENTOS ACTIVOS DE LA INTERFAZ

Elementos activos de la interfaz incluye las siguientes opciones de Kaspersky Anti-Virus:

Ícono del área de notificación de la barra de tareas.

Dependiendo de la operación que la aplicación esté ejecutando, cambiará el ícono de la aplicación en la bandeja de sistema. Por defecto, el ícono de la aplicación es animado.

➔ *Para configurar elementos activos de la interfaz, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Opciones**.
3. Active la casilla **Ícono del área de notificación de la barra de tareas animada** en la sección **Apariencia**.

REPORTES Y ALMACENAMIENTOS

La sección contiene los parámetros que controlan las operaciones con archivos de datos de la aplicación.

Archivos de datos de la aplicación, son objetos puestos en cuarentena por Kaspersky Anti-Virus, o movidos al Respaldo, y archivos con informes acerca del funcionamiento de los componentes de la aplicación.

En esta sección, Ud. puede:

- configurar la creación y almacenaje del reporte (ver página [69](#));
- configurar cuarentena y resguardo (ver página [72](#));
- eliminar el archivo de reporte, Cuarentena y Resguardo.

➔ *Para eliminar las áreas almacenadas, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Reportes y Almacenajes**.
3. En la ventana que se abrirá, haga click en el botón **Eliminar**.
4. En la ventana **Archivos de datos** que se abrirá, especifique las áreas de almacenamiento de las cuales se quitarán todos los objetos.

VER TAMBIÉN

Principios de manejo de reportes	69
Configurar reportes.....	69
Cuarentena para objetos potencialmente infectados.....	70
Acciones sobre objetos en cuarentena.....	71
Copias de resguardo de objetos peligrosos	71
Trabajo con copias de resguardo	71
Configurar cuarentena y resguardo.....	72

PRINCIPIOS DE MANEJO DE REPORTES

Cada análisis o tarea de actualización está registrado en un reporte.

➔ *Para ver los reportes, por favor haga lo siguiente:*

1. Abra la ventana principal del programa.
2. Haga click en el botón **Reportes**.

➔ *Para revisar todos los eventos sobre el rendimiento del componente o el rendimiento de la tarea registrada en el reporte, por favor haga lo siguiente:*

1. Abra la ventana principal de la aplicación y haga click en el botón **Reportes**.
2. En la ventana que se abrirá, en la pestaña **Reportes**, seleccione el nombre de la tarea y haga click en el botón **Detalles**. Como resultado emergerá una ventana que contiene información detallada sobre el rendimiento de la tarea seleccionada. Las estadísticas resultantes sobre el rendimiento se muestran en la parte superior de la ventana, y se dará información detallada en varias pestañas en la parte central. La composición de las pestañas puede variar dependiendo de la tarea.

➔ *Para importar el reporte a un archivo de texto, por favor haga lo siguiente:*

1. Abra la ventana principal de la aplicación y haga click en el botón **Reportes**.
2. En la ventana que se abrirá, en la pestaña **Reportes**, seleccione el nombre de un componente o una tarea y haga click en el enlace **Detalles**.
3. En la ventana que se abrirá, se mostrará información sobre el rendimiento de la tarea seleccionada. Haga click en el botón **Guardar como** y especifique el lugar donde desea guardar el archivo de reporte.

CONFIGURAR REPORTES

Usted puede modificar los siguientes parámetros para crear y guardar los reportes:

- Permitir o bloquear el registro de eventos informativos. Como regla, esos eventos no son graves para la protección (la casilla **Registrar eventos sin gravedad**).
- Permitir guardar en el informe sólo los eventos ocurridos desde el último inicio de la tarea. Esto ahorra espacio en disco reduciendo el tamaño del informe (la casilla **Mantener sólo eventos recientes**). Si la casilla está

activada, la información se actualizará cada vez que la tarea sea reiniciada. Sin embargo, sólo se sobrescribirá la información acerca de los objetos sin gravedad.

- Establezca el plazo de almacenamiento para los informes (la casilla **Almacenar informes no más de**). Por defecto, el plazo de almacenamiento de los objetos es de 14 días; una vez expirado, los objetos son eliminados. Puede modificar el tiempo máximo de almacenamiento, e incluso cancelar cualquier restricción impuesta al mismo.
- Especifique el tamaño máximo del reporte (la casilla **Tamaño máximo**). Por defecto, el tamaño máximo es de 100 MB. Puede cancelar cualquier restricción impuesta al tamaño del reporte, o ingresar otro valor.

➔ *Para editar los parámetros para la creación y almacenamiento de reportes, por favor haga lo siguiente:*

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Reportes y Almacenajes**.
3. En la sección **Reportes**, active todas las casillas requeridas, y establezca el término del almacenamiento y el tamaño máximo del reporte, si fuera necesario.

CUARENTENA PARA OBJETOS POTENCIALMENTE INFECTADOS

Cuarentena es un repositorio especial que almacena los objetos potencialmente infectados con virus.

Objetos potencialmente infectados son objetos sospechados de estar infectados con virus o sus modificaciones.

¿Por qué *potencialmente infectado*? No siempre es posible determinar exactamente dónde está infectado un objeto. Esto puede ser por los siguientes motivos:

- *El código del objeto analizado es similar al de una amenaza conocida, pero parcialmente modificado.*

Las bases de dato de la aplicación contienen información sobre amenazas investigadas a la fecha por especialistas de Kaspersky Lab. Si un programa nocivo ha sido modificado y estos cambios no han sido ingresados aún en las bases de datos, Kaspersky Anti-Virus clasifica el objeto infectado con el programa nocivo modificado como un objeto potencialmente infectado, e indica sin falla qué amenaza representa esta infección.

- *El código del objeto detectado tiene una estructura similar a la de un programa nocivo; sin embargo, no hay nada parecido registrado en la bases de datos de la aplicación.*

Es probable que este sea un nuevo tipo de amenaza, por lo que Kaspersky Anti-Virus clasifica el objeto como potencialmente infectado.

Los archivos son identificados como potencialmente infectados con un virus por el *analizador heurístico de código*. Este mecanismo es bastante efectivo y muy rara vez ocasiona falsas alarmas.

El objeto potencialmente infectado puede ser detectado y enviado a cuarentena en el curso del análisis anti-virus.

Cuando coloca un objeto en Cuarentena, es movido, no copiado: el objeto es eliminado del disco o mensaje de correo, y guardado en la carpeta Cuarentena. Los archivos en Cuarentena son guardados en un formato especial, y no son peligrosos.

VER TAMBIÉN

Configurar cuarentena y resguardo.....	72
Acciones sobre objetos en cuarentena.....	71

ACCIONES SOBRE OBJETOS EN CUARENTENA

Puede realizar las siguientes operaciones con objetos en cuarentena:

- poner en cuarentena los archivos que Ud. sospecha pueden estar infectados;
- analizar y desinfectar todos los objetos potencialmente infectados en Cuarentena, utilizando las bases de datos actuales de la aplicación;
- restaurar archivos a las carpetas desde que fueron enviados a Cuarentena, o a las carpetas seleccionadas por el usuario;
- eliminar cualquier objeto en cuarentena, o un grupo de objetos seleccionados.

➔ *Para tomar algunas acciones sobre objetos en cuarentena, por favor haga lo siguiente:*

1. Abra la ventana principal de la aplicación y haga click en el botón **Detectado**.
2. En la ventana que se abrirá, en la pestaña **Cuarentena**, tome las acciones requeridas.

COPIAS DE RESGUARDO DE OBJETOS PELIGROSOS

Algunas veces no puede mantenerse la integridad de los objetos durante la desinfección. Si el archivo desinfectado contiene información importante, y luego de la desinfección se torna parcial o totalmente inaccesible, puede intentar restaurar el objeto original de su copia de resguardo.

Copia de resguardo es una copia de un objeto original peligroso que es creada cuando se desinfecta o elimina el objeto por primera vez, y es guardada en resguardo.

Resguardo es un repositorio especial que contiene copias de resguardo de objetos peligrosos después de su procesamiento o eliminación. La función principal del resguardo es la capacidad de restaurar el objeto original en cualquier momento. Los archivos en Resguardo son guardados en un formato especial, y no son peligrosos.

VER TAMBIÉN

Trabajo con copias de resguardo	71
Configurar cuarentena y resguardo	72

TRABAJO CON COPIAS DE RESGUARDO

Puede aplicar las siguientes funciones a los objetos almacenados en resguardo:

- restaurar copias seleccionadas;
- eliminar objetos.

➔ *Para tomar algunas acciones sobre objetos de resguardo, por favor haga lo siguiente:*

1. Abra la ventana principal de la aplicación y haga click en el botón **Detectado**.
2. En la ventana que se abrirá, en la pestaña **Resguardo**, tome las acciones requeridas.

CONFIGURAR CUARENTENA Y RESGUARDO

Puede editar los siguientes parámetros para cuarentena y resguardo:

- Activar el modo de autoanálisis para los objetos en cuarentena después de cada actualización de las bases de datos de la aplicación (la casilla **Analizar archivos en cuarentena después de cada actualización**).

Kaspersky Anti-Virus no podrá analizar los objetos en cuarentena inmediatamente después de la actualización si usted está trabajando con la cuarentena.

- Determine el tiempo máximo de almacenamiento para los objetos en cuarentena y para copias de los objetos en el resguardo (la casilla **Guardar objetos menores a**). Por defecto, el plazo de almacenamiento de los objetos es de 30 días; una vez expirado, los objetos son eliminados. Puede modificar el tiempo máximo de almacenamiento, e incluso cancelar cualquier restricción impuesta al mismo.
- Especifique el tamaño máximo del área de almacenamiento de datos (la casilla **Tamaño máximo**). Por defecto, el tamaño máximo es de 250 MB. Puede cancelar cualquier restricción impuesta al tamaño del reporte, o ingresar otro valor.

➔ Para configurar los parámetros de cuarentena y resguardo:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, seleccione la sección **Reportes y Almacenajes**.
3. En la sección **Cuarentena y Resguardo**, active las casillas requeridas y especifique el tamaño máximo del área de almacenamiento de datos, si es necesario.

VALIDAR PARÁMETROS DE KASPERSKY ANTI-VIRUS

Después de instalar y configurar Kaspersky Anti-Virus, puede verificar si la aplicación está configurada correctamente, utilizando un virus de prueba y sus modificaciones. Se requiere una prueba individual para cada componente / protocolo de protección.

EN ESTA SECCIÓN

Verificar "virus" EICAR y sus modificaciones	73
Validar parámetros de análisis antivirus	74

VERIFICAR "VIRUS" EICAR Y SUS MODIFICACIONES

Este "virus" de prueba fue desarrollado especialmente por  (The European Institute for Computer Antivirus Research) para verificar productos antivirus.

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

¡Nunca utilice virus reales para verificar el funcionamiento de un producto antivirus!

Intente descargar este "virus" de prueba desde el sitio oficial de **EICAR** en http://www.eicar.org/anti_virus_test_file.htm.

Antes de descargar el archivo debe desactivar la protección antivirus del equipo, de otra manera la aplicación podría identificar y procesar el archivo *anti_virus_test_file.htm* como un objeto infectado transferido vía protocolo HTTP. No olvide activar la protección antivirus inmediatamente después de descargar el "virus" de prueba.

La aplicación identifica el archivo descargado desde el sitio **EICAR** como un objeto infectado que contiene un virus que **no se puede desinfectar** y realiza las acciones especificadas para este tipo de objeto.

También puede modificar el "virus" de prueba estándar para verificar el funcionamiento de la aplicación. Para modificar el "virus", modifique el contenido del "virus" estándar agregándole uno de los prefijos (ver tabla debajo). Para modificar el "virus" de prueba, puede utilizar cualquier editor de texto o hipertexto, como **Bloc de Notas de Microsoft**, **UltraEdit32**, etc.

Puede verificar el funcionamiento correcto de la aplicación antivirus, utilizando el "virus" EICAR modificado, sólo si sus bases antivirus fueron actualizadas por última vez con posterioridad al 24 de octubre de 2003.

En la tabla de abajo, la primera columna contiene los prefijos que deben agregarse al comienzo de la cadena estándar del "virus" de prueba. La segunda columna lista todos los posibles estados que la aplicación antivirus puede asignar al objeto, de acuerdo con los resultados del análisis. La tercera columna indica la manera en que la aplicación procesa objetos con el estado especificado. Por favor, tenga en cuenta que las acciones reales realizadas sobre los objetos son determinadas por la configuración de la aplicación.

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

Table 1. Modificaciones de los "virus" de prueba

Prefijo	Estado del objeto	Información de procesamiento del objeto
Sin prefijo, "virus" de prueba estándar.	Infectado. El objeto contiene el código de un virus conocido. No puede desinfectar el objeto.	La aplicación identifica el objeto como un virus no desinfectable. Ocurrió un error al intentar desinfectar el objeto; se realizará la acción especificada para objetos no desinfectables.
CORR-	Dañado.	La aplicación pudo acceder al objeto, pero no pudo analizarlo porque está dañado (por ejemplo, la estructura del archivo está dañada, o el formato del archivo es inválido). Ud. puede encontrar información de que el objeto ha sido procesado en el informe de funcionamiento de la aplicación.
WARN-	Sospechoso. El objeto contiene el código de un virus desconocido. No puede desinfectar el objeto.	El objeto fue detectado como sospechoso por el analizador de código heurístico. Al momento de la detección, las bases Antivirus de firmas de amenazas no contienen una descripción del procedimiento para tratar este objeto. Usted será notificado cuando se detecte un objeto de este tipo.
SUSP-	Sospechoso. El objeto contiene el código modificado de un virus conocido. No puede desinfectar el objeto.	La aplicación detectó una correspondencia parcial entre una sección de código del objeto y el código de un virus conocido. Al momento de la detección, las bases Antivirus de firmas de amenazas no contienen una descripción del procedimiento para tratar este objeto. Usted será notificado cuando se detecte un objeto de este tipo.
ERRO-	Error de análisis.	Ocurrió un error durante el análisis de un objeto. La aplicación no pudo acceder al objeto porque su integridad está dañada (por ejemplo, no se encuentra el final de un archivador multivolumen) o no hay conexión con el mismo (si el objeto es analizado en un recurso de red). Ud. puede encontrar información de que el objeto ha sido procesado en el informe de funcionamiento de la aplicación.
CURE-	Infectado. El objeto contiene el código de un virus conocido. Desinfectable.	El objeto contiene un virus que puede desinfectarse. La aplicación desinfectará el objeto; el texto del cuerpo del "virus" será reemplazado con la palabra CURE. Usted será notificado cuando se detecte un objeto de este tipo.
DELE-	Infectado. El objeto contiene el código de un virus conocido. No puede desinfectar el objeto.	La aplicación identifica el objeto como un virus no desinfectable. Ocurrió un error al intentar desinfectar el objeto; se realizará la acción especificada para objetos no desinfectables. Usted será notificado cuando se detecte un objeto de este tipo.

VALIDAR PARÁMETROS DE ANÁLISIS ANTIVIRUS

➤ Para verificar que el análisis antivirus esté configurado correctamente:

1. Cree una carpeta en el disco. Copie a esta carpeta el "virus" de prueba descargado del sitio oficial de **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), así como también todas las modificaciones del "virus" que haya creado.
2. Cree una nueva tarea de análisis antivirus y seleccione la carpeta, que contiene el conjunto de "virus" de prueba, como el objeto a analizar.
3. Permita que todos los eventos se registren en el informe para que éste guarde datos sobre objetos corruptos y objetos no analizados debido a errores.
4. Ejecute el análisis antivirus.

Mientras se ejecuta el análisis de virus, las acciones especificadas en la configuración de tareas serán realizadas a medida que se detecten objetos sospechosos o infectados. Seleccionando distintas acciones a realizarse sobre el objeto detectado, Ud. puede realizar una verificación completa del funcionamiento de los componentes.

Puede ver toda la información acerca de las acciones del análisis antivirus en el informe de funcionamiento del componente.

TIPOS DE NOTIFICACIONES

Cuando ocurren los eventos de Kaspersky Anti-Virus, se muestran mensajes de notificación especial. Dependiendo de la criticidad del evento para su equipo, usted podría recibir los siguientes tipos de notificación:

- **Alarma.** Ha ocurrido un evento crítico; por ejemplo, se ha detectado un objeto nocivo o actividad peligrosa en su sistema. Ud. deberá decidir inmediatamente qué hacer con esta amenaza. Este tipo de información está codificada en color rojo.
- **Advertencia.** Ha ocurrido un evento potencialmente peligroso. Por ejemplo, se han detectado en su sistema archivos potencialmente infectados o actividad sospechosa. Deberá decidir cuán peligroso cree que sea este evento. Este tipo de información está codificada en color amarillo.
- **Info.** Esta notificación brinda información sobre eventos no críticos. Este tipo incluye notificaciones mostradas en el curso de una actualización, por ejemplo. Las notificaciones informativas están codificadas en color azul.

EN ESTA SECCIÓN

Objeto nocivo detectado	75
El objeto no se puede desinfectar	76
Objeto sospechoso detectado	76

OBJETO NOCIVO DETECTADO

En caso de que una tarea de análisis antivirus detecte un objeto nocivo, se mostrará una notificación especial.

La notificación contiene:

- El tipo de amenaza (por ejemplo, *virus*, *Troyano*) y el nombre del objeto nocivo tal como está listado en la Enciclopedia de Virus Kaspersky Lab. El nombre del objeto peligroso funciona como un enlace a www.viruslist.com, donde puede encontrar información más detallada sobre el tipo de amenaza detectada en su equipo.
- Nombre completo y ruta del objeto nocivo.

Se le pedirá que seleccione una de las siguientes respuestas para el objeto:

- **Desinfectar** – intenta desinfectar el objeto malicioso. Antes del tratamiento, se realiza una copia de resguardo del objeto en caso de que surja la necesidad de restaurarlo o un retrato de su infección.
- **Eliminar** – borrar objeto malicioso. Antes de eliminarlo, se crea una copia de resguardo del objeto para el caso que surja la posibilidad de restaurarlo o un retrato de su infección.
- **Omitir** – bloquea el acceso al objeto pero no toma acciones sobre éste; simplemente registra información sobre él en un reporte.

Puede regresar más tarde a los objetos nocivos ignorados en la ventana del informe. Sin embargo, no puede posponer el procesamiento de los objetos detectados en los correos.

Para aplicar la acción seleccionada a todos los objetos con el mismo estado detectados en la sesión actual del componente de protección o tarea operativa, active la casilla **Aplicar a todo**. La sesión actual es el tiempo que transcurre entre el inicio del componente y su desactivación o reinicio de la aplicación, o el tiempo que toma una tarea de análisis de virus desde que se inicia hasta que termina.

EL OBJETO NO SE PUEDE DESINFECTAR

Hay casos en que es imposible desinfectar un objeto nocivo. Esto puede ocurrir si el archivo está tan dañado que resulta imposible eliminar el código nocivo y restaurar su integridad. El procedimiento para tratarlos no puede aplicarse a varios tipos de objetos peligrosos, como los Troyanos.

En tales casos, emergerá una notificación especial que contiene:

- El tipo de amenaza (por ejemplo, *virus*, *Troyano*) y el nombre del objeto nocivo tal como está listado en la Enciclopedia de Virus Kaspersky Lab. El nombre del objeto peligroso funciona como un enlace a www.viruslist.com, donde puede encontrar información más detallada sobre el tipo de amenaza detectada en su equipo.
- Nombre completo y ruta del objeto nocivo.

