

KASPERSKY LAB

Kaspersky Anti-Virus[®]
Mobile 6.0 Enterprise Edition

GUÍA DEL USUARIO

KASPERSKY ANTI-VIRUS® MOBILE 6.0
ENTERPRISE EDITION

Guía del usuario

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

Fecha de revisión: Octubre 2007

Índice

CAPÍTULO 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION.....	4
1.1. Requisitos hardware y software.....	5
1.2. Presentación del producto	5
CAPÍTULO 2. KASPERSKY ANTI-VIRUS PARA MICROSOFT WINDOWS MOBILE	6
2.1. Instalación de Kaspersky Anti-Virus	6
2.2. Uso de la aplicación	9
2.2.1. Inicio de la aplicación.....	9
2.2.2. Interfaz gráfica de usuario	10
2.2.3. Análisis antivirus y protección	11
2.2.4. Uso de la Cuarentena.....	15
2.2.5. Uso del componente Anti-Spam	16
2.2.6. Actualización de las bases antivirus	19
2.2.7. Recepción de informes de actividad de la aplicación	20
2.3. Desinstalación del programa	21
CAPÍTULO 3. CONTROL DE LA APLICACIÓN CON KASPERSKY ADMINISTRATION KIT	24
3.1. Control de directivas	26
3.1.1. Creación de una directiva.....	26
3.1.2. Examen y modificación de la configuración de la directiva.....	31
3.2. Administración de los parámetros de aplicación.....	37
ANEXO A. KASPERSKY LAB.....	45
A.1. Otros productos Kaspersky Lab	46
A.2. Cómo encontrarnos	57
ANEXO B. CONTRATO DE LICENCIA.....	58

CAPÍTULO 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

Kaspersky Anti-Virus® Mobile Enterprise Edition (designado a continuación como **Kaspersky Anti-Virus**) ha sido diseñado para proteger terminales móviles bajo Microsoft Windows Mobile contra programas malignos y mensajes no solicitados y ofrece las características siguientes:

- **Protección en tiempo real** del sistema de archivos del dispositivo; interceptación y análisis de:
 - todos los objetos entrantes, transmitidos mediante conexiones inalámbricas (puerto infrarrojo, Bluetooth), mensajes EMS y MMS, durante la sincronización con un equipo personal y la carga de archivos desde un navegador;
 - archivos, abiertos en dispositivo móvil;
 - programas, instalados desde la interfaz del dispositivo móvil.
- **Análisis a petición o planificados** de los objetos del sistema de archivos almacenados tanto en su dispositivo móvil como en tarjetas de ampliación de memoria.
- **Aislamiento seguro de objetos infectados** en cuarentena.
- **Actualización de las bases de Kaspersky Anti-Virus** utilizadas para detectar aplicaciones dañinas y eliminar objetos no seguros.
- **Bloqueo de mensajes SMS no solicitados.**

Kaspersky Anti-Virus sólo puede instalarse mediante las herramientas de Kaspersky Administration Kit, que también permiten al administrador realizar las acciones siguientes con él:

- recuperar información acerca del estado de protección;
- recuperar información acerca de los parámetros de la aplicación actual;
- modificar los parámetros de la aplicación mediante directivas de seguridad;
- recuperar información sobre eventos significativos.

A diferencia de otros productos Kaspersky Lab, Kaspersky Anti-Virus **no permite** realizar las acciones siguientes mediante las herramientas de Kaspersky Administration Kit:

- descargar actualizaciones de bases antivirus;
- crear tareas de grupo, globales o locales;
- ampliar el plazo de validez de la llave de licencia;
- desinstalar la aplicación a distancia.

El usuario puede personalizar la configuración de Kaspersky Anti-Virus, supervisar el estado actual de la protección y examinar informes de actividad de las aplicaciones.

La aplicación posee un menú sencillo y una interfaz amigable que permiten controlar los parámetros de Kaspersky Anti-Virus (cuando su modificación no está prohibida por la directiva de seguridad), visualizar el estado actual de la protección antivirus y el registro de eventos que recopila las acciones del programa.

Cuando detecta una aplicación dañina, Kaspersky Anti-Virus es capaz de desinfectar el objeto infectado (si es posible hacerlo), eliminarlo o moverlo a cuarentena. No se guarda copia de un objeto cuando se elimina.

1.1. Requisitos hardware y software

Kaspersky Anti-Virus puede instalarse en terminales móviles equipados con uno de los siguientes sistemas operativos:

- Microsoft Windows Mobile 2003, 2003SE.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Presentación del producto

Puede adquirir Anti-Virus Mobile Enterprise Edition por Internet, y descargar el programa de instalación y la documentación en formato electrónico. También puede adquirir Kaspersky Anti-Virus Mobile Enterprise Edition tiendas de operadores. Para obtener más información de compra, póngase en contacto con su operador de telefonía móvil.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS PARA MICROSOFT WINDOWS MOBILE

Este capítulo describe el funcionamiento de la aplicación Kaspersky Anti-Virus Mobile Enterprise Edition en dispositivos móviles con uno de los siguientes sistemas operativos:

- Microsoft Windows Mobile 2003, 2003SE,
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

2.1. Instalación de Kaspersky Anti-Virus

La instalación remota de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition se realiza con Kaspersky Administración Kit.

- Creación del paquete de instalación, con el archivo de distribución del producto, la herramienta de instalación, la llave de licencia, el archivo de configuración.
- Copia del paquete de instalación en el equipo remoto; tras esto, se inicia la herramienta de instalación en el equipo; la herramienta esperará hasta que conecte el dispositivo móvil a su equipo.
- Instalación de Kaspersky Anti-Virus en el dispositivo móvil cuando éste se encuentra conectado al equipo..

Para instalar Kaspersky Anti-Virus Mobile Enterprise Edition, siga estos pasos:

1. En la carpeta **Instalación remota** del explorador de consola , cree un paquete de instalación que será utilizado para la instalación remota de la aplicación en dispositivos móviles (ver Figura 1).

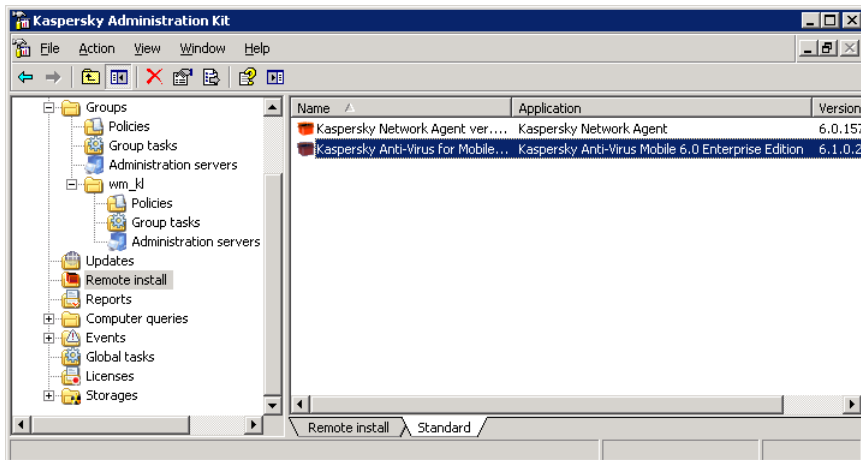


Figura 1. Selección del paquete de instalación

Para obtener más detalles acerca de la creación y utilización de paquetes de instalación, consulte la Guía de referencia de Kaspersky Administración Kit.

2. Abra el menú contextual del paquete seleccionado y utilice el comando **Instalar**.

La interfaz del Asistente de instalación está diseñada como la de cualquier Asistente de Microsoft Windows y consta de varios pasos: puede desplazarse por ellos con los botones **Anterior** y **Siguiente**, o salir con **Terminar**. Para salir del Asistente en cualquier paso, haga clic en **Cancelar**.

Advertencia.

El paquete de instalación incluye la llave de licencia que debe instalar en el dispositivo móvil junto con el propio paquete. Si la llave de licencia no se encuentra en el paquete de instalación, la aplicación no quedará activada y no podrá funcionar.

No se admite ningún otro modo de instalación de la llave de licencia.

3. Tras las operaciones realizadas por el Asistente, se instalará la herramienta **Kav Mobile EE Installer** en el equipo o grupo de equipos seleccionado; esta herramienta servirá para continuar la instalación de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

4. Cuando conecta un dispositivo móvil al equipo, Kav Mobile EE Installer sugiere al usuario que instale Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition (ver Figura 2).

Advertencia.

Para instalar Kaspersky Anti-Virus 6.0 Enterprise Edition en un dispositivo móvil, debe utilizar Microsoft Active Sync, en otro caso la herramienta **Kav Mobile EE Installer** no podrá reconocer los dispositivos conectados.

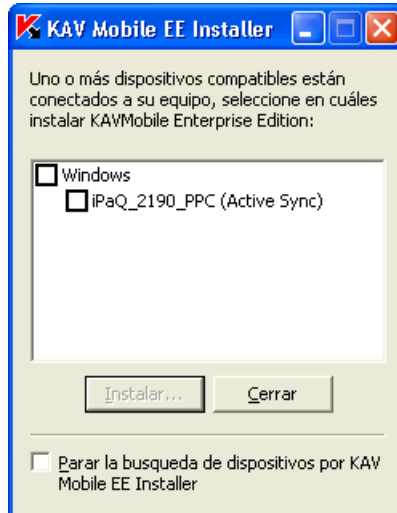


Figura 2. Selección de un dispositivo móvil

5. Seleccione uno de los dispositivos en la lista y haga clic en **Instalar**. El proceso de instalación de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition comenzará en el dispositivo móvil seleccionado.
6. Lea el contenido del contrato de licencia en el dispositivo móvil. Si está conforme con todos los términos, elija **OK**. Para cancelar la instalación, presione **Cancelar** (ver Figura 3)¹.

¹ Todas las capturas de pantalla de este documento fueron tomadas a partir de un terminal smartphone I-mate K-JAM smartphone. Otros modelos de terminales pueden variar ligeramente en la interfaz de aplicación.

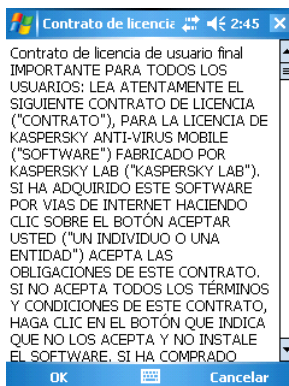


Figura 3. Contrato de licencia

2.2. Uso de la aplicación

Esta sección describe cómo configurar el antivirus y la protección en tiempo real, el filtrado de mensajes SMS, el análisis antivirus del dispositivo móvil y las actualizaciones de la aplicación.

2.2.1. Inicio de la aplicación


Para ejecutar *Kaspersky Anti-Virus Mobile Enterprise Edition*, siga estos pasos:

1. Abra el menú **Aplicaciones** de su dispositivo móvil.
2. Seleccione el icono  **KAV Mobile** y ejecute la aplicación.

Después de iniciar la aplicación, el dispositivo móvil mostrará una ventana de estado de los componentes principales de Kaspersky Anti-Virus (ver Figura 4).

- **P.T.R.:** visualización del modo de protección en tiempo real. Para obtener más detalles, ver sección 2.2.3 en la página 11).
- **Último análisis completo:** fecha del último análisis antivirus del smartphone.
- **Fecha de la base:** fecha de publicación de las bases de Kaspersky Anti-Virus utilizadas por la aplicación.

Advertencia.

Si nunca realizó un análisis antivirus del móvil o cuando dos semanas han transcurrido después de la última actualización, el texto del icono junto al elemento correspondiente cambia a . Este icono también aparece si el modo de protección en tiempo real o el módulo Anti-Spam están desactivados.

- **Anti-Spam:** el modo de operación del componente antispam utilizado para filtrar mensajes SMS.

Advertencia.

El componente Anti-spam no está disponible en modelos PDA.



Figura 4 Ventana de estado de los componentes de la aplicación

2.2.2. Interfaz gráfica de usuario

La interfaz gráfica de usuario contiene cinco fichas que puede abrir desde el **menú** (ver Figura 5):

- La ficha **Analizar** permite realizar un análisis antivirus del dispositivo móvil, modificar la configuración del análisis antivirus y el modo de protección en tiempo real así como planificar el análisis automático.
- La ficha **Anti-Spam** permite configurar los filtros de mensajes SMS y MMS entrantes.
- La ficha **Actualizar** permite actualizar las bases antivirus, modificar los parámetros o planificar la actualización.

- La ficha **Cuarentena** permite administrar la cuarentena, una zona de almacenamiento especial para objetos infectados y sospechosos.
- La ficha **Informativo** permite mostrar los informes de actividad de los componentes de la aplicación, obtener información general acerca de la aplicación y las bases utilizadas así como modificar la configuración general de la aplicación.



Figura 5. El menú de la aplicación

Para regresar a la ventana de estado de los componentes de la aplicación, elija **Estado actual**.

Para cerrar la aplicación seleccione **Salir**.

2.2.3. Análisis antivirus y protección

Desde la ficha **Analizar**, puede realizar un análisis antivirus de todo el sistema de archivos y de la memoria del dispositivo móvil, o analizar un archivo o directorio individual. También puede modificar la configuración del análisis antivirus y del modo de protección antivirus, mostrar un informe con los resultados del análisis o planificar la ejecución automática del análisis.

2.2.3.1. Protección en tiempo real y análisis a petición

La protección en tiempo real es un modo de funcionamiento en el que una parte del programa Kaspersky Anti-Virus queda residente en la memoria RAM para supervisar todos los datos del dispositivo móvil.

La protección en tiempo real se inicia al encender el dispositivo y se ejecuta hasta su parada (cuando este modo está activo en la configuración).

Además, Kaspersky Anti-Virus permite ejecutar un análisis completo del sistema de archivos del dispositivo móvil.

Los resultados de actividad de la protección en tiempo real y del análisis a petición son registrados en un informe. Para mostrar el informe, elija **Conf. análisis**. También puede consultar el informe desde la ficha **Informativo** (ver sección 2.2.7 en la página 20).

Para habilitar el modo de protección en tiempo real, haga lo siguiente:

1. Seleccione **Conf. análisis** en la ficha **Analizar**.
2. El parámetro **Prot. Tiempo Real** permite activar o desactivar el modo de protección en tiempo real.

Para modificar la configuración del análisis a petición, haga lo siguiente:

1. Seleccione Configuración del análisis en la ficha Analizar.
2. Para especificar la cobertura de análisis en la sección **Opciones**, seleccione qué tipos de archivos se analizarán como sigue:
 - **Analizar comprim.:** analiza el contenido de archivos comprimidos;
 - **Archivos ejecutables:** analiza sólo los archivos ejecutables.
3. Para especificar la acción realizada por la aplicación cuando detecta un objeto infectado, seleccione unos de los valores posibles en la sección **Acción antivirus**. Para que Kaspersky Anti-Virus intente neutralizar el objeto infectado detectado active la casilla **Intentar desinfectar**. Si no es necesaria la desinfección, seleccione una acción antivirus con alguno de los valores siguientes del parámetro **Fallo reparación**:
 - **Cuarentena:** mueve los objetos infectados detectados a la cuarentena
 - **Preguntar:** muestra un mensaje en pantalla acerca de la detección de un virus con la sugerencia de eliminar, mover a cuarentena o ignorar el objeto infectado.
 - **Eliminar:** elimina los objetos infectados detectados
 - **Ignorar:** no realiza ninguna acción con el objeto

También puede especificar alguna de estas acciones en caso de que la desinfección de un objeto no tenga éxito. Para ello active la casilla **Intentar desinfectar** y seleccione la acción necesario en la lista **Si no se puede desinfectar**.

Para iniciar un análisis antivirus:

1. Ejecute Kaspersky Anti-Virus (sección 2.2.1 en la página 9).
2. Cambie a la ficha Configuración del análisis.
 - Para especificar la cobertura de análisis en la sección **Opciones**, seleccione qué tipos de archivos se analizarán (ver más arriba).
 - Determine las acciones realizadas por la aplicación cuando detecta un objeto infectado (ver más arriba).
3. Seleccione **Análisis completo** en la ficha **Analizar** (ver Figura 6) si desea analizar el sistema de archivos del dispositivo móvil al completo o **Analizar carpeta** si desea analizar una carpeta individual.



Figura 6. Ficha **Analizar**

Cuando selecciona **Analizar carpeta**, se abre una ventana con el sistema de archivos del dispositivo móvil. Para ejecutar el análisis de una carpeta, desplace el cursor hasta la carpeta y presione el botón **Analizar**.

Después de iniciarse el análisis, se abre una ventana con el estado actual del análisis, el número de objetos analizados y la ruta de cada objeto analizado (ver Figura 7).

Figura 7. La ventana **Analizar**

Figura 8. Notificación de virus detectado

Después de terminar el análisis, la aplicación mostrará estadísticas generales acerca de los objetos detectados y eliminados.

2.2.3.2. Análisis planificado

Kaspersky Anti-Virus le permite planificar el inicio automático del análisis a horas determinadas. El análisis se ejecutará en segundo plano. Cuando detecta un objeto infectado, la aplicación aplica la acción especificada por la configuración (ver sección **Conf. análisis**).

El análisis planificado está desactivado de forma predeterminada.

Para configurar un análisis planificado, siga estos pasos:

En la página **Analizar** seleccione **Planificación** y configure los parámetros de análisis (ver Figura 9):

- **Diario:** el análisis se realiza cada día. La hora del análisis se determina con el parámetro **Hora**.
- **Semanal:** el análisis se realizará cada semana. El día y la hora del análisis están determinados por los parámetros **Día de la semana** y **Hora**.
- **Desactivar:** el análisis sólo será iniciado de forma manual.

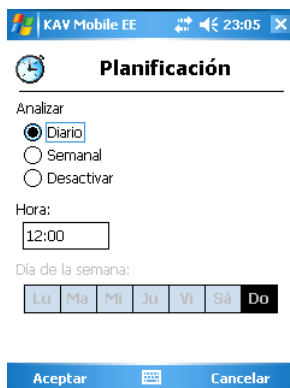


Figura 9. El menú **Planificación**

2.2.4. Uso de la Cuarentena

Los objetos infectados en cuarentena no pueden dañar su dispositivo móvil y puede eliminarlos o restaurarlos más tarde.

La aplicación puede mover los objetos infectados que detecta a cuarentena automáticamente o después de su confirmación.

Si desea configurar la aplicación para que mueva a cuarentena los objetos infectados automáticamente, abra la ficha **Analizar**, elija **Conf. análisis** y seleccione **Cuarentena** como valor del parámetro **Fallo reparación** en la sección **Acción antivirus**. Si la desinfección del objeto no tiene éxito, active la casilla **Intentar desinfectar** y seleccione **Cuarentena** en la lista **Si no se puede desinfectar**.

Si seleccionó la acción **Preguntar**, cuando detecta un objeto infectado Kaspersky Anti-Virus le propone eliminarlo o moverlo a cuarentena.

Utilice la página **Cuarentena** para consultar el contenido de la cuarentena (ver Figura 10).



Figura 10. Cuarentena

El menú disponible en la ventana Cuarentena permite:

- Mostrar información detallada de cada objeto almacenado en cuarentena (**Detalles**).
- Analizar un archivo en cuarentena en busca de virus (**Analizar**).
- Eliminar el objeto seleccionado (**Eliminar**).
- Neutralizar un objeto en cuarentena (**Desinfectar**).
- Restaura el objeto seleccionado en cuarentena y lo mueve a su carpeta de origen (**Restaurar**).
- Purgar la cuarentena al eliminar todos los objetos que contiene (**Eliminar todo**).

2.2.5. Uso del componente Anti-Spam

El componente Anti-Spam es otra novedad de Kaspersky Anti-Virus Mobile 6.0. Está diseñado para proteger el dispositivo móvil contra mensajes SMS no solicitados.

Advertencia.

El componente Anti-spam no está disponible en los modelos PDA.

El principio de filtrado de mensajes utiliza el sistema de lista negra y de lista blanca. El componente Anti-Spam bloqueará los mensajes entrantes de números incluidos en su lista negra. Los mensajes que provienen de números presentes en listas blancas no son bloqueados.

Para modificar la configuración Anti-Spam:

1. Seleccione **Configuración** en la ficha **Anti-Spam**.
2. Active o desactive el componente Anti-Spam con la casilla **Activar Anti-Spam**.
3. Especifique si desea recibir mensajes SMS que provienen de números de teléfono no incluidos en ninguna lista con la casilla **Recibir SMS: de remitentes descon.**
4. Especifique si desea recibir mensajes SMS que provienen de números de teléfono de su lista de contactos con la casilla **Recibir SMS: de mi lista de contactos**.

2.2.5.1. Modificación de las listas blanca y negra

La lista "negra" contiene los números de teléfono cuyos mensajes SMS recibidos son bloqueados por el componente Anti-Spam.

La lista "blanca" contiene los números de teléfono cuyos mensajes SMS o MMS recibidos están autorizados.

Para modificar la lista negra o la lista blanca, abra la página **Anti-Spam** (ver Figura 11) y elija la lista apropiada.

Para modificar la lista, utilice el **Menú**:

- **Agregar:** agrega un nuevo registro a la lista seleccionada.
- **Eliminar:** elimina el registro actual de la lista.
- **Modificar:** permite modificar el registro actual en la lista.

Después de seleccionar la opción **Agregar**, especifique el número de teléfono que desea agregar a la lista. El teléfono puede comenzar por un número o por el signo "+" y sólo puede contener números.

Después de modificar la lista, haga clic en **Aceptar** para regresar a la página **Anti-Spam**.