Se le pedirá que seleccione una de las siguientes respuestas para el objeto:

- **Eliminar** – borrar objeto nocivo. Antes de eliminarlo, se crea una copia de resguardo del objeto para el caso que surja la posibilidad de restaurarlo o un retrato de su infección.
- **Omitir** – bloquea el acceso al objeto pero no toma acciones sobre éste; simplemente registra información sobre él en un reporte.

Puede regresar más tarde a los objetos nocivos ignorados en la ventana del informe. Sin embargo, no puede posponer el procesamiento de los objetos detectados en los correos.

Para aplicar la acción seleccionada en todos los objetos con el mismo estado detectado en la sesión actual del componente de protección o de la tarea, active la casilla **Aplicar a todos**. La sesión actual es el tiempo que transcurre entre el inicio del componente y su desactivación o reinicio de la aplicación, o el tiempo que toma una tarea de análisis de virus desde que se inicia hasta que termina.

OBJETO SOSPECHOSO DETECTADO

Si el análisis de virus detecta un objeto que contiene código de un virus desconocido o código modificado de un virus conocido, emergerá una notificación especial.

La notificación contiene:

- El tipo de amenaza (por ejemplo, *virus*, *Troyano*) y el nombre del objeto tal como está listado en la Enciclopedia de Virus Kaspersky Lab. El nombre del objeto peligroso funciona como un enlace a www.viruslist.com, donde puede encontrar información más detallada sobre el tipo de amenaza detectada en su equipo.
- Nombre completo y ruta del objeto.

Se le pedirá que seleccione una de las siguientes respuestas para el objeto:

- **Cuarentena** – mueve el objeto a Cuarentena. Cuando coloca un objeto en Cuarentena, es movido, no copiado: el objeto es eliminado del disco o mensaje de correo, y guardado en la carpeta Cuarentena. Los archivos en Cuarentena son guardados en un formato especial, y no son peligrosos.

Cuando más tarde analice la Cuarentena con las firmas de amenazas actualizadas, el estado del objeto puede modificarse. Por ejemplo, el objeto puede ser identificado como infectado y luego procesado utilizando una base de datos actualizada. De otro manera, al objeto podría asignársele el estado no *infectado*, y luego restaurarlo.

Si un archivo es movido a cuarentena manualmente y luego de análisis subsiguientes resultara no estar infectado, su estado no cambiará a *OK* inmediatamente después del análisis. Esto sólo ocurrirá si el análisis es efectuado después de un determinado lapso de tiempo (al menos tres días) después de su puesta en cuarentena.

- **Eliminar** – borrar objeto. Antes de eliminarlo, se crea una copia de resguardo del objeto para el caso que surja la posibilidad de restaurarlo o un retrato de su infección.
- **Omitir** – bloquea el acceso al objeto pero no toma acciones sobre éste; simplemente registra información sobre él en un reporte.

Puede regresar más tarde a los objetos ignorados en la ventana del informe. Sin embargo, no puede posponer el procesamiento de los objetos detectados en los correos.

Para aplicar la acción seleccionada a todos los objetos con el mismo estado detectados en la sesión actual del componente de protección o tarea operativa, active la casilla **Aplicar a todo**. La sesión actual es el tiempo que transcurre entre el inicio del componente y su desactivación o reinicio de la aplicación, o el tiempo que toma una tarea de análisis de virus desde que se inicia hasta que termina.

Si está seguro que el objeto detectado no es nocivo, le recomendamos agregarlo a la zona confiable para evitar que la aplicación reitere falsos positivos cuando Ud. utiliza el objeto.

CÓMO TRABAJAR CON LA APLICACIÓN DESDE LA LÍNEA DE COMANDOS

Puede trabajar con Kaspersky Anti-Virus desde la línea de comandos.

Sintaxis de la línea de comando:

```
avp.com <comando> [opciones]
```

Ud. debe acceder a la aplicación desde la línea de comandos de la carpeta de instalación de Kaspersky Anti-Virus, o especificando la ruta completa al archivo avp.com.

Los siguientes comandos pueden ser utilizados como <comando>:

- **HELP** – ayuda con la sintaxis del comando y la lista de comandos.
- **SCAN** – analiza objetos en busca de software nocivo.
- **UPDATE** – inicia la actualización de la aplicación.
- **ROLLBACK** – revierte a la última actualización de Kaspersky Anti-Virus realizada (el comando sólo puede ejecutarse si se ingresa la contraseña asignada a través de la interfaz de la aplicación).
- **START** – inicia una tarea o componente.
- **STOP** – detiene un componente o una tarea (el comando sólo puede ejecutarse si se ingresa la contraseña asignada a través de la interfaz Kaspersky Anti-Virus).
- **STATUS** – muestra en pantalla el estado actual de un componente o tarea.
- **STATISTICS** – muestra en pantalla estadísticas para el componente o tarea.
- **EXPORT** – exporta parámetros de protección de la aplicación.
- **IMPORT** – importa parámetros de protección de la aplicación (el comando sólo puede ejecutarse si se ingresa la contraseña asignada a través de la interfaz Kaspersky Anti-Virus).
- **ACTIVATE** – activa Kaspersky Anti-Virus a través de Internet utilizando un código de activación.
- **ADDKEY** – activa la aplicación usando un archivo llave (el comando sólo puede ejecutarse si se ingresa la contraseña asignada a través de la interfaz de la aplicación).
- **RESTORE** – restaura un archivo de la cuarentena.
- **EXIT** – cierra la aplicación (el comando sólo puede ejecutarse si se ingresa la contraseña asignada a través de la interfaz de la aplicación).
- **TRACE** – obtiene un archivo de rastreo.

Cada comando requiere su propio conjunto específico de parámetros.

EN ESTA SECCIÓN

Visualizar la Ayuda	79
Análisis antivirus.....	79
Actualizar la aplicación	81
Reversión a la última actualización	82
Inicia / detiene la ejecución de tareas.....	82
Estadísticas sobre el funcionamiento de una tarea o componente	83
Exportar parámetros de protección	83
Importar parámetros de protección	84
Activar la aplicación.....	84
Restaurar un archivo de la cuarentena.....	85
Cerrar la aplicación.....	85
Obtener un archivo de rastreo.....	85
Devuelve códigos de la línea de comandos	86

VISUALIZAR LA AYUDA

Utilice este comando para ver la sintaxis de la línea de comandos de la aplicación:

```
avp.com [ /? | HELP ]
```

Para obtener ayuda en la sintaxis de un comando específico, puede utilizar uno de los siguientes comandos:

```
avp.com <comando> /?
```

```
avp.com HELP <comando>
```

ANÁLISIS ANTIVIRUS

El inicio del análisis de un área determinada, en busca de virus y objetos nocivos, desde la línea de comandos, generalmente se presenta así:

```
avp.com SCAN [<objeto analizado>] [<acción>] [<tipo de archivos>] [<exclusiones>]
[<configuración del informe>] [<configuración avanzada>]
```

Para analizar objetos, también se puede recurrir a las tareas creadas en la aplicación ejecutando la que se requiera desde la línea de comandos. La tarea será realizada con los parámetros especificados en la interfaz de Kaspersky Anti-Virus.

Descripción de parámetros:

<objeto analizado> – este parámetro proporciona la lista de objetos que se analizarán en busca de códigos nocivos. El parámetro puede incluir varios valores de la lista provista, separados por espacios:

- **<archivos>** – lista de rutas a los archivos y / o carpetas a analizar. Puede indicar la ruta absoluta o relativa al archivo. Los elementos de la lista aparecen separados por espacios. Comentarios:
 - si el nombre del objeto contiene un espacio, deberá colocarlo entre comillas;
 - si se hace referencia a una carpeta específica, se analizarán todos los archivos en esta carpeta.
- **/ALL** – análisis completo del equipo.
- **/MEMORY** – objetos de la RAM.
- **/STARTUP** – objeto del inicio.
- **/MAIL** – bases de datos de correo.
- **/REMDRIVES** – todas las unidades extraíbles.
- **/FIXDRIVES** – todas las unidades locales.
- **/NETDRIVES** – todas las unidades de red.
- **/QUARANTINE** – objetos en cuarentena.
- **/@:<filelist.lst>** – ruta a un archivo con una lista de objetos y catálogos para analizar. El archivo debe tener formato de texto y cada objeto de análisis debe estar listado en línea aparte. Puede indicar la ruta absoluta o relativa al archivo. La ruta debe colocarse entre comillas aun cuando la misma contenga espacios.

<acción> – este parámetro determina la acción a ejecutar con los objetos nocivos detectados durante el análisis. Si este parámetro no está definido, la acción predeterminada es **/i2**. Los siguientes valores son posibles:

- **/i0** – no se ejecuta ninguna acción con el objeto; sólo se registra en el informe los datos sobre el evento.
- **/i1** – se neutralizan los objetos infectados, se los ignora si la desinfección no es posible.
- **/i2** – trata objetos infectados, y si no es posible su desinfección, los elimina. No eliminar objetos infectados de objetos compuestos. Eliminar los objetos compuestos infectados con encabezados ejecutables (archivadores .sfx). Esta es la configuración predeterminada.
- **/i3** – trata objetos infectados y los elimina si falla la desinfección. Eliminar por completo todos los objetos compuestos si no es posible desinfectar las partes infectadas.
- **/i4** – elimina los objetos infectados. Eliminar por completo todos los objetos compuestos si no es posible desinfectar las partes infectadas.
- **/i8** – se consulta al usuario en caso de detectarse un objeto infectado.
- **/i9** – pedir al usuario que decida una acción a ejecutar al final del análisis.

<tipos de archivos> – este parámetro define los tipos de archivos que se someterán al análisis antivirus. Por defecto, si este parámetro no está definido, sólo serán analizados por contenido los archivos infectados. Los siguientes valores son posibles:

- **/fe** – analiza únicamente archivos infectados por extensión.
- **/fi** – analiza únicamente archivos por contenido.
- **/fa** – analiza todos los archivos.

<exclusiones> – este parámetro define qué objetos se excluyen del análisis. El parámetro puede incluir varios valores de la lista provista, separados por espacios.

- **/e:a** – no analiza archivadores.

- **/e:b** – no analiza bases de datos de correo.
- **/e:m** – no analiza correos de texto sin formato.
- **/e:<mask>** – no analiza objetos que coinciden con la máscara.
- **/e:<segundos>** – ignora objetos que se sometan al análisis por más tiempo del determinado por el parámetro **<segundos>**.

<parámetros de informes> – estos parámetros determinan el formato del informe con los resultados del análisis. Se puede usar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, todos los eventos y los resultados del análisis son mostrados en pantalla.

- **/R:<archivo_de_reporte>** – registrar sólo eventos importantes en el reporte.
- **/RA:<archivo_de_reporte>** – registrar todos los eventos en el reporte.

<parámetros avanzados> – parámetros que establecen el uso de las tecnologías de análisis antivirus y del archivo de configuración de parámetros:

- **/iChecker=<activado|desactivado>** – activar / desactivar el uso de tecnología iChecker.
- **/iSwift=<activado|desactivado>** – activar / desactivar el uso de tecnología iSwift.
- **/C:<nombre_de_archivo_de_configuración>** – define la ruta del archivo de configuración con los parámetros del programa para el análisis. Puede indicar la ruta absoluta o relativa al archivo. Si este parámetro no está definido, se utilizan los valores definidos en la interfaz de la aplicación.

Ejemplos:

- *Iniciar un análisis de la memoria, programas de Inicio, bases de datos de correo, los directorios Mis Documentos y Archivos de Programa, y el archivo test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documentos y Configuraciones\Todos los
Usuarios\Mis Documentos" "C:\Archivos de Programa" "C:\Descargas\test.exe"
```

- *Analiza los objetos listados en el archivo object2scan.txt. usando el archivo de configuración scan_setting.txt. Usar el archivo de configuración scan_setting.txt. Al completar el análisis, crea un reporte para registrar todos los eventos:*

```
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
```

ACTUALIZAR LA APLICACIÓN

La sintaxis para actualizar los módulos de Kaspersky Anti-Virus y las bases de datos de la aplicación desde la línea de comandos es la siguiente:

```
avp.com UPDATE [<actualizar_fuente>] [/APP=<activado|desactivado>]
[<parámetros_de_informes>] [<configuración_avanzada>]
```

Descripción de parámetros:

<actualizar_fuente> – servidor HTTP o FTP, o carpeta de red donde descargar actualizaciones. Si la ruta no es seleccionada, la fuente de actualización será la especificada en los parámetros de actualización de la aplicación.

/APP=<activado|desactivado> – activar / desactivar la actualización de módulos de la aplicación.

<parámetros de informes> – estos parámetros determinan el formato del informe con los resultados del análisis. Se puede usar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, todos los eventos y los resultados del análisis son mostrados en pantalla. Los siguientes valores son posibles:

- **/R:<archivo_de_reporte>** – registrar sólo eventos importantes en el reporte.
- **/RA:<archivo_de_reporte>** – registrar todos los eventos en el reporte.

<configuración avanzada> – parámetros que definen el uso del archivo de configuración de parámetros.

/C:<nombre_de_archivo_de_configuración> – define la ruta del archivo de configuración con los parámetros del programa para el análisis. Puede indicar la ruta absoluta o relativa al archivo. Si este parámetro no está definido, se utilizan los valores definidos en la interfaz de la aplicación.

Ejemplos:

➤ *Actualizar bases de datos de la aplicación y grabar todos los eventos en un reporte:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➤ *Actualizar los módulos de la aplicación Kaspersky Anti-Virus utilizando los parámetros del archivo de configuración updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

REVERSIÓN A LA ÚLTIMA ACTUALIZACIÓN

Sintaxis de comando:

```
avp.com ROLLBACK </contraseña=<contraseña>> [<parámetros_de_informes>]
```

Descripción de parámetros:

</contraseña=<contraseña>> – una contraseña asignada a través de la interfaz de la aplicación. El comando ROLLBACK no será ejecutado si no se ingresa la contraseña.

<parámetros de informes> – parámetros que determinan el formato del informe con los resultados del análisis. Se puede usar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, todos los eventos y los resultados del análisis son mostrados en pantalla.

- **/R:<archivo_de_reporte>** – registrar sólo eventos importantes en el reporte.
- **/RA:<archivo_de_reporte>** – registrar todos los eventos en el reporte. Se puede usar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, todos los eventos y los resultados del análisis son mostrados en pantalla.

Por ejemplo:

```
avp.com ROLLBACK/contraseña=123/RA:rollback.txt
```

INICIA / DETIENE LA EJECUCIÓN DE TAREAS

Sintaxis del comando START:

```
avp.com START <perfil|nombre_de_la_tarea> [parámetros_de_informes]
```

Sintaxis del comando STOP:

```
avp.com STOP <perfil|nombre_de_tarea> </contraseña=<contraseña>>
```

Descripción de parámetros:

</contraseña=<contraseña>> – una contraseña asignada a través de la interfaz de la aplicación. El comando STOP no será ejecutado si no se ingresa la contraseña.

<parámetros de informes> – estos parámetros determinan el formato del informe con los resultados del análisis. Se puede usar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, todos los eventos y los resultados del análisis son mostrados en pantalla. Los siguientes valores son posibles:

- **/R:<archivo_de_reporte>** – registrar sólo eventos importantes en el reporte.
- **/RA:<archivo_de_reporte>** – registrar todos los eventos en el reporte. Se puede usar una ruta absoluta o relativa al archivo. Si el parámetro no está definido, todos los eventos y los resultados del análisis son mostrados en pantalla.

El parámetro **<perfil|nombre_de_tarea>** puede tener uno de los siguientes valores:

- **Scan_My_Computer** – tarea de análisis completo del equipo;
- **Scan_Objects** – análisis de objetos;
- **Scan_Quarantine** – análisis de la cuarentena;
- **Scan_Startup (STARTUP)** – análisis de objetos de inicio;
- **Updater** – tarea de actualización;
- **Rollback** – tarea de reversión de actualizaciones.

Los componentes y tareas iniciadas desde la línea de comando son ejecutados con los parámetros modificados a través de la interfaz de la aplicación.

Ejemplos:

➔ *Para detener la tarea de análisis completo desde el prompt del comando, ingrese lo siguiente:*

```
avp.com STOP Analizar_Mi_PC /contraseña=<su_contraseña>
```

ESTADÍSTICAS SOBRE EL FUNCIONAMIENTO DE UNA TAREA O COMPONENTE

Sintaxis del comando STATUS:

```
avp.com STATUS <perfil|nombre_de_tarea>
```

Sintaxis del comando STATISTICS:

```
avp.com STATISTICS <perfil|nombre_de_tarea>
```

Descripción de parámetros:

El parámetro **<perfil|nombre_de_tarea>** puede tener uno de los valores especificados en el comando START / STOP (ver página [82](#)).

EXPORTAR PARÁMETROS DE PROTECCIÓN

Sintaxis de comando:

```
avp.com EXPORT <perfil|nombre_de_tarea> <nombre_de_archivo>
```

Descripción de parámetros:

El parámetro **<perfil|nombre_de_tarea>** puede tener uno de los valores especificados en el comando START / STOP (ver página [82](#)).

<nombre_de_archivo> – ruta del archivo al cual se exportan los parámetros de la aplicación. Debe especificar una ruta absoluta o relativa.

Por ejemplo:

```
avp.com EXPORT RTP RTP_settings.dat - formato binario
avp.com EXPORT FM FM_settings.txt - formato de texto
```

IMPORTAR PARÁMETROS DE PROTECCIÓN

Sintaxis de comando:

```
avp.com IMPORT <nombre_de_archivo> </contraseña=<su_contraseña>>
```

Descripción de parámetros:

<nombre_de_archivo> – ruta del archivo al cual se exportan los parámetros de la aplicación. Debe especificar una ruta absoluta o relativa.

</contraseña=<su_contraseña>> – una contraseña asignada a través de la interfaz de la aplicación.

Por ejemplo:

```
avp.com IMPORT settings.dat
```

ACTIVAR LA APLICACIÓN

Puede activar Kaspersky Anti-Virus en dos formas:

- a través de Internet utilizando un código de activación (el comando ACTIVATE);
- utilizando un archivo llave (el comando ADDKEY).

Sintaxis de comando:

```
avp.com ACTIVATE <código_de_activación> </contraseña=<contraseña>>
avp.com ADDKEY <nombre_de_archivo> </contraseña=<contraseña>>
```

Descripción de parámetros:

<código_de_activación> – el código de activación: xxxxx-xxxxx-xxxxx-xxxxx.

<nombre_de_archivo> – archivo llave de la aplicación con extensión .key.

</contraseña=<contraseña>> – una contraseña asignada a través de la interfaz de la aplicación.

Por ejemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </contraseña=<contraseña>>
```

RESTAURAR UN ARCHIVO DE LA CUARENTENA

Sintaxis de comando:

```
avp.com RESTORE [/REPLACE] <nombre_de_archivo>
```

Descripción de parámetros:

/REPLACE – reemplazo de archivo existente.

<nombre_de_archivo> – el nombre del archivo a restaurar.

Por ejemplo:

```
avp.com REPLACE C:\eicar.com
```

CERRAR LA APLICACIÓN

Sintaxis de comando:

```
avp.com EXIT </contraseña=<contraseña>>
```

Descripción de parámetros:

</contraseña=<contraseña>> – una contraseña asignada a través de la interfaz de la aplicación. El comando no será ejecutado si no se ingresa la contraseña.

OBTENER UN ARCHIVO DE RASTREO

Podría necesitar crear un archivo de rastreo si tiene problemas con Kaspersky Anti-Virus. Los archivos de rastreo son útiles para solucionar problemas, y son ampliamente utilizados por los especialistas en el soporte técnico.

Sintaxis de comando:

```
avp.com TRACE [archivo] [activado|desactivado] [<nivel_de_rastreo>]
```

Descripción de parámetros:

[activado|desactivado] – activar / desactivar creación de archivo de rastreo.

[archivo] – rastreo de salida al archivo.

<nivel_de_rastreo> – este valor puede ser un número entero de 100 (nivel mínimo, sólo mensajes críticos) a 600 (nivel máximo, todos los mensajes).

Al contactarse con el Servicio de Soporte Técnico deberá especificar el nivel de rastreo requerido. Si el nivel no está especificado, recomendamos establecer el valor en 500.

Ejemplos:

► *Para desactivar la creación de archivos de rastreo:*

```
avp.com archivo TRACE desactivado
```

► *Crear un archivo de rastreo con nivel de rastreo de 500:*

```
avp.com archivo TRACE activado 500
```

DEVUELVE CÓDIGOS DE LA LÍNEA DE COMANDOS

Los códigos generales pueden ser devueltos por cualquier comando de la línea de comandos. Los códigos de retorno incluyen códigos generales y códigos específicos a un tipo de tarea específico.

Códigos de retorno generales:

- 0 – operación completada exitosamente;
- 1 – valor de parámetro no válido;
- 2 – error desconocido;
- 3 – error finalizando la tarea;
- 4 – tarea cancelada.

Códigos de retorno de tarea de análisis de virus:

- 101 – todos los objetos peligrosos procesados;
- 102 – objetos peligrosos detectados.

MODIFICAR, REPARAR O QUITAR LA APLICACIÓN

Puede desinstalar la aplicación en las siguientes maneras:

- utilizando el asistente de configuración de la aplicación (ver sección "Modificar, reparar, y quitar el programa utilizando el asistente de instalación" en página [87](#));
- desde prompt del comando (ver sección "Desinstalar la aplicación desde el prompt del comando" en página [88](#));
- utilizando Kaspersky Administration Kit (por favor referirse a [Kaspersky Administration Kit Deployment Guide](#));
- utilizando políticas de grupo de dominio de Microsoft Windows Server 2000/2003 (ver sección "Desinstalar la aplicación" en página [20](#)).

EN ESTA SECCIÓN

Modificar, reparar y quitar la aplicación utilizando el Asistente de Instalación	87
Quitar la aplicación desde el prompt del comando	88

MODIFICAR, REPARAR Y QUITAR LA APLICACIÓN UTILIZANDO EL ASISTENTE DE INSTALACIÓN

Podrá necesitar reparar la aplicación si ha detectado errores en su funcionamiento luego de una configuración incorrecta o de una corrupción en el archivo.

Al cambiar los componentes en la aplicación, puede instalar los componentes faltantes de Kaspersky Anti-Virus o eliminar aquellos que no desea ni necesita.

► *Para reparar o modificar los componentes faltantes de Kaspersky Anti-Virus o desinstalar la aplicación, por favor haga lo siguiente:*

1. Inserte el CD de instalación en su unidad de CD/DVD-ROM si utilizó una para instalar la aplicación. Si ha instalado Kaspersky Anti-Virus desde una fuente diferente (carpeta de acceso público, carpeta en su disco duro, etc.), asegúrese que el paquete de instalación de la aplicación esté en la ubicación dada y que usted tenga acceso a él.
2. Seleccione **Inicio** → **Programas** → **Kaspersky Anti-Virus 6.0 SOS MP4** → **Modificar, Reparar, o Quitar**.

El asistente de instalación se abrirá para el programa. Miremos detenidamente todos los pasos que deben realizarse para reparar, modificar, o quitar la aplicación.

PASO 1. VENTANA DE BIENVENIDA A LA INSTALACIÓN

Si ha seguido todos los pasos descriptos arriba y necesita reparar o modificar la aplicación, aparecerá la ventana de bienvenida a la instalación de Kaspersky Anti-Virus. Haga click en el botón **Siguiente** para continuar.

PASO 2. SELECCIONAR UNA OPERACIÓN

En este paso, deberá seleccionar qué operación desea ejecutar en la aplicación. Puede modificar los componentes de la aplicación, reparar los componentes que ya están instalados, o quitar varios componentes o toda la aplicación. Para ejecutar la operación que necesita, haga click en el botón adecuado. La respuesta del programa de instalación depende de la operación que ha seleccionado.

Modificar la aplicación es similar a la instalación de la aplicación personalizada donde puede especificar cuáles componentes desea instalar, y cuáles desea eliminar.

Reparar la aplicación depende de los componentes de la aplicación instalados. Los archivos se repararán para todos los componentes que han sido instalados y para cada uno de ellos se establecerá el nivel de seguridad **Recomendado**.

Al quitar la aplicación, puede seleccionar qué datos creados y usados por la aplicación desea guardar en su equipo. Para eliminar todos los datos de Kaspersky Anti-Virus, seleccione la opción **Desinstalar completamente**. Para guardar los datos, seleccione la opción **Guardar los objetos de la aplicación** y especificar qué objetos no deben ser eliminados:

- *Información de activación* – archivo llave necesario para trabajar con la aplicación.
- *Bases de datos de la aplicación* - grupo completo de firmas de programas peligrosos, virus, y otras amenazas actuales al momento de la última actualización.
- *Objetos de resguardo* – copias de resguardo de objetos eliminados o desinfectados. Recomendamos guardar estos objetos, para que puedan ser restaurados luego.
- *Objetos en cuarentena* – objetos que están potencialmente infectados por virus o modificaciones de ellos. Estos objetos contienen código similar al código de un virus conocido pero es difícil determinar si son nocivos. Se recomienda guardarlos, ya que pueden no ser perjudiciales o pueden ser desinfectados después de actualizar las firmas de amenazas.
- *Parámetros de la aplicación* - parámetros para todos los componentes de la aplicación.

Para iniciar la operación seleccionada, haga click en el botón **Siguiente**. La aplicación comenzará a copiar los archivos necesarios para su equipo o eliminará los componentes y datos seleccionados.

PASO 3. COMPLETAR LA MODIFICACIÓN, REPARACIÓN O ELIMINACIÓN DE LA APLICACIÓN

El proceso de modificación, reparación, o eliminación se mostrará en la pantalla, y luego será informado sobre su terminación.

La eliminación del programa generalmente requiere que reinicie luego su equipo, ya que esto es necesario para se acomoden las modificaciones en su sistema. La aplicación le preguntará si desea reiniciar su equipo. Haga click en el botón **Sí** para reiniciar inmediatamente. Para reiniciar su equipo más tarde, haga click en el botón **No**.

QUITAR LA APLICACIÓN DESDE EL PROMPT DEL COMANDO

- *Para desinstalar Kaspersky Anti-Virus 6.0 SOS MP4 desde el prompt del comando, ingrese lo siguiente:*

```
msiexec /x <nombre_del_paquete>
```

Se abrirá el asistente de instalación. Podrá utilizarlo para desinstalar la aplicación.

- *Para desinstalar la aplicación en modo no-interactivo sin reiniciar el equipo (el equipo deberá reiniciarse manualmente luego de la desinstalación), ingrese lo siguiente:*

```
msiexec /x <nombre_del_paquete> /qn
```

- *Para desinstalar la aplicación en modo no-interactivo y luego reiniciar el equipo, ingrese lo siguiente:*

```
msiexec /x <nombre_del_paquete> ALLOWREBOOT=1 /qn
```

Si decidió proteger con contraseña en vez de desinstalar la aplicación cuando instaló la aplicación, necesitará confirmar la contraseña cuando desinstale la aplicación. De otro modo la aplicación no podrá ser desinstalada.

- *Para quitar la aplicación cuando está protegida con contraseña, ingrese lo siguiente:*

```
msiexec /x <nombre_del_paquete> KLUNINSTPASSWD=***** – para quitar la aplicación en modo interactivo;
```

```
msiexec /x <nombre_del_paquete> KLUNINSTPASSWD=***** /qn – para quitar la aplicación en modo no-interactivo.
```

ADMINISTRAR LA APLICACIÓN A TRAVÉS DE KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit es un sistema para administrar centralmente las tareas administrativas clave en el funcionamiento de un sistema de seguridad para una red corporativa, basado en las aplicaciones incluidas en Kaspersky Anti-Virus Open Space Security. Kaspersky Administration Kit soporta todas las configuraciones de red que utilizan TCP/IP.

La aplicación está intencionada para administradores de redes de equipos corporativos y empleados responsables de la protección anti-virus en sus empresas.

Kaspersky Anti-Virus 6.0 SOS MP4 es uno de los productos de Kaspersky Lab que puede ser administrado a través de su propia interfaz de aplicación, el prompt del comando (estos métodos están descritos más arriba), o utilizando el programa Kaspersky Administration Kit (si el equipo forma parte de un sistema de administración remoto centralizado).

Para administrar Kaspersky Anti-Virus a través de Kaspersky Administration Kit, por favor haga lo siguiente:

- desplegar el *Servidor de Administración* en la red;
- instalar la *Consola de Administración* en la estación de trabajo del administrador (para más detalles ver Kaspersky Administration Kit Deployment Guide);
- instalar Kaspersky Anti-Virus y *Agente de Red* (incluido con Kaspersky Administration Kit) en los equipos de la red. Para más detalles sobre la instalación remota del paquete de instalación de Kaspersky Anti-Virus en equipos de la red, vea Kaspersky Administration Kit Deployment Guide.

Note que si los equipos en la red ya tienen instalada una versión anterior de Kaspersky Anti-Virus, deberá seguir los siguientes pasos antes de actualizar a la nueva versión a través de Kaspersky Administration Kit:

- detener de antemano la versión anterior de la aplicación (puede hacerlo en forma remota a través de Kaspersky Administration Kit);
- cierre todas las aplicaciones que se están ejecutando antes de comenzar la instalación;
- instale la versión 6.0.

Antes de actualizar el complemento de administración de Kaspersky Lab a través de Kaspersky Administration Kit, cierre la Consola de Administración.

Consola de Administración (ver figura abajo) le permite administrar la aplicación a través de Kaspersky Administration Kit. Proporciona una **interfaz integrada MMC** estándar, y permite que el administrador realice las siguientes funciones:

- instalar y desinstalar remotamente Kaspersky Anti-Virus y *Agente de Red* en los equipos de la red;
- configurar remotamente Kaspersky Anti-Virus en los equipos de la red;
- actualizar las bases de datos y módulos de Kaspersky Anti-Virus;
- administrar licencias para Kaspersky Anti-Virus en los equipos de la red;
- ver información sobre el funcionamiento de la aplicación en los equipos del cliente.

Kaspersky Anti-Virus 6.0 SOS MP4 no puede asegurar la protección del equipo en tiempo real. Así, se mostrará un equipo con Kaspersky Anti-Virus instalado en el panel de resultados de la Consola de Administración de Kaspersky Administration Kit con el estado **Crítico** (ícono rojo junto al nombre del equipo).



Figura 11. Consola de Administración de Kaspersky Administration Kit

La apariencia de la ventana principal de Kaspersky Administration Kit puede variar dependiendo del sistema operativo del equipo que está utilizando.

Al trabajar a través de Kaspersky Administration Kit, la aplicación se administra por parámetros de políticas, parámetros de tareas, y parámetros de la aplicación establecidos por el administrador.

A las acciones nombradas y tomadas por la aplicación se las conoce como *tareas*. En base a las funciones que realizan, las tareas se dividen por *tipos*: tareas de análisis de virus, tareas de actualización de la aplicación, reversiones de actualizaciones, y tareas de instalación de archivos llave.

Cada tarea tiene una cantidad de parámetros para la aplicación que se utilizan cuando se ejecuta. Los parámetros de la tarea para la aplicación que son comunes a todos los tipos de tareas son los *parámetros de la aplicación*. Los parámetros de la aplicación que son específicos para un tipo de tarea forman los *parámetros de tareas*. Los parámetros de la aplicación y los parámetros de tareas no se superponen.

La característica fundamental de la administración centralizada es el agrupamiento de equipos remotos en la red y su administración, creando y configurando políticas de grupo.

Política es un conjunto de parámetros de aplicación para un grupo, así como también un conjunto de restricciones al reeditar esos parámetros cuando se establece la aplicación o tareas en un equipo de un cliente individual. Una política incluye parámetros para configurar todas las características de la aplicación, con la excepción de los parámetros que son personalizados para instancias específicas de una tarea. Los parámetros de programación son un ejemplo.

Por ello, las políticas incluyen los siguientes parámetros:

- Parámetros comunes a todas las tareas (parámetros de la aplicación);
- Parámetros comunes a todas las instancias de un tipo de tarea única (parámetros de tareas primarias).

Esto significa que la política para Kaspersky Anti-Virus, las tareas para las cuales se incluye protección anti-virus y tareas de análisis, incluye todos los parámetros necesarios para configurar la aplicación cuando se ejecutan ambos tipos de tareas pero no, por ejemplo, una programación para ejecutar esas tareas o parámetros que definen el alcance del análisis.

EN ESTA SECCIÓN

Administrar la aplicación.....92

Administrar tareas98

Administrar políticas103

ADMINISTRAR LA APLICACIÓN

Kaspersky Administration Kit le da la oportunidad de iniciar remotamente y detener Kaspersky Anti-Virus en equipos de clientes individuales, así como también modificar los parámetros generales para la aplicación, tales como activar/desactivar la protección del equipo, modificar los parámetros para Resguardo y Cuarentena y reporte.

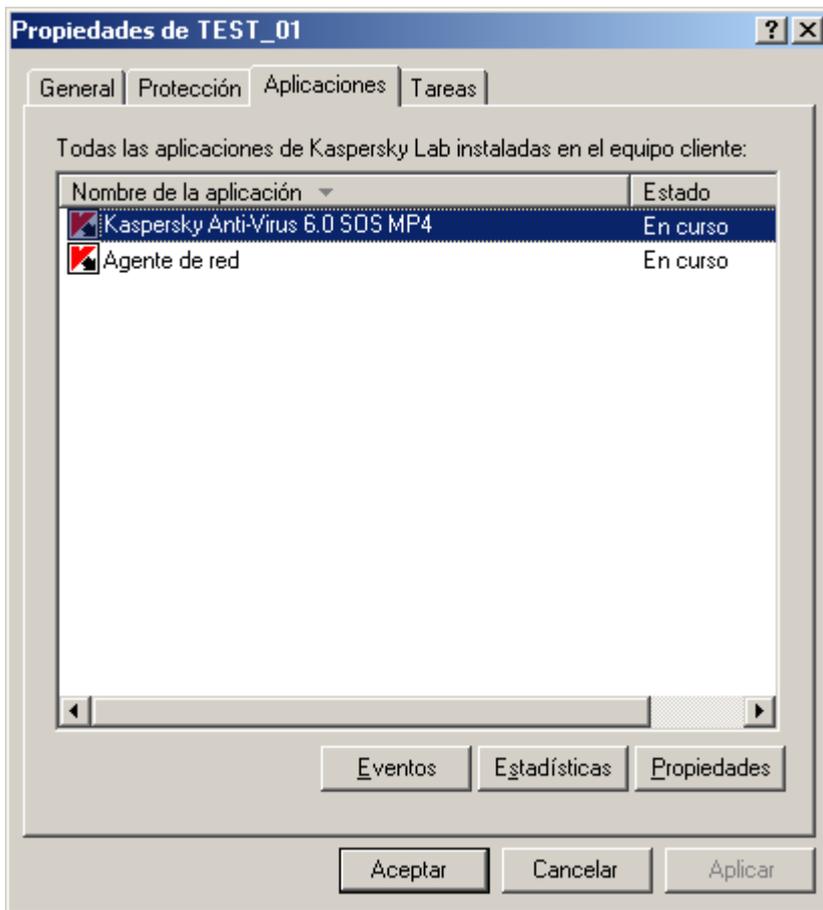


Figura 12. Ventana de propiedades del equipo del cliente. La pestaña **Aplicaciones**

➤ Para administrar los parámetros de la *por favor haga lo siguiente:*

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. Seleccione la carpeta **Equipos administrados** con el nombre del grupo que incluye el equipo del cliente.
3. En el grupo seleccionado, abra la carpeta **Equipos del cliente** y seleccione el equipo para el cual desea modificar los parámetros aplicación.
4. Seleccione el comando **Propiedades** del menú contextual o el elemento correspondiente del menú **Acción** para abrir la ventana de propiedades del equipo del cliente.
5. La pestaña **Aplicaciones** en la ventana propiedades del equipo del cliente muestra la lista completa de las aplicaciones de Kaspersky Lab instaladas en el equipo del cliente. Seleccione la aplicación **Kaspersky Anti-Virus 6.0 SOS MP4**.

Existen controles bajo la lista de aplicaciones que puede utilizar para:

- ver la lista de eventos en la operación aplicación que han ocurrido en el equipo del cliente y han sido registrados en el Servidor de Administración;
- ver estadísticas actuales en la operación aplicación;
- modificar parámetros de la aplicación (ver página [95](#)).

INICIAR Y DETENER LA APLICACIÓN

Kaspersky Anti-Virus 6.0 se instala e inicia en los equipos de clientes remotos desde la ventana de propiedades de la aplicación (ver figura abajo).

En la parte superior de la ventana, encontrará el nombre de la aplicación instalada, información sobre la versión, la fecha de instalación, su estado (si la aplicación se ejecuta o detiene en el equipo local), y la información sobre el estado de la base de datos de la firma de amenaza.

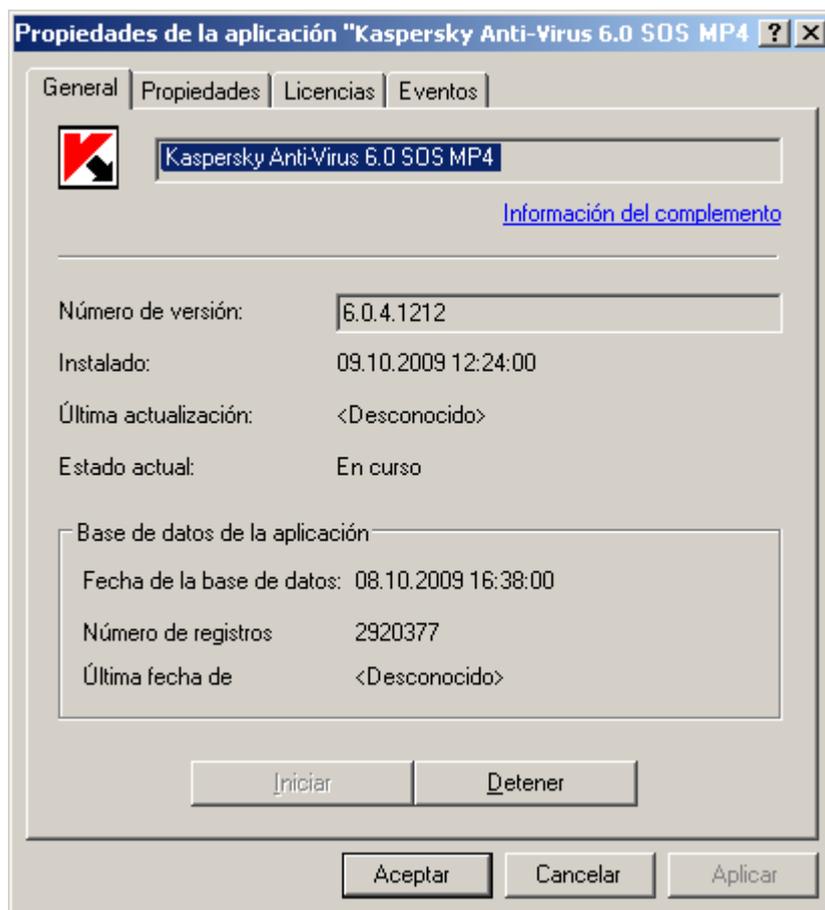


Figura 13. Ventana de propiedades de la aplicación. La pestaña **General**

- ➔ Para detener o iniciar la aplicación en un equipo remoto, por favor haga lo siguiente:
 1. Abra la ventana de propiedades para el equipo del cliente (ver página 92) en la pestaña **Aplicaciones**.
 2. Seleccione **Kaspersky Anti-Virus 6.0 SOS MP4** de la lista de aplicaciones y haga click en el botón **Propiedades**.
 3. En la ventana propiedades de la aplicación que se abrirá, en la pestaña **General**, haga click en el botón **Detener** para detener la aplicación o el botón **Iniciar** para iniciarla.