Figura 11. Menú Anti-Spam

2.2.5.2. Acciones aplicadas a mensajes

Cuando recibe un mensaje SMS desde número de teléfono que no aparece en la lista negra o blanca, y si autorizó la recepción de mensajes desde números desconocidos (ver sección 2.2.5 en la página 16), el componente Anti-Spam mostrará una advertencia en la pantalla del terminal (ver Figura 12).

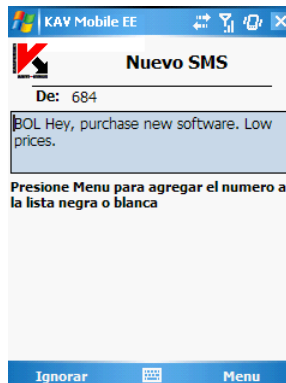


Figura 12. Advertencia del componente Anti-Spam

Utilice el **Menú** para seleccionar y aplicar una de las acciones siguientes al mensaje:

- **Agregar a la lista blanca:** autoriza la recepción del mensaje y agrega el número del remitente a la lista blanca.

- **Agregar a la lista negra:** bloquea la recepción del mensaje y agrega el número del remitente a la lista negra.

Para autorizar la recepción del mensaje presione **Ignorar**. En este caso, no se agrega el número del remitente a ninguna de las listas.

La información acerca de mensajes se agrega al informe de la aplicación. Para examinar el informe, cambie a la ficha **Anti-Spam** y haga clic en **Informe** o elija **Informe Anti-Spam** en la misma ficha. También puede consultar el informe desde la ficha **Información** (ver sección 2.2.7 en la página 20).

2.2.6. Actualización de las bases antivirus

Kaspersky Anti-Virus detecta los virus gracias a los registros de las bases antivirus, que contienen descripciones de todos los programas dañinos conocidos hasta la fecha. Es extremadamente importante para la seguridad de su smartphone actualizar las bases antivirus con frecuencia.

Puede actualizar la base manualmente o planificar su actualización. Para configurar y ejecutar la actualización, utilice la ficha Menú Actualizar (ver Figura 13). La actualización se realiza por Internet desde los servidores de Kaspersky Lab.

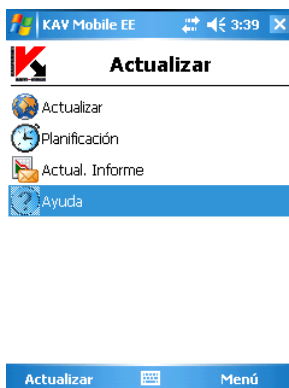


Figura 13. Ficha **Menú Actualizar**

La información acerca de la actualización de la base queda registrada en el informe. Para examinar el informe, cambie a la ficha **Menú Actualizar** y elija **Actual. Informe**. También puede consultar el informe desde la ficha **Información** (ver sección 2.2.7 en la página 20).

Para ejecutar una actualización manual de las bases antivirus desde los servidores de actualización de Kaspersky Lab:

1. Ejecute Kaspersky Anti-Virus (sección 2.2.1 en la página 9) y cambie a la ficha **Menú Actualizar**.
2. Seleccione **Actualizar** para iniciar el proceso de actualización.

Para planificar una actualización automática de las bases antivirus:

1. Ejecute Kaspersky Anti-Virus (sección 2.2.1 en la página 9) y cambie a la ficha Menú Actualizar.
2. Seleccione **Planificación** para poder modificar la configuración de las actualizaciones automáticas.
3. Para especificar la frecuencia de las actualizaciones, modifique los valores del parámetro **Actualización**:
 - **Diario**: realiza la actualización cada día. Adicionalmente, especifique la **Hora** de ejecución de las actualizaciones.
 - **Semanal**: la actualización se realiza cada semana. Adicionalmente, especifique el **Día de la semana** y la **Hora** para realizar las actualizaciones.
 - **Desactivar**: el análisis sólo será iniciado de forma manual.

La ficha **Información** le permite ver la fecha de publicación de las bases antivirus actualmente instaladas en el dispositivo móvil así como el número de firmas de virus. Para ello, seleccione **Bases antivirus** en la ficha.

2.2.7. Recepción de informes de actividad de la aplicación

Los informes de actividad de la aplicación pueden consultarse con **Informes** en la ficha **Información**. Puede recibir un informe acerca de cualquier tarea de Kaspersky Anti-Virus:

- análisis antivirus;
- módulo anti-spam;
- actualización de bases antivirus.

Por ejemplo, para ver un informe del análisis antivirus, siga estos pasos:

1. Ejecute Kaspersky Anti-Virus (sección 2.2.1 en la página 9).
2. Elija Informes en la ficha Información (ver Figura 14).

3. Seleccione el informe de protección en tiempo real en la ventana abierta.

Figura 14. Ficha **Informes**

2.3. Desinstalación del programa

Para desinstalar Kaspersky Anti-Virus:

1. Desactive la autoprotección (ver 2.2.3 en la pág. 11 para obtener detalles);

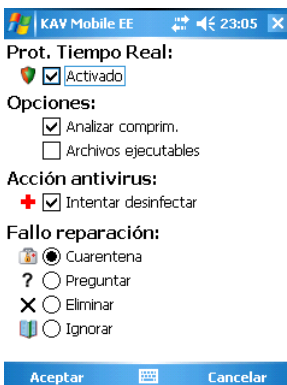


Figura 15. Desactivación de la autoprotección

2. Salga de Kaspersky Anti-Virus. Para ello, elija **Salir** en el menú del programa (ver Figura 16).



Figura 16. Salir del programa

3. Elimine el programa. Para ello:

- Haga clic en **Inicio**, seleccione **Configuración** y **Quitar programas** (ver Figura 17):

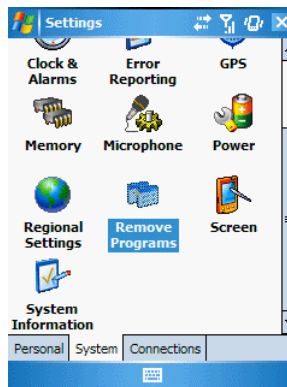


Figura 17. Comienzo de la desinstalación del programa

- Seleccione **KAV Mobile** en la lista de aplicaciones instaladas y haga clic en **Eliminar** (ver Figura 18).

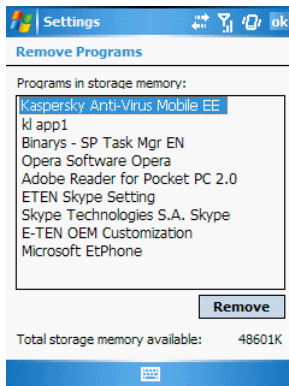


Figura 18. Selección de programa

- Para confirmar la eliminación haga clic en **Sí** (ver Figura 19).

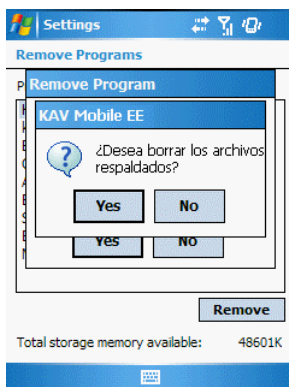


Figura 19. Confirmación de la desinstalación del programa

CAPÍTULO 3. CONTROL DE LA APLICACIÓN CON KASPERSKY ADMINISTRATION KIT

Kaspersky Administración Kit es un sistema centralizado de herramientas para llevar a cabo las principales tareas administrativas relacionadas con la seguridad de los dispositivos móviles.

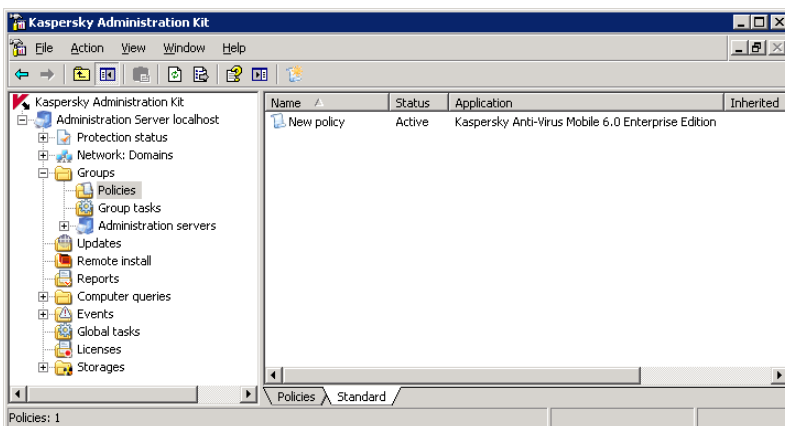


Figura 20. Consola de administración de Kaspersky Administration Kit

Cuando utiliza Kaspersky Administración Kit, el administrador configura de forma centralizada las directivas y la propia aplicación. La protección se construye de acuerdo con sus parámetros.

Una particularidad de la administración centralizada es la posibilidad de organizar los dispositivos móviles en grupos, y modificar su configuración mediante la creación y definición de directivas de grupo.

Una directiva es un conjunto de parámetros de Kaspersky Anti-Virus aplicados a un grupo dentro de la red lógica. Una directiva permite administrar el funcionamiento de la aplicación al contener múltiples parámetros de Kaspersky Anti-Virus.

También puede incluir un conjunto de restricciones a la modificación de parámetros de configuración específicos. Un usuario con derechos de administrador puede definir estas restricciones desde la interfaz de Kaspersky Administración Kit.

Nota

Para desplazar el dispositivo móvil dentro del grupo administrador, abra la **Consola de administración**, cambie al contenedor **Red** y configúrelo para reflejar los dominios.

Para asegurarse de que Kaspersky Administration Kit detecta los dispositivos móviles, active la casilla **Puerto para dispositivos móviles** en la ficha **Configuración** de las propiedades del servidor de administración.

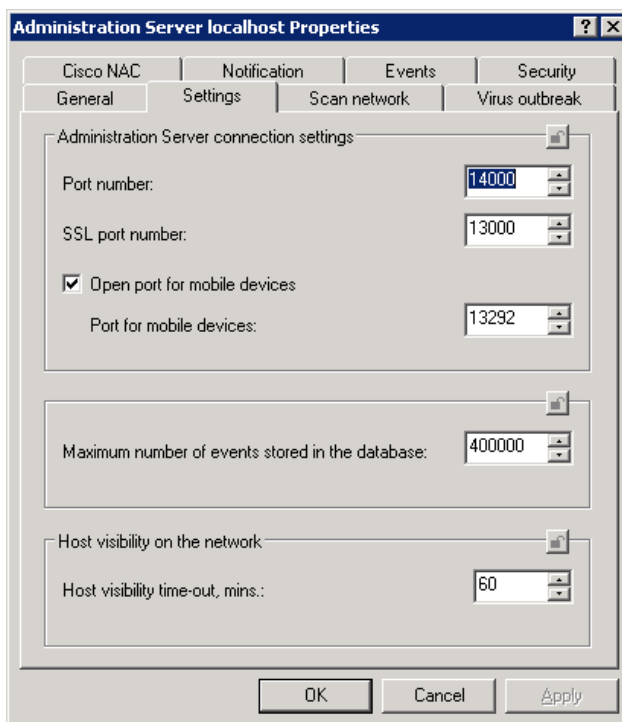


Figura 21. Ficha **Configuración**

3.1. Control de directivas

Esta sección explica cómo crear y configurar directivas para Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.


3.1.1. Creación de una directiva

Para crear una directiva, proceda de la forma siguiente:

1. Seleccione el grupo de dispositivos móviles para el que desea crear una directiva desde el explorador de consola, en la carpeta **Grupos**.
2. Seleccione la carpeta **Directivas** dentro del grupo seleccionado, abra el menú contextual y elija **Nuevo→Directiva**.

La interfaz del Asistente de instalación está diseñada como la de cualquier Asistente de Microsoft Windows y consta de varios pasos: puede desplazarse por ellos con los botones **Anterior** y **Siguiente**, o salir con **Terminar**. Para salir del Asistente en cualquier paso, haga clic en **Cancelar**.

Advertencia.

En cada etapa de la creación de una directiva, es posible bloquear los parámetros introducidos con el botón . Si el candado está cerrado, los valores especificados serán utilizados por la directiva cuando ésta se aplique a los dispositivos móviles.

Paso 1. Información general de la directiva

El primer paso del asistente es introductorio. En la primera ventana, debe especificar el nombre de la directiva (campo **Nombre**). En la segunda ventana, seleccione la aplicación Kaspersky Anti-Virus **Mobile 6.0 Enterprise Edition** en la lista desplegable **Nombre de aplicación**. Para aplicar una directiva inmediatamente después de su creación, active la casilla **Activar la directiva** en la sección **Estado de la directiva** en la tercera ventana.

Paso 2. Configuración del análisis antivirus

Esta etapa permite definir los parámetros utilizados para el análisis antivirus del dispositivo móvil: la cobertura del análisis y la planificación de su ejecución. También puede definir si el modo de protección en tiempo real estará activo.

Para ejecutar el modo de protección en tiempo real en el dispositivo móvil, active la casilla **Activar la protección en tiempo real** (ver Figura 22). Tras esto, la

protección en tiempo real se activará cuando se encienda el dispositivo y permanecerá activa hasta que lo apague.

La sección **Último análisis completo** permite definir la cobertura de análisis, seleccionar qué tipos de archivos deben analizarse y precisar qué acciones deben realizarse con los objetos infectados:

- **Analizar sólo archivos ejecutables:** analiza sólo archivos ejecutables.
- **Analizar archivos comprimidos:** analiza el contenido de archivos comprimidos.
- **Intentar desinfectar:** intenta reparar un objeto infectado. No todos los objetos pueden ser desinfectados.

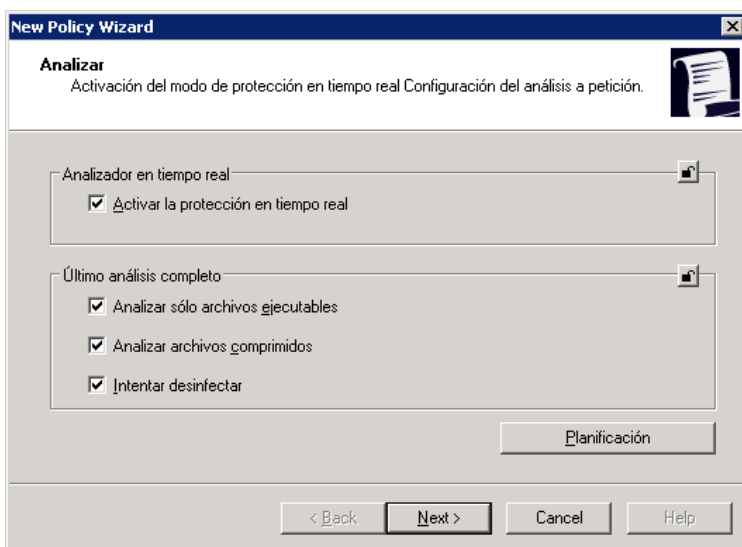


Figura 22. Configuración de los parámetros de análisis antivirus

Para planificar la ejecución del análisis a petición, haga clic en **Planificación**. El cuadro de diálogo abierto le permite especificar la frecuencia del análisis:

- **Desactivar:** el análisis sólo será iniciado de forma manual.
- **Cada N días:** la acción se ejecuta a diario. Especifique la hora de ejecución en los campos **Hora de inicio**.
- **Semanalmente:** la acción se ejecuta ciertos días de la semana. En los campos **Hora de inicio**, especifique la hora y seleccione el día de la semana de ejecución.

Paso 3. Selección del origen de las actualizaciones

Esta etapa permite definir los el origen de actualizaciones y planificar qué actualizaciones se ejecutarán.

En el campo correspondiente de la sección **Origen de actualizaciones** (ver Figura 22) especifique la dirección del origen de actualizaciones. Sólo pueden utilizarse servidores de actualización de Kaspersky Lab como origen de actualizaciones.

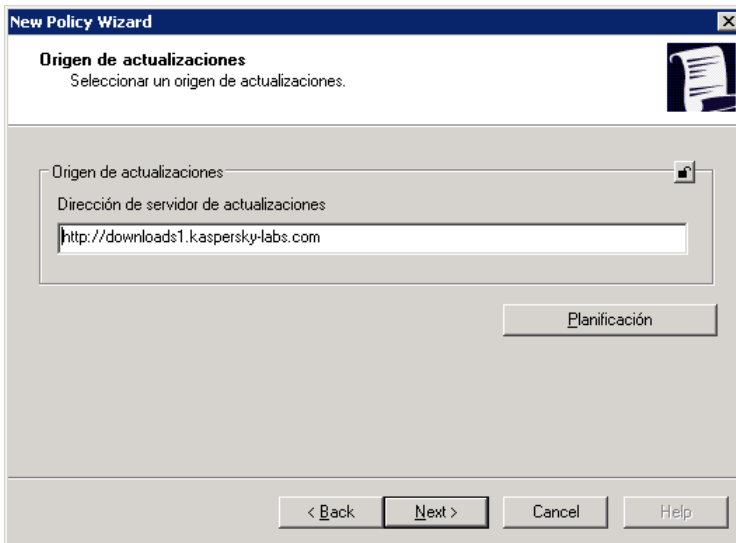


Figura 23. Selección del origen de las actualizaciones

También puede programar la descarga automática de actualizaciones. Para ello use el botón **Planificación**. El cuadro de diálogo abierto le permite especificar la frecuencia del análisis:

- **Desactivar:** el análisis sólo será iniciado de forma manual.
- **Cada N días:** la acción se ejecuta a diario. Especifique la hora de ejecución en los campos **Hora de inicio**.
- **Semanalmente:** la acción se ejecuta ciertos días de la semana. En los campos **Hora de inicio**, especifique la hora y seleccione el día de la semana de ejecución del análisis a petición.

Paso 4. Especificación de parámetros avanzados

En este paso, puede especificar los parámetros del módulo Anti-Spam y el periodo de sincronización con el Servidor de administración.

Configure el módulo Anti-Spam en la sección **Anti-Spam** (ver Figura 24). Si activa la casilla **Activar la protección antispam**, el módulo Anti-Spam analizará los mensajes entrantes de acuerdo con los criterios siguientes:

- **Entregar mensajes de números en la lista de contactos:** este criterio distingue los números que pertenecen a la lista "blanca". Los mensajes que provienen de números de la lista blanca siempre se entregan al usuario.
- **Prohibir mensajes de números no incluidos en la lista "blanca" o sin número de remite especificado:** este criterio determina qué mensajes no serán entregados al usuario.

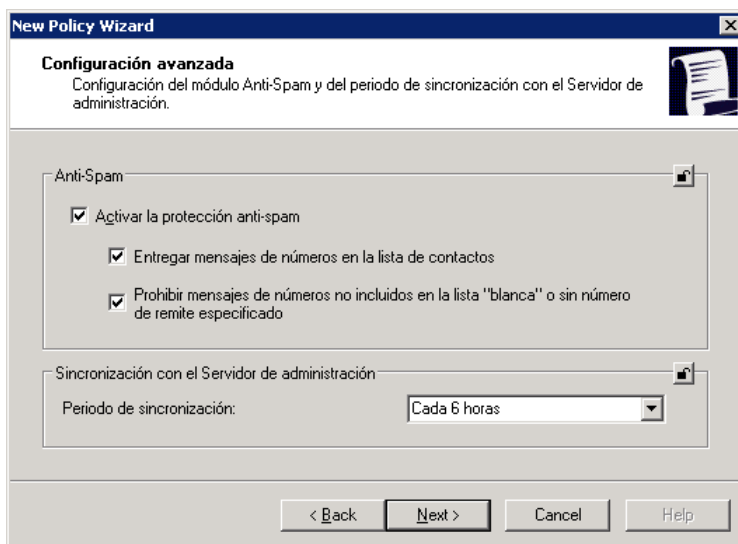



Figura 24. Configuración avanzada de la aplicación

Para especificar la frecuencia de sincronización, seleccione su valor en la lista desplegable **Periodo sincronización** en la sección **Sincronización con el Servidor de administración**.

Paso 5. Fin de la creación de una directiva

La última pantalla del Asistente informa del éxito del proceso de creación de la directiva (ver Figura 25).

Después de cerrar el asistente, las directivas para Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition se agregan a la carpeta **Directivas** del grupo asociado y se muestran en el panel de resultados.

Puede modificar los parámetros de la directiva y definir restricciones para la modificación de su configuración con el botón  para cada grupo de parámetros. Como ya mencionamos, el usuario del dispositivo móvil no podrá modificar parámetros bloqueados. La estrategia será aplicada en la siguiente sincronización del dispositivo móvil cliente con el servidor.

Puede copiar o desplazar directivas de un grupo a otro o eliminarlas, con los comandos **Copiar / Pegar**, **Cortar / Pegar** o **Eliminar** en el menú contextual o sus equivalentes en el menú **Acción**.