CONFIGURAR LOS PARÁMETROS DE LA APLICACIÓN

Usted puede ver y editar parámetros de la aplicación en la ventana de propiedades de la aplicación en la pestaña **Propiedades** (ver figura abajo). Las otras pestañas son estándar para la aplicación de Kaspersky Administration Kit y están cubiertas en más detalles en la Guía de Referencia.

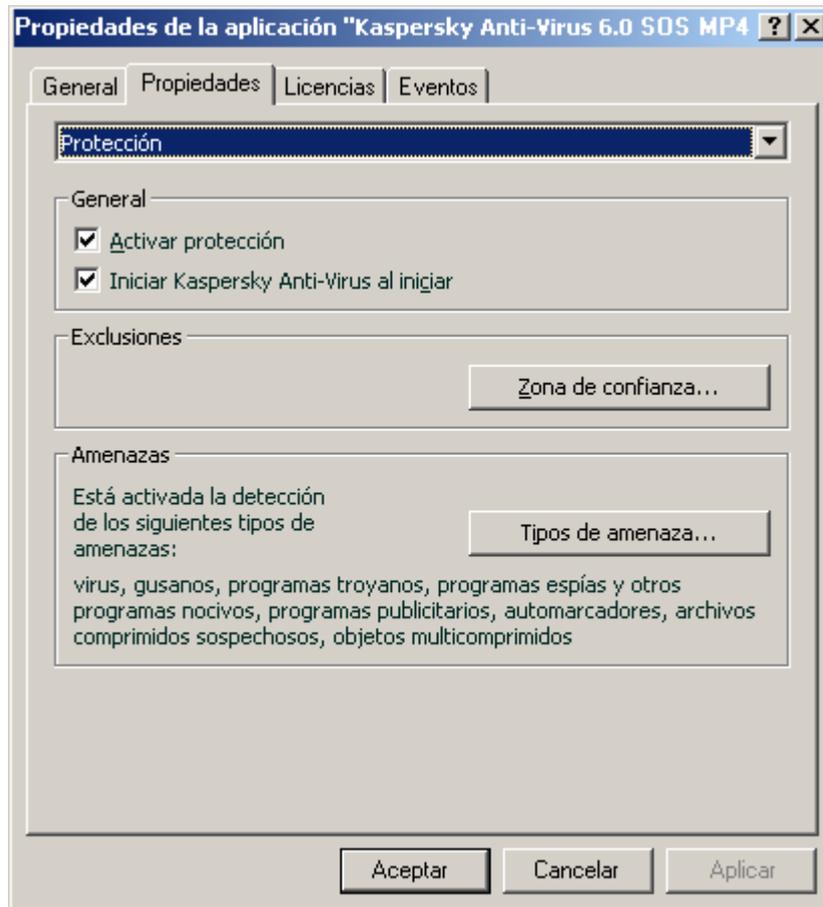


Figura 14. Ventana de propiedades de la aplicación. La pestaña **Propiedades**

Si para la aplicación se ha creado una política (ver página [104](#)) que evita que algunos parámetros sean remodificados, no podrán ser cambiados cuando se configura la aplicación.

➤ Para ver y editar la aplicación por favor haga lo siguiente:

1. Abra la ventana de propiedades para el equipo del cliente (ver página [92](#)) en la pestaña **Aplicaciones**.
2. Seleccione **Kaspersky Anti-Virus 6.0 SOS MP4** de la lista de aplicaciones y haga click en el botón **Propiedades**.
3. En la ventana de propiedades de la aplicación que se abrirá, en la pestaña **Propiedades** puede editar los parámetros generales de Kaspersky Anti-Virus, parámetros de almacenaje e informes, y parámetros de red. Para hacerlo, seleccione el valor requerido del menú desplegable en la parte superior de la ventana, y edite los parámetros.

VER TAMBIÉN

Lanzar la aplicación en el inicio del sistema operativo de la aplicación58

Selección de las categorías de amenazas detectables59

Crear una zona de confianza59

Configurar notificaciones por correo67

Configurar reportes69

Configurar cuarentena y resguardo72

Configurar parámetros específicos96

Crear una regla de exclusión60

Exportar / importar reglas de exclusión62

CONFIGURAR PARÁMETROS ESPECÍFICOS

Cuando administra Kaspersky Anti-Virus a través de Kaspersky Administration Kit, usted puede activar/desactivar la interactividad, configurar la apariencia de la aplicación, y editar información en Soporte Técnico. Estos parámetros pueden ser editados en la ventana de propiedades de la aplicación (ver figura abajo).

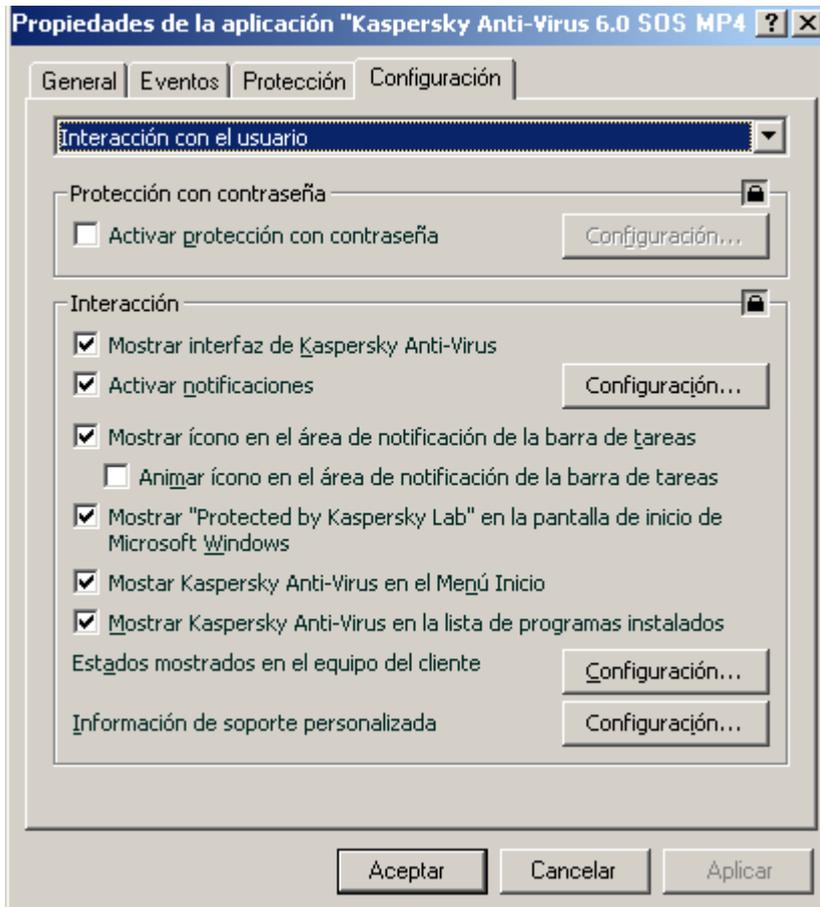


Figura 15. Ventana de propiedades de la aplicación. Configurar parámetros específicos

Para proteger con contraseña Kaspersky Anti-Virus, active la casilla **Activar protección con contraseña** en la ventana que se abrirá y haga click en el botón **Configuración**, e ingrese la contraseña y el área que cubrirá la restricción de acceso.

Para asegurar la protección contra quitas no autorizadas de una aplicación del equipo local, active la casilla **Activar protección contra desinstalación**. En la ventana que se abrirá al hacer click en el botón **Configuración**, ingrese una contraseña para desinstalar y confirmarlo.

Para proteger con contraseña Kaspersky Anti-Virus, active la casilla **Activar protección con contraseña** en la ventana que se abrirá y haga click en el botón **Configuración**, e ingrese la contraseña y el área que cubrirá la restricción de acceso.

Para asegurar la protección contra quitas no autorizadas de una aplicación del equipo local, active la casilla **Activar protección contra desinstalación**. En la ventana que se abrirá al hacer click en el botón **Configuración**, ingrese una contraseña para desinstalar y confirmarlo.

En la sección **Interacción**, puede especificar los parámetros de interacción del usuario con la interfaz de Kaspersky Anti-Virus:

- Si la casilla **Desactivar interacción** está desactivada, un usuario que trabaja en un equipo remoto, verá el ícono de Kaspersky Anti-Virus y los mensajes emergentes, y tendrá la posibilidad de tomar decisiones sobre acciones subsiguientes en las ventanas de notificación que informen acerca de un evento. Para desactivar el modo interactivo de funcionamiento de la aplicación, active la casilla. Si hay necesidad de ocultar la presencia de la aplicación del usuario, active también la casilla **Ocultar la aplicación instalada**.
- En la ventana **Ver** que se abrirá al hacer click en el botón **Configuración**, puede editar la información sobre el soporte técnico al usuario que se muestra en la ventana **Soporte** de Kaspersky Anti-Virus.

Para cambiar la información, en el campo superior ingrese el texto actual en el soporte provisto. En el campo inferior, puede editar los hipervínculos que son mostrados en la sección **Enlaces útiles** de la ventana **Soporte** que se abrirá al clickear el enlace **Soporte** en la ventana principal de Kaspersky Anti-Virus.

Edite la lista utilizando los botones **Agregar**, **Editar**, **Eliminar**. Kaspersky Anti-Virus agregará un nuevo enlace al tope de la lista. Para cambiar el orden de los enlaces en la lista, utilice los botones **Subir** y **Bajar**.

Si la ventana no contiene ningún dato, la información por defecto respecto del soporte técnico no puede editarse.

En la sección **Estados de la aplicación**, puede especificar los estados de la aplicación, que serán mostrados en la ventana principal de Kaspersky Anti-Virus. Para hacerlo, haga click en el botón **Configuración** y active las casillas para los estados requeridos en la ventana que se abrirá. Puede especificar los períodos de vigilancia de las bases de datos de la aplicación en la misma ventana.

En la sección **Ver**, puede editar la configuración para el modo interactivo de Kaspersky Anti-Virus en un equipo remoto: la animación del ícono de Kaspersky Anti-Virus en la bandeja del sistema, emisión de notificaciones sobre eventos que ocurren en la aplicación (por ejemplo, detección de objetos peligrosos).

Si para la aplicación se ha creado una política (ver página 104) que evita que algunos parámetros sean remodificados, no podrán ser cambiados cuando se configura la aplicación.

➔ Para ver y editar los parámetros avanzados de la aplicación, por favor haga lo siguiente:

1. Abrir ventana de propiedades del equipo del cliente (ver página 92) en la pestaña **Aplicaciones**.
2. Seleccione **Kaspersky Anti-Virus 6.0 SOS MP4** y haga click en el botón **Propiedades**.
3. En la ventana de propiedades de la aplicación que se abrirá, en la pestaña **Propiedades**, seleccione el elemento **Interacción con el usuario** de la lista desplegable, y edite los parámetros.

ADMINISTRAR TAREAS

Esta sección incluye información sobre tareas de gestión para Kaspersky Anti-Virus. Para más detalles sobre la gestión de tareas a través de Kaspersky Administration Kit, consulte la Guía del Administrador para ese producto.

Se crea una lista de tareas del sistema para cada equipo de red cuando se instala la aplicación. Esta lista incluye tareas de análisis (Escaneo completo, Escaneo rápido) y tareas de actualización (actualizaciones de bases de datos y módulos de programa, actualización de reversiones).

Usted puede administrar la programación para las tareas del sistema y editar sus parámetros. Estas tareas no pueden ser eliminadas.

También puede crear sus propias tareas (ver página 99), como tareas de análisis, actualizaciones de aplicaciones y reversiones de actualización, y tareas de instalación de archivos llave.

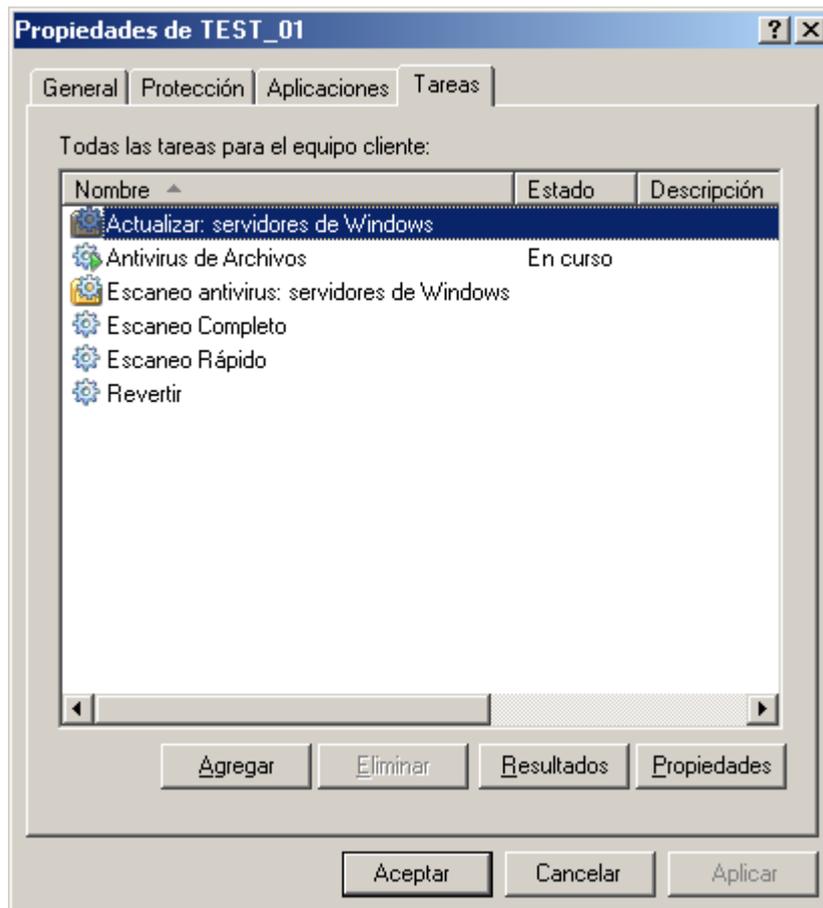


Figura 16. Ventana de propiedades del equipo del cliente. La pestaña **Tareas**

➔ Para abrir la lista de tareas creada para un equipo del cliente, por favor haga lo siguiente:

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. Seleccione la carpeta **Equipos administrados** con el nombre del grupo que incluye el equipo del cliente.
3. En el grupo seleccionado, abra la carpeta **Equipos del cliente** y seleccione el equipo para el cual desea modificar los parámetros de la aplicación.
4. Seleccione el comando **Propiedades** del menú contextual o el elemento correspondiente del menú **Acción** para abrir la ventana de propiedades del equipo del cliente.

5. En la ventana de propiedades del equipo del cliente, seleccione la pestaña **Tareas**. Aquí encontrará la lista completa de tareas creada para el equipo del cliente.

INICIO Y DETENCIÓN DE TAREAS

Las tareas se inician en el equipo del cliente sólo si se está ejecutando la aplicación correspondiente (ver página [93](#)). Si la aplicación se detiene, terminarán todas las tareas que se están ejecutando.

Las tareas se inician y detienen automáticamente, de acuerdo con una programación, o manualmente usando comandos del menú contextual y de la ventana de Vista de los Parámetros de Tareas. También puede pausar tareas y reanudarlas.

➔ *Para iniciar/detener/pausar/reanudar una tarea manualmente, por favor haga lo siguiente:*

1. Abra ventana de propiedades del equipo del cliente (ver página [98](#)) en la pestaña **Tareas**.
2. Seleccione la tarea requerida y abra el menú contextual. Seleccione el ítem **Inicio** para iniciar la tarea o el ítem **Detener** para detenerla. También puede utilizar los elementos correspondientes en el menú **Acción**.

Usted no puede pausar o reanudar una tarea del menú contextual.

o

Seleccionar la tarea requerida de la lista y haga click en el botón **Propiedades**. No puede utilizar los botones en la pestaña **General** en la ventana de propiedades de tareas que se abrirá para iniciar, detener, pausar, o reanudar una tarea.

CREAR TAREAS

Cuando trabaja con la aplicación a través de Kaspersky Administration Kit, usted puede crear los siguientes tipos de tareas:

- tareas locales definidas para equipos de clientes individuales;
- tareas grupales definidas para equipos de clientes que pertenecen a los grupos de administración;
- tareas para grupos de equipos que están definidas para equipos fuera del grupo de administración;
- las tareas de Kaspersky Administration Kit son específicas para Actualizar el Servidor: tareas de descarga de actualizaciones, tareas de resguardo, y tareas de envío de reportes.

Las tareas de grupo del equipo se realizan sólo en el grupo de equipos seleccionado. Si los nuevos equipos de clientes se agregan a un grupo con equipos para los cuales se ha creado una tarea de instalación remota, esta tarea no se ejecutará para ellos. Usted deberá crear una nueva tarea o realizar los cambios adecuados en los parámetros de la tarea existente.

Puede realizar las siguientes acciones en las tareas:

- especificar los parámetros de la tareas;
- vigilar la ejecución de las tareas;
- copiar y mover las tareas de un grupo a otro, y también eliminarlas utilizando los comandos estándar **Copiar/Pegar**, **Cortar/Pegar**, **Eliminar** del menú contextual, o los mismos comandos desde el menú **Acción**;
- importar y exportar tareas.

Consultar la Guía de Referencia de Kaspersky Administration Kit para más información sobre el trabajo con tareas.

➤ *Para crear una tarea local, por favor haga lo siguiente:*

1. Abrir la ventana de propiedades del equipo del cliente (ver página [98](#)) en la pestaña **Tareas**.
2. Haga click en el botón **Agregar**.
3. El Nuevo Asistente de Tareas se iniciará luego (ver página [100](#)). Por favor siga sus instrucciones.

➤ *Para crear una tarea de grupo, por favor haga lo siguiente:*

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. En la carpeta **Equipos administrados**, abra la carpeta con el nombre del grupo requerido.
3. En el grupo que ha seleccionado, abra la carpeta **Tareas de grupo**, donde encontrará todas las tareas creadas para ese grupo.
4. Abra el Asistente de Tarea Nueva haciendo click en el enlace **Crear una nueva tarea** en la barra de tareas. Los detalles de crear tareas de grupo son cubiertos en la Guía de Referencia de Kaspersky Administration Kit.