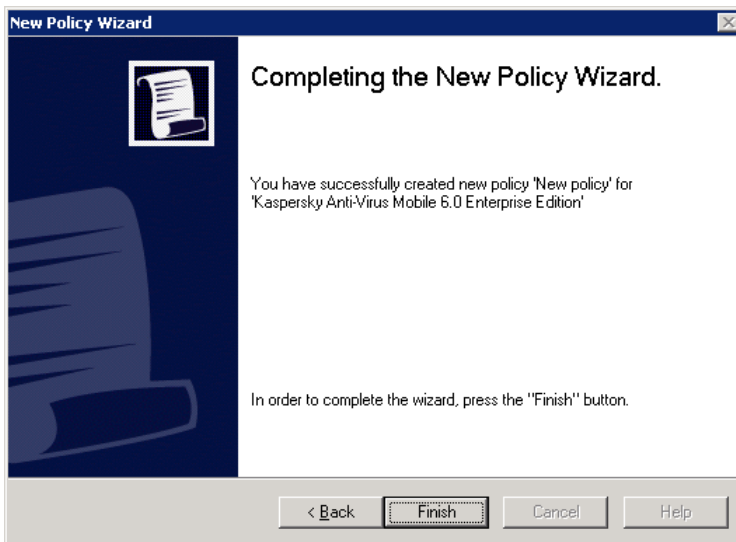


Figura 25. Fin del proceso de creación de una directiva

3.1.2. Examen y modificación de la configuración de la directiva

Durante esta etapa, puede modificar la directiva, prohibir la modificación de parámetros en grupos anidados, aplicación y tareas.


1. Seleccione el grupo de equipos desde el explorador de consola, en la carpeta **Grupos**, cuyos parámetros desea modificar.
2. Seleccione la carpeta **Directivas** dentro de este grupo; todas las directivas creadas para este grupo se mostrarán en el panel de resultados.
3. Seleccione la directiva requerida para **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition** en la lista de directivas (el nombre de la aplicación se indica en el campo **Aplicación**).
4. Seleccione **Propiedades** en el menú contextual de la directiva seleccionada.

Se abrirá un cuadro de diálogo de configuración de las directivas de aplicación con varias fichas.

Las fichas **General**, **Uso** y **Eventos** son fichas estándar de Kaspersky Administration Kit (para más detalles, consulte el Manual del administrador de Kaspersky Administración Kit).

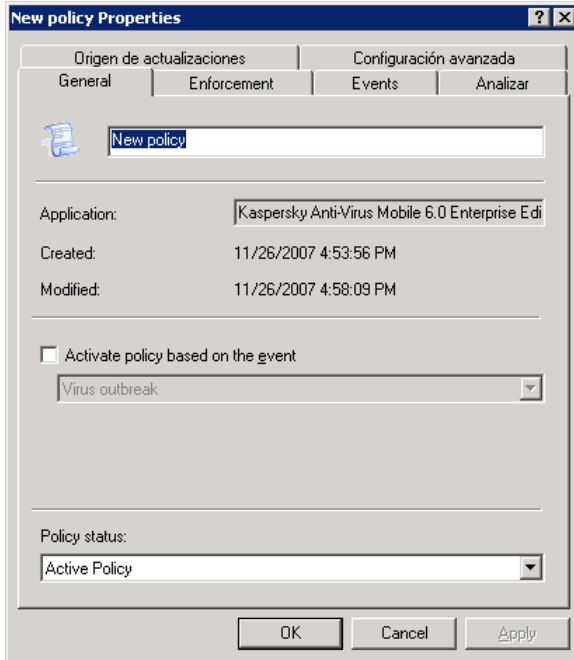
Las demás fichas contienen controles de configuración de los parámetros de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition. Encontrará a continuación la descripción de cada ficha.

Nota

Cuando modifique la configuración de la directiva, utilice el botón  para bloquear los datos introducidos en la directiva. Como ya mencionamos, el usuario del dispositivo móvil no podrá modificar más tarde los parámetros bloqueados.

3.1.2.1. Información acerca de la aplicación

La información siguiente sobre la directiva aparece en la ficha **General** (ver Figura 26): nombre de la directiva, nombre de la aplicación asociada, versión de la aplicación, fecha y hora de creación de la directiva, fecha y hora de su última modificación.

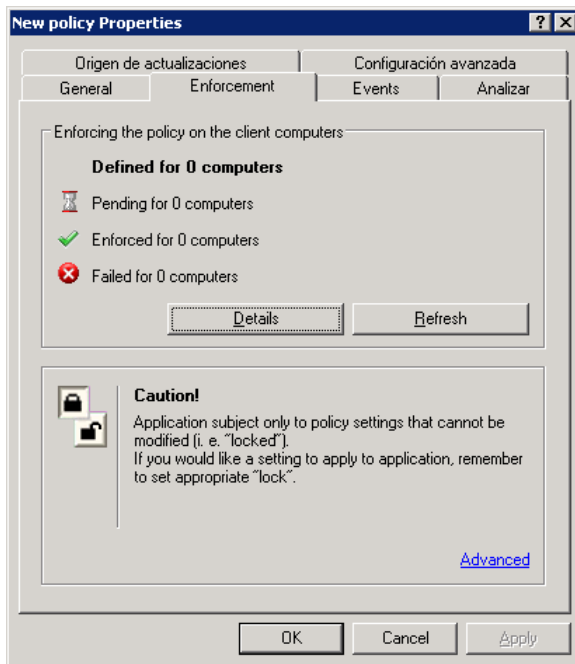
Figura 26. Ficha **General**

Este cuadro de diálogo permite cambiar el nombre de la directiva, activarla o desactivarla o configurar su activación cuando se produce algún evento.

3.1.2.2. Examen de los resultados de la aplicación de la directiva

La ficha **Aplicación** (ver Figura 27) muestra información general acerca de la aplicación de la directiva en los dispositivos móviles del grupo, así como el número de dispositivos en los que la directiva:

- no ha sido definida;
- ha sido aplicada;
- no ha sido aplicada todavía;
- no se pudo aplicar debido a un error.

Figura 27. Ficha **Aplicación**

Encontrará resultados detallados sobre la aplicación de la directiva en cada equipo cliente del grupo en el cuadro de diálogo abierto con **Detalles** (para obtener detalles, consulte el Manual del administrador de Kaspersky Administración Kit 6.0).

3.1.2.3. Parámetros de registro del funcionamiento de la aplicación

Durante su funcionamiento, Kaspersky Anti-Virus genera un cierto conjunto de eventos. Cada evento incluye un indicador de su nivel de importancia. Existen cuatro niveles de importancia: evento crítico, fallo, advertencia y mensaje de información.

Los eventos de un mismo tipo pueden presentar diferentes niveles de importancia, en función de la situación en que éstos se producen.

La ficha **Eventos** (ver Figura 28) muestra los tipos de eventos que se producen durante el funcionamiento de la aplicación y que son registrados en el informe,

así como la ubicación del informe y las condiciones de notificación del administrador o de otros usuarios.

Para mostrar los tipos de eventos, seleccione el nivel de importancia deseado en la lista desplegable **Nivel de importancia**. En el campo de información inferior se muestran los tipos de eventos para el nivel seleccionado.

Para cada evento, puede indicar su inclusión en el informe y configurar el envío de una notificación al administrador en caso de producirse.

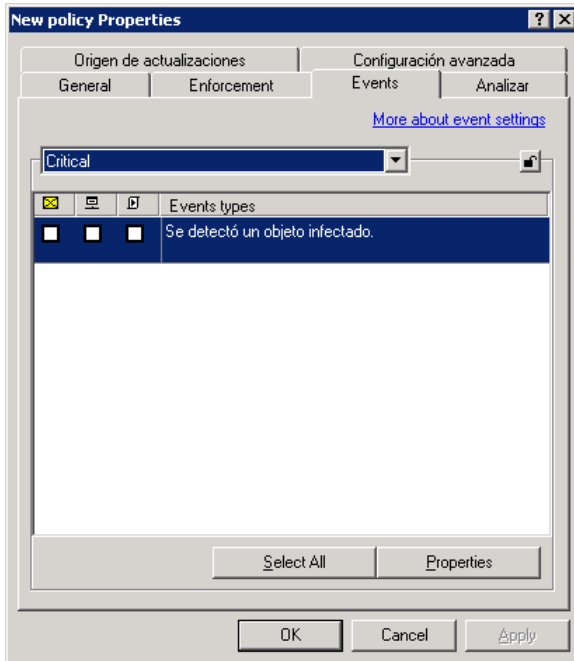
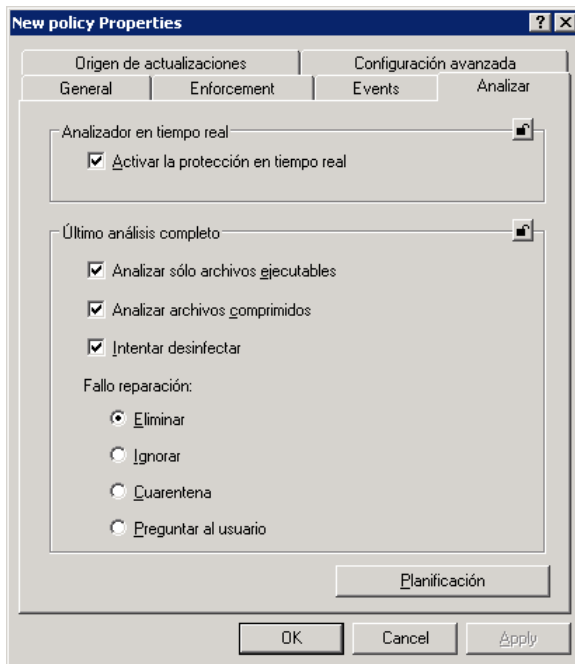


Figura 28. Ficha **Eventos**

Para una descripción detallada del resto de parámetros de la ficha **Eventos**, vea el Manual del administrador de Kaspersky Administración Kit 6.0.

3.1.2.4. Configuración del análisis antivirus

La ficha **Analizar** (ver Figura 29) permite definir los parámetros de análisis a la demanda: su cobertura, las acciones aplicadas a objetos infectados, la planificación de su ejecución. Esta ficha también sirve para determinar si el modo de protección en tiempo real estará activo.

Figura 29. Ficha **Analizar**

En la sección **Acción seleccionada en presencia de un objeto infectado**, especifique la acción aplicada en presencia de un objeto infectado:

- **Eliminar.**
- **Ignorar:** deja intacto el objeto infectado.
- **Cuarentena:** mueve los objetos infectados detectados a la carpeta de cuarentena.
- **Preguntar al usuario:** muestra un mensaje en pantalla acerca de la detección de un virus con la sugerencia de eliminar, mover a cuarentena o dejar intacto el objeto infectado.

Los demás parámetros son similares a los descritos en la sección 3.1.1 en la página 26.

3.1.2.5. Selección del origen de actualizaciones de las bases de Kaspersky Anti-Virus

La ficha **Origen de actualizaciones** (ver Figura 30) permite especificar el origen de las descargas de las actualizaciones de la base antivirus. Esta ficha también permite planificar la ejecución de las actualizaciones.

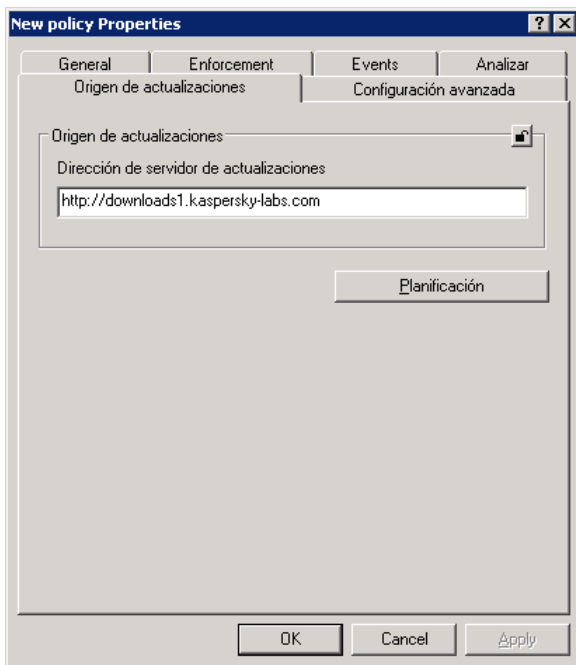
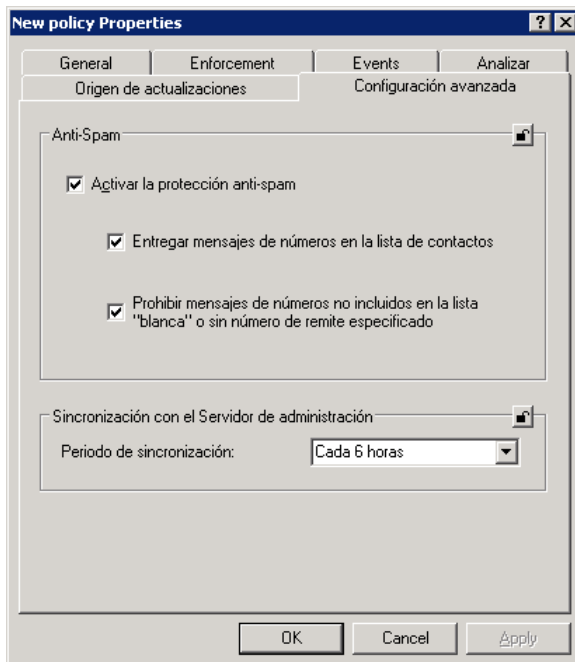


Figura 30. Ficha **Origen de actualizaciones**

3.1.2.6. Especificación de parámetros avanzados

La ficha **Configuración avanzada** (ver Figura 31) permite configurar el módulo Anti-Spam y definir la frecuencia de conexión con el Servidor de administración.

Figura 31. Ficha **Configuración avanzada**

3.2. Administración de los parámetros de aplicación

Los parámetros de la aplicación le permiten configurar la instalación de Kaspersky Anti-Virus en dispositivos móviles individuales dentro de un grupo, o en un dispositivo móvil local. Sólo puede modificar parámetros que no han sido bloqueados por una directiva (para obtener detalles ver sección 3.1 en la página 26).

Para modificar la configuración de la aplicación:

1. En la carpeta **Grupos**, seleccione la carpeta con el nombre del grupo contenedor del dispositivo móvil.
2. En el panel de resultados, seleccione el dispositivo en el que desea modificar los parámetros de aplicación. Seleccione **Propiedades** en el menú contextual o en el menú **Acciones**.

3. Se abrirá el cuadro de diálogo **Propiedades: Nombre de equipo** en la ventana principal de la aplicación. Seleccione la ficha **Aplicaciones** (ver Figura 32).

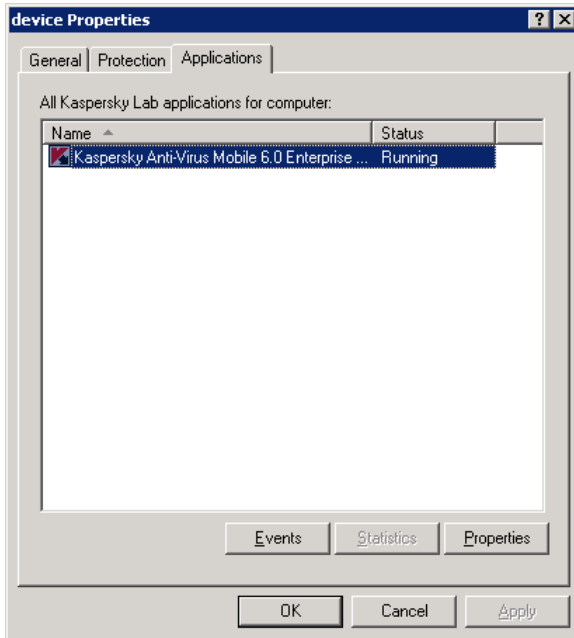


Figura 32. Ventana de propiedades del dispositivo móvil.
Ficha **Aplicaciones**

4. Seleccione la aplicación **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition**. En la parte inferior de la ventana se encuentran los botones siguientes:
 - **Eventos:** muestra la lista de eventos de aplicación ocurridos en los dispositivos móviles y registrados por el servidor de administración.
 - **Estadísticas:** visualiza las estadísticas de funcionamiento de la aplicación.
 - **Propiedades:** permite configurar la aplicación en la ventana abierta de propiedades de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition

3.2.1.1. Información acerca de la aplicación

La ficha **General** (ver Figura 33) permite examinar la información relativa a Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

La parte superior de la ventana contiene el nombre de la aplicación instalada, información sobre la versión, la fecha de instalación, su estado en el dispositivo móvil (en ejecución o detenida) así como información sobre el estado de las bases de Kaspersky Anti-Virus.

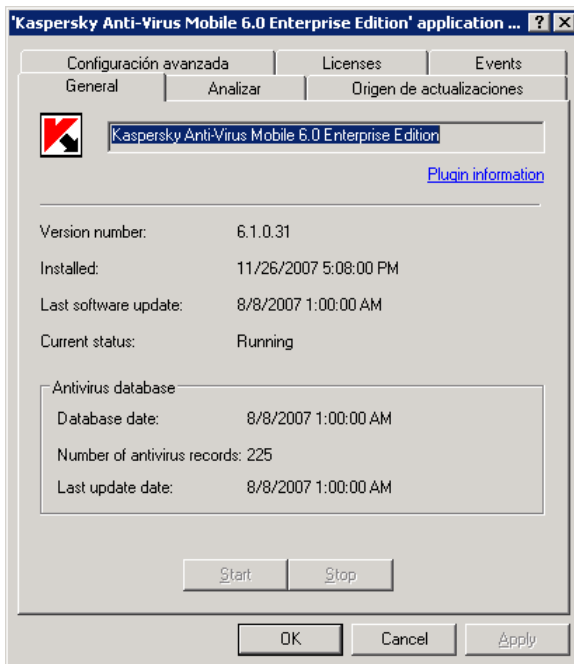
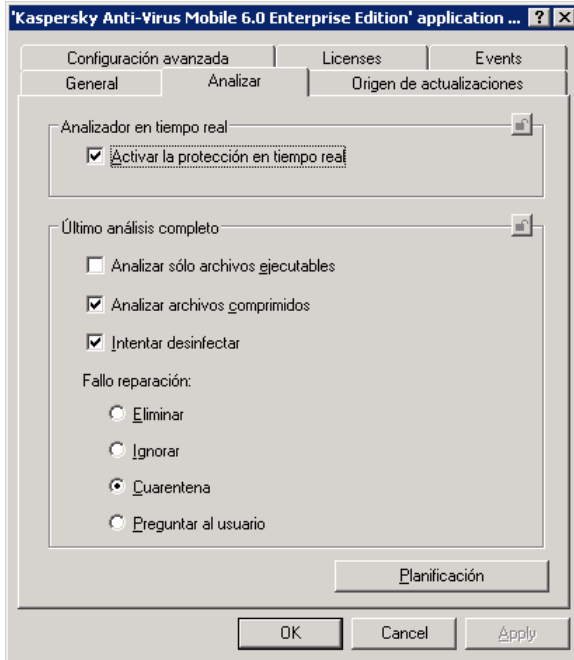


Figura 33. cuadro de diálogo de propiedades de la aplicación. La ficha **General**.

3.2.1.2. Información sobre los parámetros de la aplicación antivirus

La ficha **Analizar** (ver Figura 34) permite mostrar información relativa a la tarea de análisis a petición: su cobertura, la acción aplicada a objetos y la planificación de su ejecución. Esta ficha indica si la protección en tiempo real está activa en el dispositivo móvil.

Figura 34. Ficha **Analizar**

3.2.1.3. Información sobre el origen de actualizaciones

La ficha **Origen de actualizaciones** (ver Figura 35) proporciona información acerca del servidor origen de las descargas de las actualizaciones, de acuerdo con la configuración y los parámetros de planificación definidos para el dispositivo móvil seleccionado.

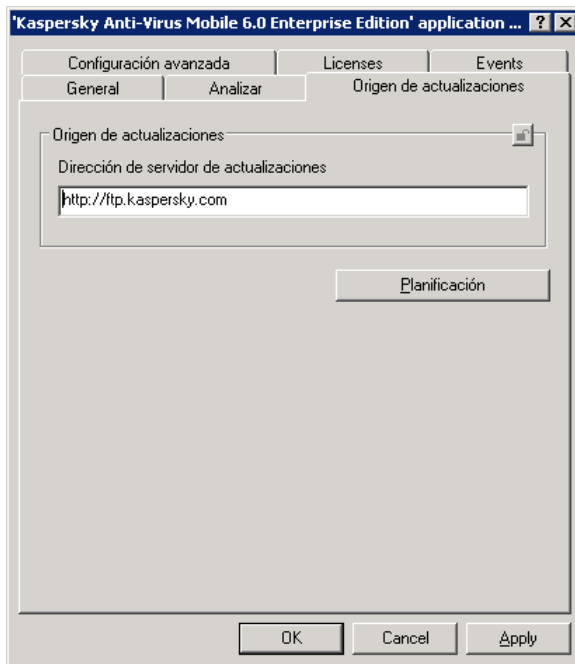


Figura 35. Ficha Origen de actualizaciones

3.2.1.4. Información acerca de los parámetros avanzados

La ficha **Configuración avanzada** (ver Figura 36) proporciona información acerca de la configuración del módulo Anti-Spam y la frecuencia de las comunicaciones con el Servidor de administración.