➤ *Para crear una tarea para un grupo de equipos (una tarea de Kaspersky Administration Kit), por favor haga lo siguiente:*

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. Seleccione la carpeta **Tareas para equipos específicos (tareas de Kaspersky Administration Kit)**.
3. Abra el Asistente de Tarea Nueva haciendo click en el enlace **Crear una nueva tarea** en la barra de tareas. Los detalles de crear tareas de Kaspersky Administration Kit y tareas para grupos de equipos son cubiertas en la Guía de Referencia de Kaspersky Administration Kit.

ASISTENTE DE TAREAS LOCAL

El Asistente de Tareas Local se inicia cuando selecciona los comandos correspondientes del menú contextual para el equipo del cliente o de la ventana de propiedades para ese equipo.

Este asistente consiste en una serie de casillas (pasos) que se navegan utilizando los botones **Atrás** y **Siguiente**; para cerrar el asistente una vez que se ha completado el trabajo, utilice el botón **Finalizar**. Para cancelar el asistente en cualquier momento, pulse el botón **Cancelar**.

PASO 1. INGRESAR DATOS GENERALES EN LA TAREA

La primera ventana del asistente es introductoria: todo lo que debe ingresar aquí es el nombre de la tarea (el campo **Nombre**).

PASO 2. SELECCIONAR UNA APLICACIÓN Y TIPO DE TAREA

En este paso, deberá especificar la aplicación para la cual se crea la tarea (Kaspersky Anti-Virus 6.0 SOS MP4, o Agente de Red). También deberá seleccionar el tipo de tarea. Las posibles tareas para Kaspersky Anti-Virus 6.0 son:

- *Análisis en busca de virus* – tarea de análisis de virus de las áreas especificadas por el usuario.
- *Actualizar* – recupera y aplica los paquetes de actualización para la aplicación.
- *Actualizar Reversión* – revierte a la última actualización de la aplicación.

- *Instalación del archivo llave* - instalación de un archivo llave para una nueva licencia según sea necesario para operar la aplicación.

PASO 3. CONFIGURAR EL TIPO DE TAREA SELECCIONADA

Dependiendo del tipo de tarea seleccionada en el paso anterior, los contenidos de la ventana de parámetros pueden variar.

Las tareas de análisis de virus requiere que especifique la acción que realizará Kaspersky Anti-Virus si detecta un objeto nocivo (ver página [38](#)) y requiere que cree una lista de objetos a analizar (ver página [37](#)).

Para tareas de actualización de la base de datos y el módulo de aplicación, deberá especificar la fuente que será utilizada para descargar actualizaciones (ver página [48](#)). La fuente de actualización predeterminada es el servidor de actualización de Kaspersky Administration Kit.

Las tareas de reversión de actualización no tienen parámetros específicos.

Para tareas de instalación de llave de licencia, especifique la ruta al archivo llave con el botón **Examinar**. Para agregar un archivo como una llave de licencia para una licencia adicional, active la casilla correspondiente . La llave de licencia adicional tendrá efecto al vencimiento de la llave de licencia activa.

La información sobre la licencia especificada (número de licencia, tipo y fecha de vencimiento) se muestra en el campo de abajo.

PASO 4. CONFIGURAR UNA PROGRAMACIÓN

Luego de configurar las tareas, se le ofrecerá configurar la programación automática de ejecución de tarea.

Para hacerlo, seleccione la frecuencia para la ejecución de la tarea desde el menú desplegable en la ventana de parámetros de programación y modifique los parámetros de programación en la parte inferior de la ventana.

PASO 5. COMPLETAR LA CREACIÓN DE LA TAREA

La última ventana del asistente le informará que ha creado la tarea en forma exitosa.

CONFIGURAR TAREAS

La configuración de tareas de aplicación a través de la interfaz Kaspersky Administration Kit es similar a la configuración a través de una interfaz local de Kaspersky Anti-Virus, a excepción de los parámetros que se editan individualmente para cada usuario, como es el caso de tareas de análisis que se ejecutan según programación, o parámetros específicos para Kaspersky Administration Kit, tales como parámetros que permiten/bloquean la administración de tareas de análisis locales por los usuarios.

Si para la aplicación se ha creado una política (ver página [104](#)) que evita que algunos parámetros sean remodificados, no podrán ser cambiados cuando se configura la aplicación.

Todas las tareas en la ventana de propiedades de tareas al lado de la pestaña **Propiedades** (ver figura abajo) son estándar para Kaspersky Administration Kit y están cubiertas con más detalles en la Guía de Referencia. La pestaña **Propiedades** contiene parámetros específicos para Kaspersky Anti-Virus. Los contenidos de esta pestaña varían dependiendo del tipo de tarea seleccionada.

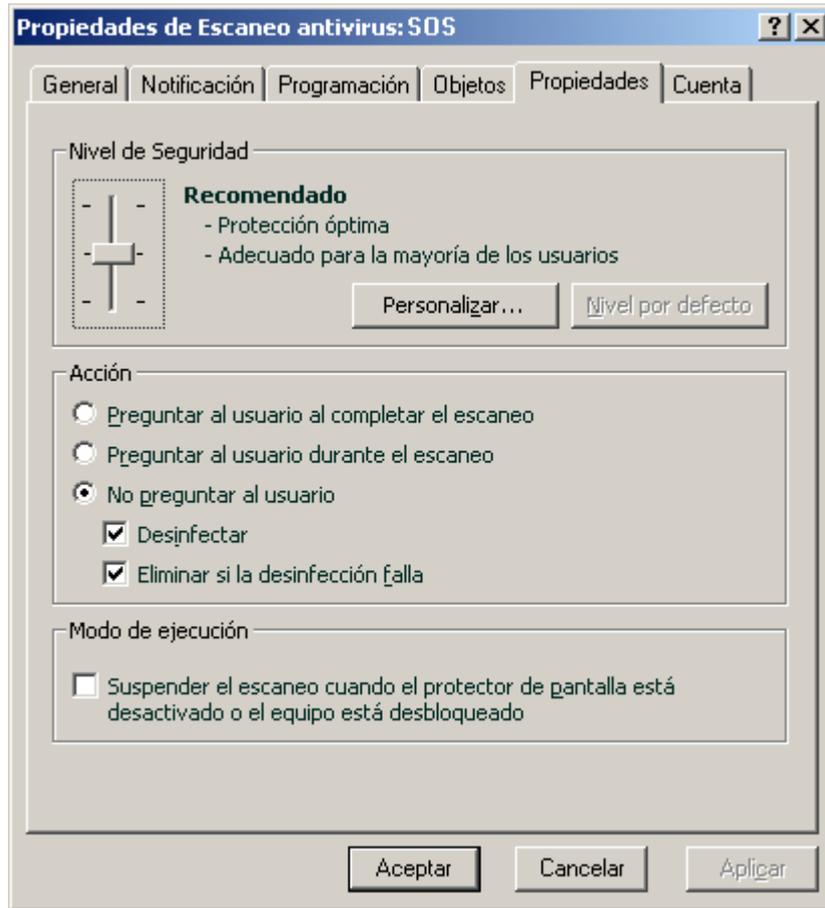


Figura 17. Ventana de propiedades de tareas. La pestaña **Propiedades**

➤ Para ver y editar las tareas locales, por favor haga lo siguiente:

1. Abra la ventana de propiedades del equipo del cliente (ver página [98](#)) en la pestaña **Tareas**.
2. Seleccione una tarea de la lista y haga click en el botón **Propiedades**. Como resultado, se abrirá la ventana de parámetros de tareas.

➤ Para ver las tareas de grupo, por favor haga lo siguiente:

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. En la carpeta **Equipos administrados**, abra la carpeta con el nombre del grupo requerido.
3. En el grupo que ha seleccionado, abra la carpeta **Tareas de grupo**, donde encontrará todas las tareas creadas para ese grupo.
4. Seleccione la tarea requerida del árbol de consola para ver y editar sus propiedades.

La barra de tareas mostrará información comprensiva de la tarea y los enlaces para administrar la ejecución de tareas y editar sus parámetros. Los detalles de crear tareas de grupo son descriptos en la Guía de Referencia de Kaspersky Administration Kit.

➤ *Para ver tareas para un grupo de equipos (una tarea de Kaspersky Administration Kit), por favor haga lo siguiente:*

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. Seleccione la carpeta **Tareas para equipos específicos (tareas de Kaspersky Administration Kit)**.
3. Seleccione la tarea requerida del árbol de consola para ver y editar sus propiedades.

La barra de tareas mostrará información comprensiva de la tarea y los enlaces para administrar la ejecución de tareas y editar sus parámetros. Los detalles de las tareas de Kaspersky Administration Kit y tareas para grupos de equipos se pueden encontrar en la Guía de Referencia de Kaspersky Administration Kit.

ADMINISTRAR POLÍTICAS

El establecimiento de políticas le permite aplicar una aplicación universal y parámetros de tareas para los equipos de clientes que pertenecen a un mismo grupo de administración.

Esta sección incluye información sobre la creación y configuración de políticas para Kaspersky Anti-Virus 6.0 SOS MP4. Para más detalles sobre el concepto de políticas de administración a través de Kaspersky Administration Kit, vea la Guía del Administrador para la aplicación.

Al crear y configurar una política, puede bloquear total o parcialmente la edición de parámetros en las políticas para subgrupos, configuración de tareas, y configuración de la aplicación. Para ello, haga click en el botón . Deberá cambiar a  para los parámetros bloqueados.

➤ *Para abrir la lista de políticas para Kaspersky Anti-Virus, por favor haga lo siguiente:*

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. Seleccione la carpeta **Equipos administrados** con el nombre del grupo que incluye el equipo del cliente.
3. En el grupo que ha seleccionado, abra la carpeta **Políticas**, donde encontrará todas las tareas creadas para ese grupo.

CREAR POLÍTICAS

Cuando trabaja con Kaspersky Anti-Virus a través de Kaspersky Administration Kit, podrá crear los siguientes tipos de políticas:

Puede realizar las siguientes acciones en las políticas:

- configurar políticas;
- copiar y mover políticas de un grupo a otro, y también eliminarlas utilizando los comandos estándar **Copiar/Pegar**, **Cortar/Pegar**, **Eliminar** del menú contextual, o los mismos comandos desde el menú **Acción**;
- importar y exportar parámetros de políticas.

El trabajo con políticas está cubierto más detalladamente en la Guía de Referencia de Kaspersky Administration Kit.

➤ *Para crear una política, por favor haga lo siguiente:*

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. En la carpeta **Equipos administrados**, abra la carpeta con el nombre del grupo requerido.
3. En el grupo que ha seleccionado, abra la carpeta **Políticas**, donde encontrará todas las tareas creadas para ese grupo.

- Abra el Asistente de Tarea Nueva haciendo click en el enlace **Crear una nueva política** en la barra de tareas.
- El Asistente de Tarea Nueva luego se iniciará en la ventana que se abrirá (ver página [104](#)): y siga sus instrucciones.

ASISTENTE DE CREACIÓN DE POLÍTICA

El Asistente de Política puede iniciarse seleccionando la acción correspondiente del menú contextual de la carpeta **Políticas** del grupo de administración requerido, o haciendo click en el enlace en el panel de resultados (para las carpetas **Políticas**).

Este asistente consiste en una serie de casillas (pasos) que se navegan utilizando los botones **Atrás** y **Siguiente**; para cerrar el asistente una vez que se ha completado el trabajo, utilice el botón **Finalizar**. Para cancelar el asistente en cualquier momento, pulse el botón **Cancelar**.

PASO 1. INGRESAR DATOS GENERALES EN LA POLÍTICA

Las primeras ventanas del asistente son ventanas de bienvenida. Aquí deberá especificar el nombre de la política (el campo **Nombre**) y seleccione **Kaspersky Anti-Virus 6.0 SOS MP4** del menú desplegable **Nombre de la aplicación**.

Si ejecuta el Asistente de Creación de Política del nodo **Políticas** de la barra de tareas (usando la **Crear una política para Kaspersky Anti-Virus SOS MP4**), no podrá seleccionar una aplicación.

Si desea crear una política basada en los parámetros de una política existente creada para la versión anterior de la aplicación, active la casilla **Tome los parámetros desde una política existente** y seleccione la política cuyos parámetros deberán ser utilizados en la nueva política. Para seleccionar una política, haga click en el botón **Seleccionar**, que abrirá la lista de políticas existentes que podrá utilizar cuando crea una nueva.

PASO 2. SELECCIONAR EL ESTADO DE LA POLÍTICA

En esta ventana, se le ofrecerá especificar el estado de la política luego de su creación, seleccionando una de las siguientes opciones: política activa o política inactiva. Consultar la Guía de Referencia de Kaspersky Administration Kit para más detalles sobre los estados de las políticas.

Se podrán crear varias políticas para una aplicación única en un grupo, pero sólo una de ellas puede ser la política actual (activa).

PASO 3. IMPORTAR LOS PARÁMETROS DE LA APLICACIÓN

Si tiene un archivo con los parámetros de la aplicación guardado con anterioridad, puede especificar la ruta del mismo utilizando el botón **Cargar**; de aquí en adelante las ventanas asistentes le mostrarán los parámetros importados.

PASO 4. CONFIGURAR LA PROTECCIÓN

En este paso, puede activar (desactivar), y configurar los parámetros de la aplicación que serán utilizados en la política.

La aplicación está activada por defecto. Para desactivar la aplicación, desactive la casilla **Protección**. Para ajustar la aplicación, active la casilla **Protección** y presione el botón **Configurar**.

PASO 5. CONFIGURAR PROTECCIÓN CON CONTRASEÑA

En esta ventana del asistente, se le ofrecerá configurar la protección con contraseña aplicada a las operaciones con la aplicación y a la desinstalación.

PASO 6. CONFIGURAR LA ZONA DE CONFIANZA

En esta ventana del asistente, se le ofrecerá configurar los parámetros de la zona de confianza: agregar el software utilizado para la administración de la red para lista de aplicaciones de confianza, y excluir del análisis varios tipos de archivos.

PASO 7. CONFIGURAR LA INTERACCIÓN CON EL USUARIO

En este paso, puede especificar los parámetros para la interacción entre el usuario y Kaspersky Anti-Virus:

- mostrar la interfaz de la aplicación en un equipo remoto;
- notificar al usuario sobre los eventos;
- mostrar el ícono de la aplicación en el área de notificación de la barra de tareas y animarlo;
- mostrar "Protegido por Kaspersky Lab" en pantalla de inicio de Microsoft Windows;
- mostrar la aplicación en el Menú Inicio;
- mostrar la aplicación en la lista de aplicaciones instaladas.

PASO 8. COMPLETAR LA POLÍTICA DE CREACIÓN

La última ventana del asistente le informará que ha creado la política en forma exitosa.

Una vez que se cierra el asistente, la política para la aplicación se agregará a la carpeta **Políticas** del grupo correspondiente, volviéndose visibles en el árbol de consola.

Usted puede editar los parámetros de la política creada y establecer restricciones sobre la modificación de sus parámetros utilizando los botones  y  para cada grupo de parámetros. Si se muestra el ícono  el usuario del equipo cliente no podrá editar los parámetros. Si se muestra el ícono  el usuario podrá editar los parámetros. La política se aplicará a los equipos del cliente la primera vez que los clientes sincronicen con el servidor.

CONFIGURAR LA POLÍTICA

En la etapa de edición, puede modificar la política y bloquear la modificación de los parámetros en las políticas de grupo anidadas, y en la aplicación y parámetros de tareas. Los parámetros de las políticas pueden ser editados en la ventana de propiedades de la política (ver figura abajo).

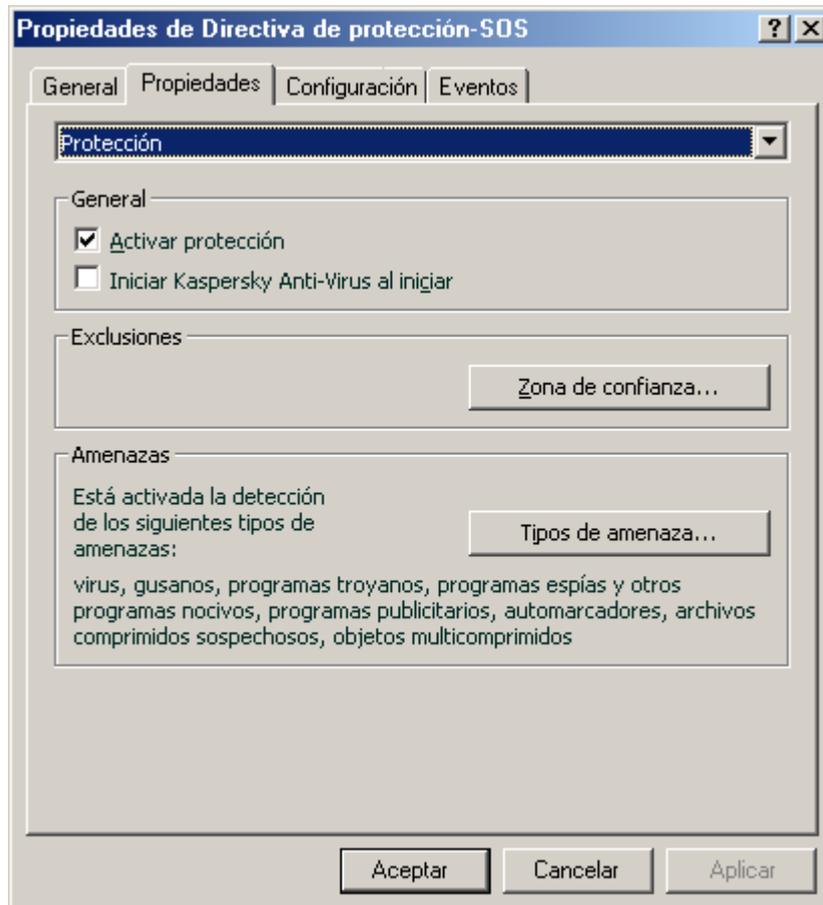


Figura 18. Ventana de propiedades de la política. La pestaña **Protección**

Todas las pestañas, a excepción de las pestañas **Protección** y **Parámetros**, son estándar para Kaspersky Administration Kit. Están cubiertas con más detalles en la Guía del Administrador.

Los parámetros de las políticas para Kaspersky Anti-Virus 6.0 incluyen parámetros de la aplicación (ver página 95) y parámetros de tareas. La pestaña de **Parámetros** muestra los parámetros de la aplicación y la pestaña **Protección** muestra los parámetros de la tarea.

Para editar los parámetros, seleccione el valor requerido del menú desplegable en la parte superior de la ventana, y fíjelos.

➔ Para ver y editar los parámetros de las políticas, por favor haga lo siguiente:

1. Abra la Consola de Administración de Kaspersky Administration Kit.
2. En la carpeta **Equipos administrados**, abra la carpeta con el nombre del grupo requerido.
3. En el grupo que ha seleccionado, abra la carpeta **Políticas**, donde encontrará todas las tareas creadas para ese grupo.
4. Seleccione la política requerida del árbol de consola para ver y editar sus propiedades.