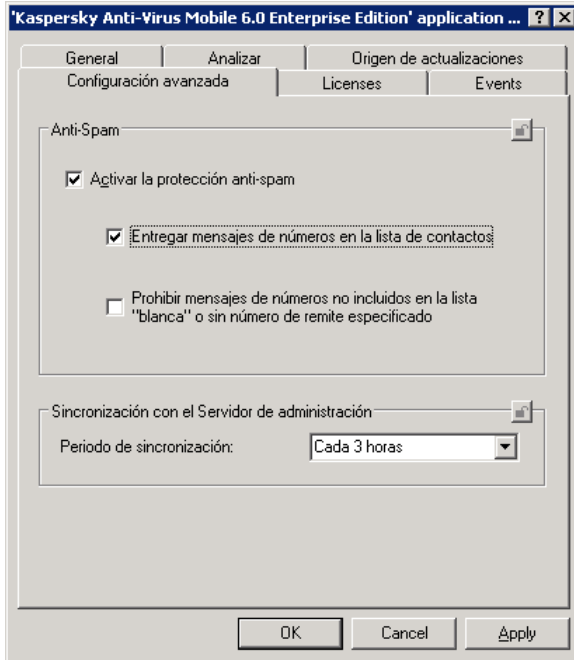
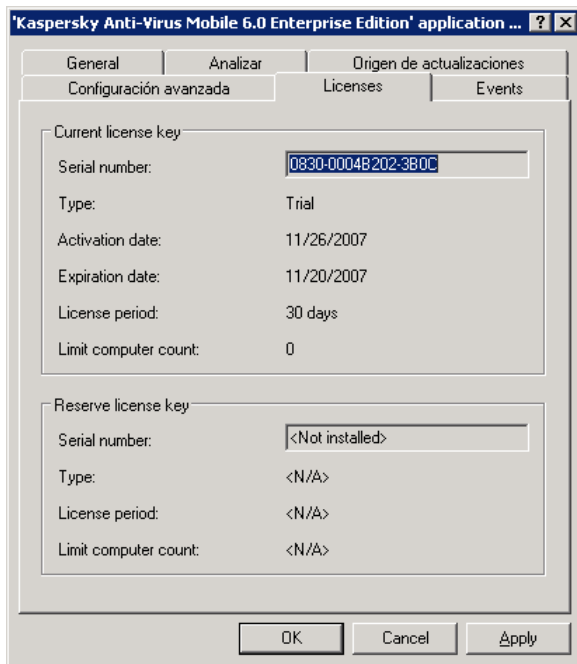


Figura 36. Ficha **Configuración avanzada**

3.2.1.5. Información sobre las llaves de licencia

La ficha **Licencia** (ver Figura 36) contiene información acerca de las llaves activa o de respaldo instaladas en este dispositivo móvil en particular. También informa sobre el periodo de validez y las restricciones de licencia de la llave activa. También informa sobre el periodo de validez y las restricciones de licencia de la llave activa.

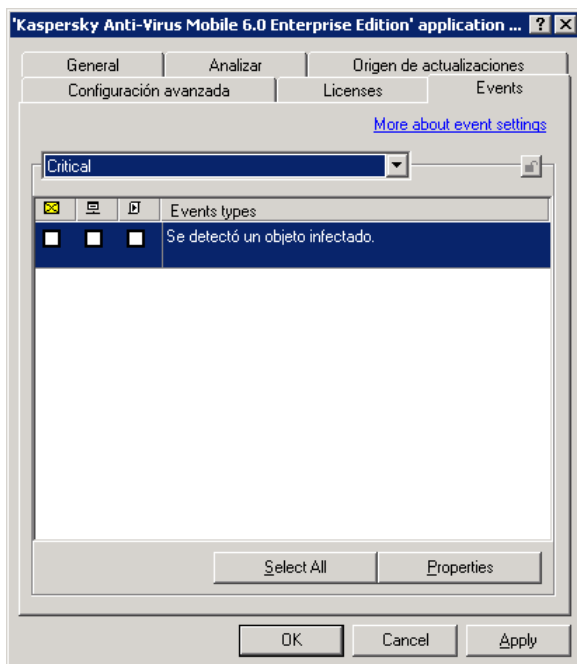
Figura 37. Ficha **Licencia**

3.2.1.6. Información acerca de eventos

Durante su funcionamiento, Kaspersky Anti-Virus genera un cierto conjunto de eventos. Cada evento incluye un indicador de su nivel de importancia. Existen cuatro niveles de importancia: evento crítico, fallo, advertencia y mensaje de información.

Los eventos de un mismo tipo pueden presentar diferentes niveles de importancia, en función de la situación en que éstos se producen.

La ficha **Eventos** (ver Figura 38) muestra los tipos de eventos que se producen durante el funcionamiento de la aplicación y que son registrados en el informe, así como la ubicación del informe y las condiciones de notificación del administrador o de otros usuarios.

Figura 38. Ficha **Eventos**

ANEXO A. KASPERSKY LAB

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

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

Hoy día, Kaspersky Lab tiene contratados a más de 450 especialistas, cada uno de los cuales es un experto en tecnología antivirus, con 10 de ellos en posesión de un M.B.A., otros 16 con un Doctorado, y dos expertos miembros permanentes de la CARO (Computer Anti-Virus Researcher's Organization).

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

Años de duro trabajo han convertido la empresa en uno de los fabricantes líderes de software de seguridad. Kaspersky Lab fue una de las primeras empresas de este tipo en desarrollar los mejores estándares para la defensa antivirus. Nuestro producto estrella, Kaspersky Internet Security, ofrece protección integral para todos los equipos de una red: estaciones de trabajo, servidores de archivos, sistemas de correo, cortafuegos y pasarelas Internet, así como equipos portátiles. Sus herramientas de administración adaptadas y sencillas utilizan los avances de la automatización para una rápida protección antivirus de toda la organización. Numerosos fabricantes conocidos utilizan el núcleo de Kaspersky Internet Security: Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israel), Sybari (EEUU), G Data (Alemania), Deerfield (EEUU), Alt-N (EEUU), Microworld (India) y BorderWare (Canadá).

Los clientes de Kaspersky Lab se benefician de una amplia oferta de servicios adicionales que garantizan no sólo un funcionamiento estable de nuestros productos sino también la compatibilidad con cualquier necesidad específica de negocio. La base antivirus de Kaspersky Lab se actualiza cada hora. Nuestra

organización ofrece a sus usuarios un servicio de asistencia técnica de 24 horas, disponible en numerosos idiomas, capaz de adaptarse a su clientela internacional.

A.1. Otros productos Kaspersky Lab

Kaspersky Lab News Agent

El agente de noticias está diseñado para entregar de forma periódica noticias publicadas por Kaspersky Lab, con notificaciones acerca de la actividad vírica actual y noticias recientes. El programa lee las cabeceras y contenidos de noticias disponibles desde el servidor de noticias de Kaspersky Lab con una frecuencia determinada.

El agente de noticias permite a los usuarios:

- Ver el indicador antivirus actualizado en la barra del sistema
- Suscribirse o cancelar su suscripción a las noticias
- Descargar las cabeceras de noticias a intervalo especificado y recibir notificaciones acerca de noticias frescas
- Examinar las noticias de los hilos seleccionados
- Revisar la lista y estado de las cabeceras
- Abrir el artículo completo en su navegador

El agente de noticias es una aplicación Microsoft Windows independiente, que puede usarse por sí sola o integrada en varias soluciones ofrecidas por Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

El programa es un servicio gratuito ofrecido a los visitantes del sitio Web corporativo de Kaspersky Lab. El servicio ofrece en línea un análisis antivirus eficiente de su equipo. Kaspersky OnLine Scanner se ejecuta directamente en su navegador. De este modo, el usuario obtiene rápidamente respuestas a cuestiones relacionadas con la posible infección de su equipo. Con este servicio, los visitantes pueden:

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

Kaspersky® OnLine Scanner Pro

Se trata de un servicio por suscripción ofrecido a los visitantes del sitio Web corporativo de Kaspersky Lab. El servicio ofrece en línea un análisis antivirus eficiente de su equipo y la neutralización de los archivos peligrosos. Kaspersky OnLine Scanner Pro se ejecuta directamente en su navegador. Con este servicio, los visitantes pueden:

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

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 está diseñado para proteger los equipos personales contra software dañino y es una combinación óptima de métodos convencionales de protección antivirus y de nuevas tecnologías proactivas.

El programa ofrece medios de análisis avanzados que incluyen:

- Análisis antivirus del tráfico de correo a nivel del protocolo de transmisión de datos (POP3, IMAP y NNTP para correo entrante y SMTP para mensajes salientes) sin tener en cuenta el cliente de correo utilizado, así como la desinfección de las bases de correo.
- Análisis antivirus en tiempo real del tráfico Internet que transita por HTTP.
- Análisis antivirus de archivos, directorios o unidades individuales. Además, es posible utilizar una tarea de análisis predeterminada para iniciar el análisis antivirus exclusivamente de zonas críticas y de objetos de inicio del sistema operativo Microsoft Windows.

La protección proactiva ofrece las características siguientes:

- **Control de cambios dentro del sistema de archivos.** El programa permite a los usuarios crear una lista de aplicaciones, para controlarlas de acuerdo con sus componentes. Ayuda a proteger la integridad de la aplicación contra los efectos de software dañino.
- **Supervisión de procesos en memoria viva (RAM).** Kaspersky Anti-Virus 7.0 informa a tiempo a los usuarios cuando detecta procesos peligrosos, sospechosos u ocultos, o cuando ocurren cambios no autorizados en los procesos activos.
- **Control de cambios en el Registro del sistema** gracias al control interno del Registro del sistema.

- **Control de procesos ocultos**, que ayuda a proteger contra el código dañino disimulado en el sistema operativo por técnicas de ocultación (rootkit).
- **Analizador heurístico**. Cuando analiza un programa, el analizador simula su ejecución y registra cualquier actividad sospechosa, como por ejemplo, la apertura o escritura en un archivo, el desvío de vectores de interrupción, etc. De acuerdo con este comportamiento, el programa toma una decisión acerca de la posible infección del programa por un virus. La simulación se realiza en un entorno virtual aislado que protege el equipo contra cualquier infección.
- **Restauración del sistema** después de ataques por software dañino, al registrar todos los cambios en el Registro o el sistema de archivos y posibilidad de anular estos cambios a petición del usuario.

Kaspersky® Internet Security 7.0

Kaspersky® Internet Security 7.0 es una solución integral de protección de equipos personales contra las principales amenazas a los datos, por ejemplo, virus, intrusos, correo no solicitado y software espía. Una interfaz de usuario común permite configurar y administrar todos los componentes de esta solución.

La característica de protección antivirus incluye:

- **Análisis antivirus del tráfico de correo** a nivel del protocolo de transmisión de datos (POP3, IMAP y NNTP para correo entrante y SMTP para mensajes salientes) sin tener en cuenta el cliente de correo utilizado. El programa dispone de complementos para clientes de correo más difundidos (Microsoft Office Outlook, Microsoft Outlook Express y The Bat!) y es capaz de desinfectar sus bases de correo.
- **Análisis antivirus en tiempo real del tráfico Internet** que transita por HTTP.
- **Protección del sistema de archivos**: análisis antivirus de archivos, directorios o unidades individuales. Además, la aplicación puede realizar un análisis antivirus exclusivamente de zonas críticas y de los objetos de inicio de Microsoft Windows.
- **Defensa proactiva**: el programa asegura la supervisión constante de la actividad de aplicaciones y procesos que se ejecutan en la memoria de acceso aleatorio, impidiendo cualquier cambio peligroso en el sistema de archivos o el Registro, y restaura el sistema después de una afección dañina.