5. La barra de tareas mostrará información comprensiva de la política y los enlaces para administrar el estado de la política y editar sus parámetros.

o

Abra el menú contextual para la política seleccionada y utilice el elemento **Propiedades** para abrir la ventana de parámetros de la política de Kaspersky Anti-Virus.

Las particularidades de trabajar con políticas se pueden encontrar en la Guía de Referencia de Kaspersky Administration Kit.

UTILIZAR CÓDIGO DE UN TERCERO

En la creación de Kaspersky Anti-Virus se ha utilizado código de terceros.

EN ESTA SECCIÓN

Biblioteca Boost 1.30.....	109
Biblioteca LZMA SDK 4.40, 4.43	109
Biblioteca Windows Template Library (WTL 7.5).....	109
Biblioteca Windows Installer XML (WiX-2.0)	110
Biblioteca ZIP-2.31	113
Biblioteca ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3.....	114
Biblioteca UNZIP-5.51	114
Biblioteca LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12	115
Biblioteca LIBJPEG-6B.....	117
Biblioteca LIBUNGIF-4.1.4	118
Biblioteca MD5 MESSAGE-DIGEST ALGORITHM-REV. 2	118
Biblioteca MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004	118
Biblioteca INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999.....	119
Biblioteca CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004.....	119
Biblioteca COOL OWNER DRAWN MENUS-V. 2.4, 2.63 Por Brent Corkum.....	119
Biblioteca PLATFORM INDEPENDENT IMAGE CLASS.....	120
Biblioteca FLEX PARSER (FLEXLEXER)-V. 1993.....	120
Biblioteca ENSURECLEANUP, SWMRG, LAYOUT-V. 2000	120
Biblioteca STDSTRING- V. 1999.....	121
T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006.....	121
Biblioteca NTSERVICE- V. 1997	122
Biblioteca SHA-1-1.2	122
Biblioteca COCOA SAMPLE CODE- V. 18.07.2007	122
Otra información.....	123

BIBLIOTECA BOOST 1.30

Al crear la aplicación se ha utilizado la biblioteca Boost 1.30. Copyright (C) 2003, Christof Meerwald.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTECA LZMA SDK 4.40, 4.43

Al crear la aplicación se ha utilizado la biblioteca LZMA SDK 4.40, 4.43. Copyright (C) 1999-2006, Igor Pavlov.

BIBLIOTECA WINDOWS TEMPLATE LIBRARY (WTL 7.5)

Al crear la aplicación se ha utilizado Windows Template Library 7.5. Copyright (C) 2006, Microsoft Corporation.

Microsoft Public License (Ms-PL)

Published: 12 de octubre de 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definiciones

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

BIBLIOTECA WINDOWS INSTALLER XML (WIX-2.0)

Al crear la aplicación se ha utilizado la biblioteca de herramientas de Windows Installer XML (WiX). Copyright (C) 2009, Microsoft Corporation.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a. in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b. in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTECA ZIP-2.31

Al crear la aplicación se ha utilizado la biblioteca ZIP-2.31. Copyright (C) 1990-2005, Info-ZIP.

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTECA ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3

Al crear la aplicación se ha utilizado la biblioteca ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3. Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

BIBLIOTECA UNZIP-5.51

Al crear la aplicación, se utilizó la biblioteca UNZIP-5.51. Copyright (c) 1990-2004 Info-ZIP.

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborh, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being

Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTECA LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

Al crear la aplicación, se utilizó la biblioteca LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, 15 de agosto de 2004, through 1.2.39, 13 de agosto de 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, 1 de julio de 2000, through 1.2.5 - 3 de octubre de 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, 20 de marzo de 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

13 de agosto de 2009

BIBLIOTECA LIBJPEG-6B

Al crear la aplicación, se utilizó la biblioteca LIBJPEG-6B. Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch,

sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead

by the usual distribution terms of the Free Software Foundation; principally,

that you must include source code if you redistribute it. (See the file

ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part

of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

BIBLIOTECA LIBUNGIF-4.1.4

Al crear la aplicación, se utilizó la biblioteca LIBUNGIF-4.1.4. Copyright (C) 1997, Eric S. Raymond.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTECA MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

Al crear la aplicación se ha utilizado la biblioteca MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.

BIBLIOTECA MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

Al crear la aplicación se ha utilizado la biblioteca MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.

BIBLIOTECA INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

Al crear la aplicación se ha utilizado la biblioteca INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999. Copyright (C) 1991-2, RSA Data Security, Inc.

RSA's MD5 disclaimer

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

BIBLIOTECA CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

Al crear la aplicación se ha utilizado la biblioteca CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004. Copyright 2001-2004 Unicode, Inc.

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

BIBLIOTECA COOL OWNER DRAWN MENUS-V. 2.4, 2.63 POR BRENT CORKUM

Al crear la aplicación se ha utilizado la biblioteca COOL OWNER DRAWN MENUS-V. 2.4, 2.63 Por Brent Corkum.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware, Shareware, Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

BIBLIOTECA PLATFORM INDEPENDENT IMAGE CLASS

Al crear la aplicación se ha utilizado la biblioteca PLATFORM INDEPENDENT IMAGE CLASS. Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx).

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BIBLIOTECA FLEX PARSER (FLEXLEXER)-V. 1993

Al crear la aplicación se ha utilizado la biblioteca FLEX PARSER (FLEXLEXER)-V. 1993. Copyright (c) 1993 The Regents of the University of California.

This code is derived from software contributed to Berkeley by Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: ``This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

BIBLIOTECA ENSURECLEANUP, SWMRG, LAYOUT-V. 2000

Al crear la aplicación, se utilizó la biblioteca ENSURECLEANUP, SWMRG, LAYOUT-V. 2000. Copyright (C) 2009, Microsoft Corporation.

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License <http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL>.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

BIBLIOTECA STDSTRING- V. 1999

Al crear la aplicación se ha utilizado la biblioteca STDSTRING- V. 1999. Copyright (C) 1999, Joseph M. O'Leary.

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes your \$30 billion dollar satellite explode in orbit. If you redistribute it in any form, I'd appreciate it if you would leave this notice here.

T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

Al crear la aplicación se ha utilizado la biblioteca T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006. Copyright (C) 2003-2006, Alberto Demichelis.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BIBLIOTECA NTSERVICE- V. 1997

Al crear la aplicación, se utilizó la biblioteca NTSERVICE- V. 1997. Copyright (C) 1997 by Joerg Koenig and the ADG mbH, Mannheim, Germany.

Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "///!! TCW MOD"

BIBLIOTECA SHA-1-1.2

Al crear la aplicación, se utilizó la biblioteca SHA-1-1.2. Copyright (C) 2001, The Internet Society.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

BIBLIOTECA COCOA SAMPLE CODE- V. 18.07.2007

Al crear la aplicación se ha utilizado la biblioteca Cocoa sample code- v. 18.07.2007. Copyright (C) 2007, Apple Inc.

Disclaimer: IMPORTANT: This Apple software is supplied to you by Apple Inc. ("Apple")

in consideration of your agreement to the following terms, and your use, installation, modification or redistribution of this Apple software constitutes acceptance of these terms. If you do not agree with these terms, please do not use, install, modify or redistribute this Apple software.

In consideration of your agreement to abide by the following terms, and subject to these terms, Apple grants you a personal, non – exclusive license, under Apple's copyrights in this original Apple software (the "Apple Software"), to use, reproduce, modify and redistribute the Apple Software, with or without modifications, in source and / or binary forms;

provided that if you redistribute the Apple Software in its entirety and without modifications, you must retain this notice and the following text and disclaimers in all such redistributions of the Apple Software. Neither the name, trademarks, service marks or logos of Apple Inc. may be used to endorse or promote products derived from the Apple Software without specific prior written permission from Apple. Except as expressly stated in this notice, no other rights or licenses, express or implied, are granted by Apple herein, including but not limited to any patent rights that may be infringed by your derivative works or by other works in which the Apple Software may be incorporated.

The Apple Software is provided by Apple on an "AS IS" basis.

APPLE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON - INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH YOUR PRODUCTS.

IN NO EVENT SHALL APPLE BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) ARISING IN ANY WAY OUT OF THE USE, REPRODUCTION, MODIFICATION AND / OR DISTRIBUTION OF THE APPLE SOFTWARE, HOWEVER CAUSED AND WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OTRA INFORMACIÓN

El Software puede incluir algunos programas de software que están bajo licencia (o sublicencias) al usuario bajo la Licencia Pública General (GPL, por sus siglas en inglés) de GNU u otras licencias de software libre similares, las cuales, entre otros derechos, permiten al usuario copiar, modificar y redistribuir ciertos programas o partes de los mismos, y tener acceso al código fuente (Software de Código Abierto). Si tales licencias exigieran, en relación a cualquier software que se distribuya a alguien en un formato binario ejecutable, que el código fuente también se ponga a disposición de aquellos usuarios, entonces el código podrá ponerse a disposición enviando una solicitud a source@kaspersky.com.

GLOSARIO

A

ACTUALIZACIONES DISPONIBLES

Es un conjunto de actualizaciones de los módulos de la aplicación Kaspersky Lab que incluye actualizaciones acumuladas por un período de tiempo y modificaciones en la estructura de la aplicación.

ACTUALIZACIONES URGENTES

Actualizaciones críticas de los módulos de la aplicación Kaspersky Lab.

ACTUALIZACIÓN

Es el procedimiento de reemplazar/agregar nuevos archivos (bases de datos o módulos para las aplicaciones) recolectados de los servidores de actualización de Kaspersky Lab.

ACTUALIZACIÓN DE BASES DE DATOS

Es una de las funciones realizadas por la aplicación Kaspersky Lab que permite mantener la protección actual. Al realizarla, las bases de datos son descargadas de los servidores de actualización de Kaspersky Lab al equipo y conectadas automáticamente a la aplicación.

ALMACENAMIENTO DE RESGUARDO

Una carpeta especial de almacenamiento para copias de datos del Servidor de Administración creado utilizando una utilidad de resguardo.

ANALIZADOR HEURÍSTICO

Esta tecnología se usa para detectar amenazas que no pueden detectar las bases de datos antivirus. Detecta objetos sospechosos de infectarse con virus desconocidos o con variantes de virus conocidos.

El analizador heurístico detecta hasta 92% de las amenazas. Este mecanismo es bastante efectivo y muy rara vez ocasiona falsas alarmas.

Los archivos detectados por el analizador heurístico se consideran sospechosos.

ANÁLISIS DEL ALMACENAMIENTO

Analizar el correo almacenado en el servidor de correo y los contenidos de las carpetas compartidas utilizando la última versión de la base de datos. El análisis se ejecuta en el fondo y puede ser ejecutado utilizando una programación o según demanda. Se analizan todas las carpetas compartidas y el almacenaje del buzón de correo. Se pueden detectar nuevos virus durante el análisis del cual no hay información en la base de datos en el momento de los análisis previos.

ANÁLISIS SEGÚN DEMANDA

El modo operativo de la aplicación de Kaspersky Lab que es iniciada por el usuario y puede direccionar cualquier archivo en el equipo.

APLICACIÓN INCOMPATIBLE

Es una aplicación antivirus de un tercero o una aplicación de Kaspersky Lab que no soporta la administración a través del Kit de Administración Kaspersky.

ARCHIVADOR

El archivo que "contiene" uno o más objetos, también puede ser un archivo comprimido.

ARCHIVO COMPRIMIDO

Es un archivador que contiene un programa descompresor e instrucciones para que el sistema operativo lo ejecute.

ARCHIVO LLAVE

Es un archivo de extensión .key, el cual es su "llave" personal", necesario para trabajar con la aplicación Kaspersky Lab. Un archivo llave está incluido en el producto si ha adquirido el mismo a distribuidores de Kaspersky Lab, o le es enviado por correo electrónico si ha adquirido el producto en una tienda en línea.

B

BASES DE DATOS

Las bases de datos creadas por los expertos de Kaspersky Lab contienen descripciones detalladas de todas las amenazas existentes contra la seguridad informática, así como de los métodos usados para su detección y desinfección. Kaspersky Lab actualiza permanentemente sus bases de datos a medida que aparecen nuevas amenazas. Para lograr una mayor calidad en la detección de amenazas, le recomendamos copiar regularmente las bases de datos de los servidores de actualización de Kaspersky Lab.

BLOQUEAR EL OBJETO

Denegar acceso al objeto desde aplicaciones externas. Un objeto bloqueado no puede ser leído, ejecutado, modificado, ni eliminado.

BORRAR MENSAJES

Método para procesar un mensaje que contiene signos de spam, en el cual el mensaje es físicamente eliminado. Este método es el recomendado para los mensajes que efectivamente contienen spam. Antes de eliminar un mensaje, una copia del mismo es guardada en el resguardo (a menos que esta opción esté desactivada).

C

CARPETA DE DATOS

La carpeta que contiene carpetas de servicio y bases de datos necesarias para trabajar con la aplicación. Si se mueve la carpeta de datos, toda la información que incluye debe ser guardada en la ubicación nueva.

COLOCAR OBJETOS EN CUARENTENA

Es un método para procesar un objeto potencialmente infectado bloqueando el acceso al archivo y moviéndolo de su ubicación original a la carpeta Cuarentena, donde el objeto es guardado en forma cifrada, para descartar la amenaza de infección. Los objetos en cuarentena pueden ser analizados utilizando bases de datos Anti-Virus actualizadas, analizadas por el administrador, o enviadas a Kaspersky Lab.

COPIA DE RESGUARDO

Crear una copia de resguardo de un archivo antes de cualquier procesamiento, y colocar esa copia en el almacenamiento de resguardo con la posibilidad de restaurar el archivo posteriormente (por ejemplo, volver a analizarlo tras la actualización de las bases de datos).

CUARENTENA

Esta es una carpeta en la que se ponen todos los objetos potencialmente infectados detectados durante el análisis o por la protección en tiempo real.

D

DESINFECTAR OBJETO

El método utilizado para procesar objetos infectados que resulta en la recuperación completa o parcial de datos, o la decisión que los objetos no pueden ser desinfectados. La desinfección de objetos se realiza mediante los registros de las bases de datos. Si la desinfección es la primera acción a realizarse con el objeto (es decir, la primera acción a realizarse con el objeto tras su detección), se creará una copia de resguardo de este objeto antes de proceder a su desinfección. Es posible que se pierda parte de la información durante el proceso de desinfección. La copia de resguardo puede usarse para restaurar el objeto a su estado original.

DESINFECTAR OBJETOS AL REINICIAR

Es un método para procesar objetos infectados que al momento de la desinfección están siendo utilizados por otras aplicaciones. Consiste en crear una copia del objeto infectado, desinfectar esta copia, y reemplazar el objeto original infectado con la copia desinfectada después del próximo reinicio del sistema.

E**ELIMINA UN OBJETO**

El método de procesamiento llega a eliminar físicamente el objeto peligroso en su ubicación original (disco duro, carpeta, recurso de red). Se le recomienda aplicar este método de procesamiento en objetos peligrosos que, por alguna razón, no se pueden desinfectar.

ENCABEZADO

Información al comienzo de un archivo o mensaje, la cual comprende información de bajo nivel acerca del estado y procesamiento de un archivo (o mensaje). Particularmente, el encabezado de un mensaje de correo contiene información acerca del remitente y el receptor, y la fecha.

EPIDEMIA DE VIRUS

Es una serie de intentos deliberados de infectar un equipo con un virus.

ESTADO DE LA PROTECCIÓN

Estado actual de la protección, resumiendo el grado de seguridad del equipo.

EXCLUSIÓN

Exclusión, es un objeto excluido del análisis por la aplicación Kaspersky Lab. Puede excluir determinados formatos de archivo del análisis, utilizar una máscara de archivo, o excluir un área determinada (por ejemplo, una carpeta o un programa), procesos de programa, u objetos por tipo de amenaza de acuerdo con la clasificación de la Enciclopedia. A cada tarea puede asignarse un conjunto de exclusiones.

F**FALSA ALARMA**

Situación en la que la aplicación de Kaspersky Lab considera un objeto no infectado como infectado debido a su código similar al de un virus.

I**INTERCEPTADOR**

Es un subcomponente de la aplicación, responsable de analizar tipos específicos de correos. El conjunto de interceptadores específicos para su instalación depende del rol o combinación de roles para los que la aplicación se esté implementando.

L**LICENCIA ACTIVA**

Es la licencia utilizada actualmente para el funcionamiento de una aplicación de Kaspersky Lab. La licencia establece la fecha de vencimiento para las características completas y la política de licencia para la aplicación. La aplicación no puede tener más de una licencia en estado activo.

LICENCIA ADICIONAL

Es una licencia para el funcionamiento de la aplicación Kaspersky Lab que ha sido agregada, pero no activada. La licencia adicional entra en efecto al expirar la licencia activa.

LISTA NEGRA DE ARCHIVOS LLAVE

Es una base de datos que contiene información acerca de archivos llave de Kaspersky Lab cuyos propietarios han violado los términos de uso del acuerdo de licencia e información sobre archivos llave que fueron distribuidos y, por alguna razón, no fueron vendidos o fueron reemplazados. Una lista negra de archivos es necesaria para el funcionamiento de las aplicaciones Kaspersky Lab. El contenido del archivo es actualizado junto con las bases de datos.

M

MÁSCARA DE SUBRED

La máscara de subred (también conocida como máscara de red) y la dirección de red determinan las direcciones de los equipos en una red.

MÁSCARA DE ARCHIVO

Representación de un nombre de archivo y extensión utilizando caracteres genéricos. Los dos caracteres genéricos utilizados en máscaras de archivos son * y ?, donde * representa cualquier cantidad de caracteres y ? representa cualquier carácter individual. Ud. puede representar cualquier archivo usando los caracteres ajustables. Tenga en cuenta que el nombre y la extensión van siempre separados por un punto.

N

NIVEL DE GRAVEDAD DEL EVENTO

Descripción de un evento conectado durante el funcionamiento de una aplicación de Kaspersky Lab. Existen cuatro niveles de gravedad:

- **Evento crítico.**
- **Falla de funcionamiento.**
- **Advertencia.**
- **Mensaje informativo.**

Eventos del mismo tipo poseen distintos niveles de gravedad, dependiendo de la situación al momento de ocurrir el evento.

NIVEL RECOMENDADO

Es el nivel de seguridad basado en los parámetros recomendados por los expertos de Kaspersky Lab para brindarle un nivel óptimo de protección para su equipo. Este es el nivel utilizado por defecto.

O

OBJETO OLE

Un objeto adjunto o incrustado en otro archivo. La aplicación Kaspersky Lab permite analizar objetos OLE en busca de virus. Por ejemplo, si Ud. inserta una tabla de Microsoft Office Excel en un documento de Microsoft Office Word, esta tabla se analizará como un objeto OLE.

OBJETO INFECTADO

Objeto que contiene un código nocivo: es detectado cuando una sección del código del objeto concuerda completamente con una sección del código de una amenaza conocida. Kaspersky Lab no recomienda usar estos objetos ya que pueden causar la infección de su equipo.

OBJETO PELIGROSO

Objeto que contiene un virus. Le recomendamos no activar estos objetos, pues podrían infectar su equipo. Una vez que se detecta un objeto infectado, le recomendamos que lo desinfecte usando una de las aplicaciones antivirus de Kaspersky Lab, y si su desinfección no es posible, entonces elimínelo.

OBJETO POTENCIALMENTE INFECTABLE

Un objeto que, por su estructura o formato, puede servir a los piratas como un "contenedor" para almacenar y distribuir un objeto nocivo. Por lo general, se trata de archivos ejecutables, por ejemplo archivos con la extensión **com, exe, dll**, etc. El riesgo de activar un código nocivo incluido en esos archivos es muy elevado.

OBJETO POTENCIALMENTE INFECTADO

Un objeto que contiene el código modificado de un virus conocido, o un código que se parece al código de un virus aún desconocido para Kaspersky Lab. Los archivos potencialmente infectados se detectan mediante el análisis heurístico.

OBJETO SIMPLE

Cuerpo del correo o adjuntos simples, por ejemplo, un archivo ejecutable. También ver objetos contenedores.

OBJETO SOSPECHOSO

Un objeto que contiene el código modificado de un virus conocido, o un código que se parece al código de un virus aún desconocido para Kaspersky Lab. Los objetos sospechosos son detectados utilizando el analizador heurístico.

OBJETO VIGILADO

Es un archivo transferido vía protocolos HTTP, FTP, o SMTP a través del firewall y enviado a la aplicación Kaspersky Lab para su análisis.

OBJETOS DE INICIO

Es el conjunto de programas necesarios para iniciar y operar correctamente el sistema operativo y el software instalado en su equipo. Estos objetos son ejecutados cada vez que su sistema operativo es iniciado. Existen virus capaces de infectar específicamente estos objetos, lo que podría ocasionar, por ejemplo, bloqueos en el acceso al sistema operativo.

OMITIR OBJETOS

Un método de procesamiento en el cual se pasa un objeto al usuario sin modificaciones. Si el registro de eventos está activado para este tipo de evento, la información sobre el evento detectado será registrada en el reporte.

P

PAQUETE DE ACTUALIZACIÓN

Es el paquete de archivos para actualizar el software. Se descarga de Internet y se instala en su equipo.

PERÍODO DE VALIDEZ DE LA LICENCIA

Es el período de tiempo durante el cual puede utilizar todas las características de la aplicación de Kaspersky Lab. Generalmente el período de validez de la licencia es de un año calendario a partir de su fecha de instalación. Una vez expirada la licencia, la funcionalidad de la aplicación se verá reducida. Ud. no podrá actualizar las bases de datos de la actualización.

PROCESOS CONFIABLES

Son procesos de aplicaciones cuyas operaciones con archivos no son vigiladas por la aplicación Kaspersky Lab en el modo de protección en tiempo real. En otras palabras, no se analizarán los objetos lanzados, abiertos o guardados por procesos de confianza.

PROTECCIÓN EN TIEMPO REAL

Es el modo de funcionamiento de la aplicación bajo el cual los objetos son analizados en tiempo real en busca de código nocivo.

La aplicación intercepta los intentos de abrir cualquier objeto (leer, escribir, o ejecutar) y analiza el objeto en busca de amenazas. Los objetos no infectados son entregados al usuario; lo objetos que contienen amenazas, o se sospecha que las contienen, son procesados de acuerdo con los parámetros de la tarea (son desinfectados, eliminados, o puestos en cuarentena).

PROTECCIÓN MÁXIMA

El nivel de seguridad para su equipo corresponde a la protección más completa que una aplicación pueda dar. En este nivel de protección, todos los archivos del equipo, medios de almacenaje removibles, y unidades de red son analizados en busca de virus si se conectan al equipo.

R

RESPALDO

Almacenamiento especial diseñado para guardar copias de resguardo de objetos creados, antes de su primera desinfección o borrado.

RESTAURAR

Mover un objeto original desde la Cuarentena o resguardo a la carpeta donde fue originalmente encontrado antes de ser puesto en Cuarentena, desinfectado, o eliminado, o a una carpeta distinta especificada por el usuario.

S

SECTOR DE ARRANQUE DEL DISCO

Un sector de arranque es un área especial en el disco duro del equipo, diskette, u otro dispositivo de almacenamiento. Éste contiene información sobre el sistema de archivos del disco y un programa cargador de arranque que es responsable del inicio del sistema operativo.

Existe una cantidad de virus que infectan los sectores de arranque, que son llamados virus de arranque. La aplicación Kaspersky Lab permite analizar los sectores de arranque en busca de virus y desinfectarlos si se encuentra alguna infección.

SERVIDORES DE ACTUALIZACIÓN DE KASPERSKY LAB

Es una lista de servidores HTTP y FTP de Kaspersky Lab de los cuales la aplicación descarga a su equipo actualizaciones de módulos y bases de datos.

T

TECNOLOGÍA iCHECKER

La tecnología iChecker permite incrementar la velocidad del análisis antivirus excluyendo objetos que no sufrieron ninguna modificación desde su último análisis, siempre y cuando la configuración del análisis (base de datos antivirus y parámetros) no haya cambiado. La información de cada archivo se guarda en una base de datos especial. Esta tecnología se emplea en los modos protección en tiempo real y análisis a petición.

Por ejemplo, usted tiene un archivo analizado por la aplicación de Kaspersky Lab al cual se le ha asignado el estado no infectado. La próxima vez la aplicación omitirá analizar este archivo a menos que haya sido modificado o que hayan sido modificados los parámetros de análisis. Si modificó el contenido del archivo añadiéndole un nuevo objeto, o modificó los parámetros del análisis, o actualizó la base de datos antivirus, se volverá a analizar el archivo.

Restricciones a la tecnología iChecker:

- esta tecnología no trabaja con archivos de gran tamaño ya que es más rápido analizar un archivo si este ha sido modificado desde la última vez que fue analizado;
- la tecnología soporta una cantidad limitada de formatos (.exe, .dll, .lnk, .tff, .inf, .sys, .com, .chm, .zip, .rar).

U

UMBRAL DE ACTIVIDAD DE VIRUS

Es el nivel máximo de permisividad de un tipo específico de evento durante un período de tiempo que, al ser excedido, se considerará como actividad excesiva de virus y una amenaza de epidemia de virus. Esta característica es importante

durante las epidemias de virus y permite al administrador reaccionar en tiempo y forma a las amenazas de epidemia de virus que surgen.

V

VIRUS DE ARRANQUE

Es un virus que infecta los sectores de arranque del disco duro de un equipo. El virus fuerza al sistema a cargarlo en la memoria durante el reinicio y a direccionar el control al código del virus en vez de al código cargador de arranque original.

VIRUS DESCONOCIDO

Es un virus sobre el que no hay ninguna información en la base de datos. Por lo general, los virus desconocidos son detectados por la aplicación en objetos utilizando el analizador heurístico, y esos objetos son clasificados como potencialmente infectados.

KASPERSKY LAB

Kaspersky Lab fue fundada en 1997. Hoy es el desarrollador ruso principal en una amplia gama de productos de software de alto rendimiento para seguridad de la información, incluyendo sistemas anti-virus, anti-spam y anti-hacker.

Kaspersky Lab es una compañía internacional. Con su casa matriz en la Federación Rusa, la compañía posee oficinas en el Reino Unido, Francia, Alemania, Japón, Benelux, China, Polonia y los Estados Unidos (California). Una nueva oficina de la compañía, el Centro Europeo de Investigación Antivirus, se ha establecido recientemente en Francia. La red de socios de Kaspersky Lab incluye más de 500 compañías alrededor del mundo.

Hoy, Kaspersky Lab emplea más de mil especialistas altamente calificados, incluyendo 10 personas con maestría en administración de empresas (MBA) y 16 personas con doctorados en ciencias. (pHD). Todos los expertos senior de anti-virus de Kaspersky Lab son miembros de la Organización de Investigadores de Antivirus para Equipos (Computer Anti-Virus Researchers Organization - CARO).

Los activos más importantes de nuestra empresa son el conocimiento único y la experiencia colectiva acumulados durante catorce años de una batalla continua contra los virus de los equipos. El análisis minucioso de las actividades de virus de los equipos permite a los especialistas de la compañía anticipar las tendencias en el desarrollo de malware, y brindar a nuestros usuarios una protección oportuna contra nuevos tipos de ataques. Esta ventaja es la base de los productos y servicios de Kaspersky Lab. Los productos de la compañía permanecen un paso adelante de otros distribuidores en la oferta de una cobertura antivirus comprensiva para nuestros clientes.

Años de trabajo duro han hecho de la compañía uno de los desarrolladores líderes de software antivirus. Kaspersky Lab fue el primero en desarrollar muchos de los estándares modernos de software antivirus. El producto insignia de la compañía, El Antivirus Kaspersky®, protege confiablemente de ataques de virus a todo tipo de sistemas de computadoras, incluyendo estaciones de trabajo, servidores de archivos, sistemas de correo, firewalls, gateways de Internet y equipos portátiles. Sus herramientas de control fáciles de utilizar maximizan la automatización de la protección antivirus para equipos y redes corporativas. Un gran número de desarrolladores alrededor del mundo utilizan el núcleo de Kaspersky Antivirus en sus productos, incluyendo Nokia ICG (EE.UU.), Aladdin (Israel), Sybari (EE.UU.), G Data (Alemania), Deerfield (EE.UU.), Alt-N (EE.UU.), Microworld (India), y BorderWare (Canadá).

Los clientes de Kaspersky Lab disfrutan de una amplia gama de servicios adicionales que garantizan un funcionamiento estable de los productos de la compañía, y plena compatibilidad con los requerimientos específicos del negocio del cliente. Diseñamos, implementamos y respaldamos sistemas antivirus corporativos. La base de datos de antivirus de Kaspersky Lab es actualizada cada hora. La compañía brinda a sus clientes servicio de soporte técnico en varios idiomas las 24 horas.

Si tiene preguntas, comentarios, o sugerencias, puede contactarnos a través de nuestros vendedores, o directamente a Kaspersky Lab. Con mucho gusto lo asistiremos, vía telefónica o por email, en todo asunto relacionado con nuestros productos. Recibirá respuestas completas y comprensivas a todas sus preguntas.

Sitio oficial de Kaspersky Lab: <http://latam.kaspersky.com>

Enciclopedia de Virus: <http://www.viruslist.com>

Laboratorio Antivirus: newvirus@kaspersky.com
(sólo para enviar archivos de objetos sospechosos)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>
(para consultas a analistas de virus)

ACUERDO DE LICENCIA

AVISO LEGAL IMPORTANTE PARA TODOS LOS USUARIOS: LEA CUIDADOSAMENTE ESTE CONTRATO LEGAL ANTES DE COMENZAR A UTILIZAR EL SOFTWARE.

AL HACER CLIC EN EL BOTÓN ACEPTAR EN LA VENTANA DEL CONTRATO DE LICENCIA, USTED ACEPTA ATENERSE A LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO. **TAL ACCIÓN SE ENTIENDE COMO UN SÍMBOLO EQUIVALENTE A SU FIRMA Y USTED ESTÁ CONSENTIENDO EN ATENERSE A ESTE CONTRATO Y SER PARTE DEL MISMO, Y ACEPTA QUE ESTE CONTRATO ES EJECUTABLE COMO CUALQUIER CONTRATO POR ESCRITO NEGOCIADO Y FIRMADO POR USTED.** SI NO ACEPTA TODOS LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO, CANCELE LA INSTALACIÓN DEL SOFTWARE Y NO LO INSTALE.

DESPUÉS DE HACER CLIC EN EL BOTÓN ACEPTAR DE LA VENTANA DEL CONTRATO DE LICENCIA, USTED TIENE EL DERECHO DE USAR EL SOFTWARE, DE ACUERDO CON LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO.

1. Definiciones

- 1.1. Software significa el software, el manual del usuario, materiales explicativos relacionados u otros, incluida cualquier Actualización.
- 1.2. **Titular del derecho**(el propietario de todos los derechos, ya sean exclusivos o no, del Software) significa Kaspersky Lab ZAO, una sociedad constituida de conformidad con las leyes de la Federación Rusa.
- 1.3. **Computadora(s)**significa el o los hardware(s), (incluidas computadoras personales, computadoras portátiles (laptops), estaciones de trabajo (workstations), asistentes digitales personales (PDA), 'teléfonos inteligentes', dispositivos móviles u otros dispositivos electrónicos para los cuales el Software fue diseñado) en donde el Software será instalado.
- 1.4. **Usuario Final (Usted/Su)** significa la(s) persona(s) que instala(n) o usa(n) el Software por su propia cuenta o que está(n) utilizando legalmente una copia del Software; o, si el Software se está descargando o instalando a nombre de una organización, tal como un empleador, "Usted" significa además la organización para la cual el Software se descarga o instala y se declara en el presente que tal organización ha autorizado a la persona que acepta este contrato, a hacerlo a su nombre. Para los fines del presente contrato, el término "organización," sin limitación, incluye cualquier sociedad, sociedad de responsabilidad limitada, sociedad anónima, asociación, sociedad de capital conjunto, compañía fiduciaria, unión temporal de empresas, organización laboral, empresa sin personería jurídica, o autoridad gubernamental.
- 1.5. **Socio(s)** significa organización(es) o persona(s), que distribuyen el Software sobre la base de un contrato y licencia del Titular del derecho.
- 1.6. **Actualización(es)** significa todas las actualizaciones, revisiones, parches, mejoras, arreglos, modificaciones, copias, adiciones, paquetes de mantenimiento, etc.
- 1.7. **Manual del usuario** se refiere al manual del usuario, la guía del administrador, el libro de referencia y materiales explicativos y de otra naturaleza, relacionados.

2. Otorgamiento de Licencia

- 2.1. Por medio del presente contrato, el Titular del derecho le otorga una licencia no exclusiva para almacenar, cargar, instalar, ejecutar y mostrar ("usar") el Software en una cantidad determinada de Computadoras, a fin de ayudarle a proteger Su Computadora en la que el Software está instalado, contra las amenazas descritas en el manual del usuario, de conformidad con los términos y condiciones de este Contrato (la "Licencia") y usted acepta esta Licencia:

Versión de Prueba. Si usted recibió, descargó y/o instaló una versión de prueba del Software y por medio del presente contrato se le otorga una licencia de evaluación para el Software, puede utilizar el Software sólo para fines de evaluación y solamente durante el periodo único de evaluación aplicable, a menos que se indique lo contrario, a partir de la fecha de la instalación inicial. Queda estrictamente prohibido cualquier uso del Software para otros fines o después de cumplido el periodo de evaluación aplicable.

Software de Ambiente Múltiple; Software de Idioma Múltiple; Software de Medios Dobles; Múltiples Copias; Combinaciones. Si utiliza distintas versiones del Software o diferentes ediciones de idioma del Software, si recibe el Software en varios medios, si recibe de cualquier forma varias copias del Software, o si recibió el Software combinado con otro software, la cantidad total permitida de sus Computadoras en las que todas las versiones del Software se instalan, corresponderá a la cantidad de licencias que hubiera obtenido del Titular del derecho quedando entendido que, a menos que los términos de la licencia estipulen lo contrario, cada licencia comprada le da el derecho a instalar y usar el Software en la cantidad de Computadora(s) especificada(s) en las Cláusulas 2.2 y 2.3.

- 2.2. Si el Software se compró en un medio físico, Usted tiene el derecho a usar el Software para la protección de la cantidad de Computadora(s) especificada(s) en el paquete del Software.
- 2.3. Si el Software se compró a través de la Internet, Usted tiene el derecho de usar el Software para la protección de la cantidad de Computadoras que se especificaron en el momento que compró la Licencia del Software.
- 2.4. Usted tiene el derecho a hacer una copia del Software sólo con fines de copia de seguridad y sólo para reemplazar la copia legalmente adquirida, si tal copia se pierde, destruye o inutiliza. Esta copia de seguridad no puede usarse para otros fines y debe destruirse cuando pierda el derecho a usar el Software o cuando Su licencia expire o haya sido finalizada por cualquier otra razón, de conformidad con la legislación vigente en el país de su residencia principal o en el país en el que Usted está usando el Software.
- 2.5. Usted puede transferir la licencia no exclusiva para usar el Software a otras personas o entidades legales, dentro del alcance de la licencia otorgada a Usted por el Titular del derecho, siempre y cuando el beneficiario acepte estar sujeto a todos los términos y condiciones de este Contrato, y sustituirlo a Usted plenamente en la licencia otorgada por el Titular del derecho. En caso que Usted transfiera totalmente los derechos otorgados por el Titular del derecho para usar el Software, debe destruir todas las copias del Software, incluida la copia de seguridad. Si Usted es un receptor de una licencia transferida, debe aceptar cumplir todos los términos y condiciones de este Contrato. Si no acepta atenerse a todos los términos y condiciones de este Contrato, no podrá instalar ni usar el Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User, who purchased the Software from the Rightholder, did.
- 2.6. Desde el momento de la activación del Software (con excepción de una versión de prueba del Software) Usted tiene el derecho a recibir los siguientes servicios durante el periodo definido, especificado en el paquete del Software (si compró el Software en un medio físico) o especificado durante la compra (si compró el Software por Internet)::
 - Actualizaciones del Software por Internet, cuando y de la manera en que el Titular del derecho las publique en su sitio web o a través de otros servicios en línea. Cualquier Actualización que Usted pudiera recibir forman parte del Software y los términos y condiciones de este Contrato se aplican a las mismas;
 - Asistencia Técnica a través de Internet y de la línea telefónica de Asistencia Técnica.

3. **Activación y término**

- 3.1. Si Usted modifica Su Computadora o realiza cambios en el software de otros proveedores instalado en la misma, el Titular del derecho podría requerirle que repita la activación del Software. El Titular del derecho se reserva el derecho a usar cualquier medio y procedimiento de verificación, para verificar la validez de la Licencia y/o la legalidad de una copia del Software instalado y/o usado en Su Computadora.
- 3.2. Si el Software se compró en un medio físico, el Software se puede utilizar, luego de su aceptación de este Contrato, por el periodo especificado en el paquete, a partir de la fecha de aceptación de este Contrato.
- 3.3. Si el Software se compró a través de Internet, el Software se puede usar, luego de su aceptación de este Contrato, por el tiempo que se especificó durante la compra.
- 3.4. Usted tiene el derecho a usar sin cargo una versión de prueba del Software, de acuerdo con lo establecido en la Cláusula 2.1, durante el periodo único de evaluación aplicable, contado desde el momento de la activación del Software de conformidad con este Contrato, quedando establecido que la versión de prueba no le da el derecho a Actualizaciones, Asistencia Técnica a través de Internet ni a la línea telefónica de Asistencia Técnica.
- 3.5. Su Licencia para Usar el Software está limitada al periodo de tiempo especificado en las Cláusulas 3.2 o 3.3 (según corresponda) y el periodo restante puede visualizarse usando la interfaz gráfica para el usuario del Software.

- 3.6. If You have purchased the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
- 3.7. Sin perjuicio de cualquier otro recurso establecido en la ley o basado en el sistema de equidad que el Titular del derecho pudiese tener, en caso de cualquier incumplimiento de Su parte con cualquiera de los términos y condiciones de este Contrato, el Titular del derecho estará facultado, en cualquier momento y sin aviso previo, a dar por terminada esta Licencia de uso del Software, sin reembolsar el precio de la compra ni ninguna parte del mismo.
- 3.8. Usted acepta que, al usar el Software o cualquier informe o información derivado como resultado del uso de este Software, cumplirá con todas las leyes y reglamentos internacionales, nacionales, estatales, regionales y locales que sean aplicables, incluidos, sin limitación, leyes de privacidad, de derechos de autor, de control de exportaciones y contra la obscenidad.
- 3.9. A menos que en el presente se estipule específicamente lo contrario, usted no podrá transferir o ceder ninguno de los derechos que le son otorgados bajo este Contrato, ni ninguna de sus obligaciones de conformidad al mismo.

4. **Asistencia Técnica**

La Asistencia Técnica descrita en la Cláusula 2.5 de este Contrato es provista a Usted cuando se instale la última actualización del Software (a menos que se trate de una versión de prueba del Software).

Technical support service: <http://support.kaspersky.com>

5. **Limitaciones**

- 5.1. Usted no deberá emular, clonar, alquilar, arrendar, prestar, vender, modificar, descompilar o aplicar ingeniería inversa al Software, o desmantelarlo o crear trabajos derivados basados en el Software o cualquier parte del mismo, salvo que la legislación aplicable le otorgue a Usted un derecho no renunciante; y usted no deberá reducir de cualquier otra forma, cualquier parte del Software, a una forma legible por el ser humano o transferir el Software bajo licencia o cualquier subporción del Software bajo licencia, ni permitirá que un tercero lo haga, a menos que las restricciones anteriores estén expresamente prohibidas por la legislación aplicable. Ni el código binario ni la fuente del Software podrán usarse ni podrá aplicárseles ingeniería inversa para recrear el algoritmo del programa, el cual está protegido por derechos de autor. Todos los derechos que no estén expresamente otorgados en el presente se reservan para el Titular del derecho y/o para sus proveedores, según corresponda. Cualquier uso no autorizado del Software dará lugar a una finalización inmediata y automática de este Contrato y de la Licencia otorgada bajo el mismo, y podría dar lugar a acciones penales y/o civiles en Su contra.
- 5.2. Usted no deberá transferir los derechos de uso del Software a ningún tercero, salvo lo establecido en la Cláusula 2.5 de este Contrato.
- 5.3. Usted no deberá suministrar el código de activación y/o el archivo de clave de licencia a terceros, ni permitir que terceros accedan al código de activación y/o clave de licencia, los cuales se consideran información confidencial del Titular del derecho y usted tomará las precauciones razonables para proteger el código de activación y/o clave de licencia que le fueron provistos en confidencia, quedando establecido que usted puede transferir el código de activación y/o la clave de licencia a terceros, de acuerdo a lo establecido en la Cláusula 2.4 de este Contrato.
- 5.4. Usted no deberá alquilar, arrendar o prestar el Software a ningún tercero.
- 5.5. Usted no deberá usar el Software para la creación de datos o software utilizado para la detección, bloqueo o tratamiento de amenazas descritos en el manual del usuario.
- 5.6. El Titular del derecho tiene el derecho a bloquear el archivo de clave o dar por terminada Su Licencia para el uso del Software en caso que Usted incumpla cualquiera de los términos y condiciones de este Contrato y sin reembolso en Su favor.
- 5.7. Si Usted utiliza la versión de prueba del Software, no tiene el derecho a recibir la Asistencia Técnica especificada en la Cláusula 4 de este Contrato y no tiene el derecho de transferir la licencia o los derechos de uso del Software a ningún tercero.

6. **Garantía limitada y exención de responsabilidad**

- 6.1. El Titular del derecho garantiza que el Software se desempeñará básicamente de acuerdo con las especificaciones y descripciones establecidas en el manual del usuario quedando establecido, sin embargo, que tal garantía limitada no aplicará a lo siguiente: (w) las deficiencias de Su Computadora e infracción relacionada por las cuales el Titular del derecho queda expresamente exento de cualquier responsabilidad por garantía; (x) desperfectos, defectos o fallas resultantes por el mal uso; abuso; accidente; negligencia; instalación, operación o mantenimiento inapropiados; robo; vandalismo; casos de fuerza mayor; actos de terrorismo; fallas o sobrecargas en el suministro eléctrico; muerte; alteración, modificación no permitida o reparaciones por terceros, que no sean del Titular del derecho; o cualquier otra acción de terceros o suya, o causas fuera del control razonable del Titular del derecho; (y) cualquier defecto que Usted no ponga en conocimiento del Titular del derecho, tan pronto sea posible, después de que el defecto aparece por primera vez; y (z) incompatibilidad causada por componentes de hardware y/o software instalados en Su Computadora.
- 6.2. Usted reconoce, consiente y acepta que ningún software está libre de errores y se le aconseja crear copias de seguridad de Su Computadora, con la frecuencia y confiabilidad que le parezca apropiada.
- 6.3. El Titular del derecho no ofrece ninguna garantía de que el Software funcionará correctamente en caso de violaciones a los términos descritos en el manual del usuario o en este Contrato.
- 6.4. El Titular del derecho no garantiza que el Software funcionará correctamente si Usted no descarga de forma periódica las Actualizaciones especificadas en la Cláusula 2.6 de este Contrato.
- 6.5. El Titular del derecho no garantiza la protección contra las amenazas descritas en el manual del usuario, después del vencimiento del periodo especificado en las Cláusulas 3.2 o 3.3 de este Contrato, o después de que la Licencia para uso del Software hubiera finalizado por cualquier razón.
- 6.6. EL SOFTWARE ES PROVISTO "EN EL ESTADO EN QUE SE ENCUENTRA " Y EL TITULAR DEL DERECHO NO REALIZA NINGUNA DECLARACIÓN O GARANTÍA EN CUANTO A SU USO O DESEMPEÑO. CUALQUIER GARANTÍA, CONDICIÓN, DECLARACIÓN O TÉRMINO, EN LA MEDIDA EN QUE NO PUEDA EXCLUIRSE O LIMITARSE POR LA LEY APLICABLE, EL TITULAR DEL DERECHO Y SUS SOCIOS NO DAN NINGUNA GARANTÍA, CONDICIÓN, DECLARACIÓN O TÉRMINO (EXPRESO O IMPLÍCITO, YA SEA POR LEY, DERECHO CONSUETUDINARIO, COSTUMBRE, USOS U OTRO) SOBRE NINGÚN ASPECTO, INCLUYENDO, SIN LIMITACIÓN, LA NO VIOLACIÓN DE DERECHOS DE TERCEROS, APTITUD COMERCIAL, CALIDAD SATISFACTORIA, INTEGRACIÓN O POSIBILIDAD DE APLICACIÓN PARA UN FIN PARTICULAR. USTED ASUME TODAS LAS FALLAS Y TODO EL RIESGO EN CUANTO AL DESEMPEÑO Y LA RESPONSABILIDAD DE ELEGIR EL SOFTWARE PARA LOGRAR LOS RESULTADOS QUE USTED ESPERA Y POR LA INSTALACIÓN, USO Y RESULTADOS OBTENIDOS DEL SOFTWARE. SIN LIMITAR LAS ESTIPULACIONES ANTERIORES, EL TITULAR DEL DERECHO NO REALIZA NINGUNA DECLARACIÓN Y NO DA NINGUNA GARANTÍA DE QUE EL SOFTWARE ESTARÁ LIBRE DE ERRORES O LIBRE DE INTERRUPCIONES U OTRAS FALLAS, O QUE EL SOFTWARE CUMPLIRÁ CUALQUIERA O TODOS SUS REQUERIMIENTOS YA SEA QUE ÉSTOS HUBIERAN SIDO INFORMADOS O NO AL TITULAR DEL DERECHO.

7. Exclusión y limitación de responsabilidad

HASTA EL LÍMITE MÁXIMO PERMITIDO POR LA LEY APLICABLE, EL TITULAR DEL DERECHO Y SUS SOCIOS EN NINGÚN CASO SERÁN RESPONSABLES, POR DAÑOS Y PERJUICIOS ESPECIALES, INCIDENTALES, PUNITIVOS, INDIRECTOS O EMERGENTES DE CUALQUIER TIPO (INCLUYENDO, SIN LIMITACIÓN, LOS DAÑOS Y PERJUICIOS POR LUCRO CESANTE, PÉRDIDA DE INFORMACIÓN CONFIDENCIAL O DE OTRO TIPO, INTERRUPCIÓN DE LOS NEGOCIOS, PÉRDIDA DE PRIVACIDAD, CORRUPCIÓN, DAÑO O PÉRDIDA DE DATOS O PROGRAMAS, POR LA OMISIÓN DE CUMPLIR CUALQUIER DEBER, INCLUIDO CUALQUIER DEBER LEGAL, DE BUENA FE O DE CUIDADO RAZONABLE, NEGLIGENCIA, PÉRDIDA ECONÓMICA Y CUALQUIER OTRA PÉRDIDA PECUNIARIA O DE CUALQUIER OTRO TIPO) QUE SURJA O QUE SE RELACIONE DE CUALQUIER FORMA CON EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, LA PRESTACIÓN DE ASISTENCIA U OTROS SERVICIOS, INFORMACIÓN, SOFTWARE Y CONTENIDO RELACIONADO A TRAVÉS DEL SOFTWARE O DE CUALQUIER OTRA FORMA, O LA OMISIÓN DE HACERLO, QUE SURJA DEL USO DEL SOFTWARE, O DE CUALQUIER OTRA FORMA DE CONFORMIDAD O EN RELACIÓN CON CUALQUIER ESTIPULACIÓN DE ESTE CONTRATO, O QUE SURJA DE CUALQUIER INCUMPLIMIENTO DEL CONTRATO O CUALQUIER ACTO ILÍCITO (INCLUYENDO NEGLIGENCIA, TERGIVERSACIÓN, CUALQUIER OBLIGACIÓN O DEBER POR RESPONSABILIDAD CIVIL OBJETIVA), O CUALQUIER INCUMPLIMIENTO DE DEBERES LEGALES, O CUALQUIER INCUMPLIMIENTO EN LAS GARANTÍAS OFRECIDAS POR EL TITULAR DEL DERECHO, O CUALQUIERA DE SUS SOCIOS, AUN CUANDO ÉSTOS HUBIERAN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

USTED ACEPTA QUE EN CASO DE QUE EL TITULAR DEL DERECHO Y/O SUS SOCIOS FUERAN DECLARADOS RESPONSABLES, LA RESPONSABILIDAD DE ÉSTOS ESTARÁ LIMITADA AL COSTO DEL

SOFTWARE. EN NINGÚN CASO LA RESPONSABILIDAD DEL TITULAR DEL DERECHO Y/O SUS SOCIOS EXCEDEN LAS TARIFAS PAGADAS A ÉSTOS POR EL SOFTWARE (SEGÚN CORRESPONDA).

NADA EN ESTE CONTRATO EXCLUYE O LIMITA NINGÚN RECLAMO POR MUERTE O LESIONES PERSONALES. ASIMISMO, EN CASO DE QUE CUALQUIER EXENCIÓN DE RESPONSABILIDAD, EXCLUSIÓN O LIMITACIÓN EN ESTE CONTRATO NO PUEDA EXCLUIRSE O LIMITARSE DE CONFORMIDAD A LA LEY APLICABLE, SÓLO TAL EXENCIÓN DE RESPONSABILIDAD, EXCLUSIÓN O LIMITACIÓN DEJARÁ DE APLICAR CON RELACIÓN A USTED Y USTED CONTINUARÁ ESTANDO SUJETO A LAS DEMÁS.

8. **GNU y otras licencias de terceros.**

El Software puede incluir algunos programas de software que están bajo licencia (o sublicencias) al usuario bajo la Licencia Pública General (GPL, por sus siglas en inglés) de GNU u otras licencias de software libre similares, las cuales, entre otros derechos, permiten al usuario copiar, modificar y redistribuir ciertos programas o partes de los mismos, y tener acceso al código fuente ("Software de Código Abierto"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. Si cualquier licencia de Software de Código Abierto requiriere que el Titular del derecho provea derechos de uso, copia o modificación de un programa de Software de Código Abierto, que sean más amplios que los derechos otorgados en este Contrato, entonces tales derechos prevalecerán a los derechos y restricciones del presente contrato.

9. **Titularidad de la propiedad intelectual.**

Usted acepta que el Software y la autoría, sistemas, ideas, métodos de operación, documentación y otra información contenida en el Software, son propiedad intelectual protegida por derechos de autor y/o secretos comerciales valiosos del Titular del derecho o sus socios, y que éstos, según corresponda, están protegidos por las leyes civiles y penales, y por las leyes de derechos de autor, secretos comerciales, marcas comerciales y patentes de la Federación Rusa, la Unión Europea y los Estados Unidos, así como las de otros países y tratados internacionales. Este contrato no le otorga ningún derecho a la propiedad intelectual, incluyendo las Marcas Comerciales o Marcas de Servicio del Titular del derecho y/ o sus socios ("Marcas Comerciales"). Usted podrá usar las Marcas Comerciales sólo en la medida necesaria para identificar las impresiones producidas por el Software de conformidad con prácticas aceptadas de marcas comerciales, incluyendo la identificación del nombre del propietario de la Marca Comercial. Tal uso de cualquier Marca Comercial no le da ningún derecho de propiedad sobre tal Marca Comercial. El Titular del derecho y/o sus socios son propietarios y retienen todos los derechos, títulos e intereses sobre el Software, incluyendo, sin limitación, cualquier corrección de errores, mejoras, Actualizaciones u otras modificaciones al Software, ya sea que las realice el Titular del derecho o cualquier tercero, y todos los derechos de autor, patentes, derechos sobre secretos comerciales, marcas comerciales y otros derechos de propiedad intelectual contenidos en el mismo. Su posesión, instalación o uso del Software no le transfiere ningún derecho sobre la propiedad intelectual en el Software, y usted no adquirirá ningún derecho sobre el Software a menos que se estipule expresamente en este Contrato. Todas las copias del Software realizadas de acuerdo al presente, deben contener los mismos avisos de protección de propiedad intelectual que aparecen en el Software. Salvo lo expresado en el presente, este Contrato no le otorga ningún derecho de propiedad intelectual sobre el Software y Usted reconoce que la Licencia, de acuerdo a lo definido en el presente, otorgada bajo este Contrato, sólo le otorga un derecho limitado de uso, bajo los términos y condiciones de este Contrato. El Titular del derecho se reserva todos los derechos no otorgados expresamente a Usted en este Contrato.

Usted reconoce que el código fuente, el código de activación y/o el archivo de clave de licencia del Software, son propiedad del Titular del derecho y constituyen un secreto comercial de éste. Usted acepta no modificar, adaptar, traducir, aplicar ingeniería inversa, descompilar, desensamblar o intentar de cualquier otra forma descubrir el código fuente del Software, de ninguna forma.

9.3 Usted acepta no modificar ni alterar el Software de ninguna forma. No podrá retirar o alterar ningún aviso de derechos de autor u otros avisos de propiedad intelectual en ninguna de las copias del Software.

10. **Lev aplicable; arbitraje**

Este Contrato se regirá e interpretará de acuerdo con las leyes de la Federación Rusa sin hacer referencia a las reglas y principios sobre conflictos de leyes. Este Contrato no se regirá por la Convención de las Naciones Unidas sobre Contratos de Compraventa Internacional de Mercaderías, cuya aplicación se excluye expresamente. Cualquier controversia que surja de la interpretación o aplicación de los términos de este Contrato o cualquier incumplimiento del mismo, a menos que se resuelva por negociación directa, se resolverá en el Tribunal de Arbitraje Comercial Internacional en la Cámara de Comercio e Industria de la Federación Rusa, en Moscú, Federación Rusa. Cualquier laudo dictado por el árbitro será definitivo y vinculante para las partes y cualquier fallo en tal laudo arbitral podrá ejecutarse en cualquier corte con jurisdicción competente. Nada en esta Sección 10 impedirá a una Parte que

busque u obtenga una reparación imparcial de una corte con jurisdicción competente, ya sea antes, durante o después del procedimiento de arbitraje.

11. **Plazo para entablar acciones.**

Ninguna acción, sin importar su forma, que surja de las transacciones de este Contrato, podrá entablarse por ninguna de las partes del mismo, más de un (1) año después de ocurrida o descubierta la causa que motiva la acción, salvo la acción por infracción de los derechos de propiedad intelectual, que podrá entablarse dentro del plazo máximo permitido por ley.

12. **Totalidad del Contrato; divisibilidad; reserva de derechos.**

Este Contrato constituye la totalidad del acuerdo entre usted y el Titular del derecho y reemplaza a cualquier acuerdo, propuesta, comunicaciones o publicidades anteriores, orales o por escrito, con respecto al Software o al objeto de este Contrato. Usted reconoce que ha leído este Contrato, lo entiende y acepta atenerse a sus términos. Si cualquier estipulación de este Contrato fuera declarada inválida, nula o no ejecutable por cualquier razón, en todo o en parte, por una corte con jurisdicción competente, tal estipulación se interpretará de forma más limitada para que sea legal y ejecutable, y el Contrato completo no fracasará por esta causa; el resto del Contrato continuará completamente vigente en la máxima medida permitida por ley o basada en el sistema de equidad mientras preserve, en la mayor medida posible, su intención original. Ninguna renuncia a una estipulación o condición aquí contenida será válida a menos que se realice por escrito y se firme por Usted y un representante autorizado del Titular del derecho, quedando establecido que ninguna renuncia a reclamar por un incumplimiento de cualquier estipulación de este Contrato se interpretará como una renuncia a reclamar por cualquier incumplimiento anterior, consecutivo o subsiguiente. La omisión del Titular del derecho de insistir o ejecutar el cumplimiento de cualquier estipulación de este Contrato o cualquier derecho, no se interpretará como una renuncia a tal estipulación o derecho.

13. **Información de contacto**

Si tuviera cualquier pregunta en relación a este Contrato o si deseara contactar al Titular del derecho por cualquier razón, por favor contacte a nuestro Departamento de Servicio al Cliente en:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd

Moscow, 123060

Russian Federation

Tel: +7-495-797-8700

Fax: +7-495-645-7939

Correo electrónico: info@kaspersky.com

Sitio web: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved. Todos los derechos reservados. El Software y cualquier documentación que le acompaña están registrados como derechos de autor y protegidos por las leyes y tratados internacionales sobre derechos de autor, así como otras leyes y tratados sobre propiedad intelectual.

INDEX

A

Acciones a realizar en los objetos	38
Actualización	
manualmente	47
reversión a la última actualización	48
Actualizar	
configuración regional.....	49
desde una carpeta local.....	52
modo de ejecución.....	50, 51
objeto para actualizar.....	51
origen de actualización	48
según planificación	51
utilizar el servidor proxy	49
Análisis	
optimización del análisis	40
Analizar	
acción a realizar en el objeto detectado.....	38
análisis de archivos compuestos	41
lanzamiento automático de la tarea omitida.....	43
modo de ejecución.....	43
nivel de seguridad.....	38
según cronograma.....	43
tecnologías de análisis.....	42
tipo de objetos a analizar	39
Auto-defensa de la aplicación	65

C

Categorías de amenazas detectables	59
Cuarentena.....	70, 71, 72
Cuarentena y Resguardo	70, 71

I

Icono del área de notificación de la barra de tareas	30
Informes	69
Iniciar tarea	
actualización	47, 50, 51
análisis.....	36, 43, 44
Interfaz de la aplicación.....	30

K

Kaspersky Lab.....	9
--------------------	---

M

Menú contextual	31
-----------------------	----

N

Notificaciones	66
----------------------	----

R

Reacción ante la amenaza	
análisis de virus	38
Respaldo	71, 72

Restricción de acceso a la aplicación.....	65
V	
Ventana Principal de la Aplicación	32
Z	
Zona de confianza	
aplicaciones de confianza.....	59
reglas de exclusión	59, 60