La protección contra fraudes por Internet está garantizada por la capacidad de identificar intentos de fraude (phishing), para prevenir la pérdida de datos confidenciales (ante todo, sus contraseñas, sus cuentas bancarios y los números de tarjetas de crédito), así como de bloquear la ejecución de

secuencias de comandos peligrosas en páginas Web, ventanas emergentes y pancartas publicitarias. La característica de **bloqueo de llamadas con sobrecosto** ayuda a identificar cualquier software que intente utilizar su modem para conexiones ocultas no autorizadas a servicios telefónicos de pago, para evitar su actuación.

Kaspersky® Internet Security 7.0 **registra los intentos de análisis de los puertos de su equipo**, que anuncian con frecuencia ataques por la red y le defiende con éxito contra los ataques normales de intrusos. El programa utiliza **reglas definidas como básicas** para controlar todas las transacciones de red, examinando todos los **paquetes de datos entrantes y salientes**. **El modo invisible** (derivado de la tecnología SmartStealth™) **impide la detección de su equipo desde el exterior**. Cuando activa este modo, el sistema bloquea cualquier actividad de la red con la excepción de una pocas transacciones autorizadas por reglas definidas por el usuario.

El programa realiza un tratamiento complejo del filtrado del correo no deseado en mensajes de correo entrantes:

- Verificación de remitentes en listas negras y blancas (con las direcciones de sitios de fraudes).
- Examen de las frases en el cuerpo de los mensajes.
- Análisis del texto del mensaje mediante un algoritmo de autoaprendizaje.
- Identificación de datos no deseados enviados en archivos de imagen.

Kaspersky Anti-Virus for File Servers

Esta distribución ofrece una protección segura de los sistemas de archivos de servidores con Microsoft Windows, Novell NetWare, Linux y Samba, contra todos los tipos de software dañino. La suite incluye las aplicaciones Kaspersky Lab siguientes:

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

Características y funciones:

- *Protege el sistema de archivos del servidor en tiempo real*: Todos los archivos del servidor son analizados cuando se abren o guardan en el servidor
- *Prevención de epidemias víricas*;

- *Análisis a petición:* del sistema de archivos completo o de archivos o carpetas individuales;
- *Utiliza tecnologías de optimización* cuando analiza objetos en el sistema de archivos del servidor;
- *Anula los cambios en el sistema después de ataques de virus;*
- *Escalabilidad del paquete software* dentro de los límites de disponibilidad de los recursos del sistema;
- *Control del equilibrio de carga del sistema;*
- *Creación de una lista de procesos de confianza* cuya actividad en el servidor no está controlada por el paquete software;
- *Administración remota* del paquete software, incluyendo su instalación, configuración y administración centralizadas;
- *Copias de respaldo de los objetos infectados y eliminados* en caso de necesitar restaurarlos;
- *Cuarentena de los objetos sospechosos;*
- *Envío de notificaciones de eventos* sobre la actividad del programa al administrador del sistema;
- *Registro en informes detallados;*
- *Actualización automática* de las bases del programa.

Kaspersky Open Space Security

Kaspersky Open Space Security es un paquete a software con un acercamiento novedoso a la seguridad de las redes corporativas actuales, de cualquier tamaño, que ofrece sistemas de protección centralizados de la información y soporte para oficinas remotas y usuarios móviles.

La suite incluye cuatro programas:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Las particularidades de cada programa se indican a continuación.

Kaspersky WorkSpace Security es un programa de protección centralizada de estaciones de trabajo, tanto dentro como fuera de las redes corporativas, contra todas las amenazas modernas de Internet (virus, software espía, intrusiones y correo no solicitado).

Características y funciones:

- *Protección integral contra virus, software espía, intrusiones de piratas y correo no solicitado;*
- *Defensa proactiva* contra nuevos programas malignos cuyas firmas no han sido todavía incluidas en la base de datos;
- *Personal Firewall* con sistema detector de intrusiones y tentativas de ataque a la red;
- *Anulación de los cambios malévolos en el sistema;*
- *Protección contra tentativas de estafa y correo no solicitado;*
- *Redistribución dinámica de recursos* durante los análisis del sistema completo;
- *Administración remota* del paquete software, incluyendo su instalación, configuración y administración centralizadas;
- *Soporte para Cisco® NAC* (Network Admission Control);
- *Análisis del correo y tráfico Internet* en tiempo real;
- *Bloqueo de ventanas emergentes y pancartas publicitarias* cuando navega en Internet;
- *Funcionamiento seguro en cualquier tipo de red*, incluso inalámbrica (Wi-Fi);
- *Herramientas para crear discos de emergencia* que permiten recuperar el sistema después de un ataque vírico;
- *Amplio sistema de generación de informes* sobre el estado de la protección;
- *Actualizaciones automáticas de bases de datos;*
- *Soporte completo para sistemas operativos de 64 bits;*
- *Optimización del rendimiento de programas en portátiles* (tecnología Intel® Centrino® Duo);
- *Posibilidades de desinfección remota* (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security ofrece una protección óptima de los datos de su organización contra las amenazas actuales de Internet. Kaspersky Business Space Security protege las estaciones de trabajo y los servidores de archivos contra cualquier tipo de virus, troyanos y gusanos, evita epidemias víricas y asegura su información mientras los usuarios se benefician de un acceso instantáneo a los recursos de la red.

Características y funciones:

- Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;
- *Soporte para Cisco® NAC (Network Admission Control);*
- *Protección estaciones de trabajo y los servidores de archivos contra cualquier tipo de amenaza Internet;*
- *Tecnología iSwift para no repetir el análisis de archivos dentro de la red;*
- *Distribución de la carga entre los procesadores del servidor;*
- *Cuarentena de los objetos sospechosos en estaciones de trabajo;*
- *Anulación de los cambios malévolos en el sistema;*
- *Escalabilidad del paquete software dentro de la disponibilidad de los recursos del sistema;*
- *Defensa proactiva para estaciones de trabajo contra nuevos programas malignos cuyas firmas no han sido todavía incluidas en la base de datos;*
- *Análisis del correo y tráfico Internet en tiempo real;*
- *Personal Firewall con sistema detector de intrusiones y tentativas de ataque a la red;*
- *Protección del uso de redes inalámbricas (Wi-Fi);*
- *Autoprotección contra programas malignos;*
- *Cuarentena de los objetos sospechosos;*
- *actualizaciones automáticas de bases de datos.*

Kaspersky Enterprise Space Security

Este programa incluye componentes de protección de estaciones de trabajo y servidores vinculados contra cualquier tipo de amenaza Internet contemporánea. Elimina los virus del correo, mantiene segura la información mientras ofrece a los usuarios acceso seguro a los recursos de la red.

Características y funciones:

- *Protección de estaciones de trabajo y servidores de archivos contra cualquier tipo de virus, troyanos y gusanos;*

- *Protección de servidores de correo Sendmail, Qmail, Postfix y Exim;*
- *Análisis de todos los correos en Microsoft Exchange Server, incluyendo carpetas compartidas;*
- *Procesado de correos, bases de datos y otros objetos de servidores Lotus Domino;*
- *Protección contra tentativas de estafa y correo no solicitado;*
- *prevención contra el envío masivo de correo y las epidemias víricas;*
- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;
- Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;
- Soporte para Cisco® NAC (Network Admission Control);
- Defensa proactiva para estaciones de trabajo contra nuevos programas malignos cuyas firmas no han sido todavía incluidas en la base de datos;
- Personal Firewall con sistema detector de intrusiones y tentativas de ataque a la red;
- *Protección del uso de redes inalámbricas (Wi-Fi);*
- *Análisis del tráfico Internet en tiempo real;*
- *Anulación de los cambios malévolos en el sistema;*
- *Redistribución dinámica de recursos durante los análisis del sistema completo;*
- Cuarentena de los objetos sospechosos;
- *Amplio sistema de generación de informes sobre el estado de la protección;*
- *actualizaciones automáticas de bases de datos.*

Kaspersky Total Space Security

Esta solución supervisa todos los flujos de datos entrantes y salientes (correo, Internet y todas las comunicaciones de red). Incluye componentes de protección para estaciones de trabajo y equipo móviles, ofrece a los usuarios acceso seguro a la información de la organización y a Internet y garantiza comunicaciones seguras por correo.

Características y funciones:

- *Protección integral contra virus, software espía, intrusiones de piratas y correo no solicitado* en todos los niveles de la red corporativa, desde las estaciones de trabajo a las pasarelas Internet;
- Defensa proactiva para estaciones de trabajo contra nuevos programas malignos cuyas firmas no han sido todavía incluidas en la base de datos;
- *Protección de servidores de correo y servidores vinculados;*
- *Análisis del tráfico Internet* (HTTP/FTP) que entra en la red local, en tiempo real;
- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;
- *Prohibición de acceso a estaciones de trabajo infectadas;*
- *Prevención de epidemias víricas;*
- *Sistema de generación de informes centralizado* sobre el estado de la protección;
- Administración remota del paquete software, incluyendo su instalación, configuración y administración centralizadas;
- *Soporte para Cisco® NAC* (Network Admission Control);
- *Soporte para servidores proxy hardware;*
- *Filtra el tráfico Internet* mediante una lista de servidores de confianza, tipos de objetos y grupos de usuarios;
- *Tecnología iSwift para no repetir el análisis de archivos* dentro de la red;
- Redistribución dinámica de recursos durante los análisis del sistema completo;
- Personal Firewall con sistema detector de intrusiones y tentativas de ataque a la red;
- *Seguridad para los usuarios de cualquier tipo de red*, incluso inalámbrica (Wi-Fi);
- *Protección contra tentativas de estafa y correo no solicitado;*
- *Posibilidades de desinfección remota* (Intel® Active Management, Intel® vPro™);

- *Anulación de los cambios malévolos en el sistema;*
- *Autoprotección contra programas malignos;*
- *soporte completo para para sistemas operativos de 64 bits;*
- *actualizaciones automáticas de bases de datos.*

Kaspersky Security for Mail Servers

Este programa protege los servidores de correo y los servidores vinculados contra los programas malignos y el correo no solicitado. El programa incluye aplicaciones para la protección de todos los servidores de correo estándar (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix y Exim) y también le permite configurar una pasarela de correo dedicada. Esta solución incluye:

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

Sus características incluyen:

- Protección segura contra programas malignos o potencialmente peligrosos;
- Filtrado de correo no solicitado;
- Análisis de correos entrantes y salientes, incluyendo los adjuntos;
- Análisis antivirus de todos los correos en Microsoft Exchange Server, incluyendo carpetas compartidas;
- Procesado de correos, bases de datos y otros objetos de servidores Lotus Notes/Domino;
- Filtrado del correo por el tipo de adjunto;
- Cuarentena de objetos sospechosos;
- Sencillo sistema administrador del programa;
- Prevención de epidemias víricas;
- Supervisión del estado del sistema de protección mediante notificaciones;
- Generación de informes de actividad del programa;

- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;
- Actualizaciones automáticas de bases de datos.

Kaspersky Security for Internet Gateways

Este programa ofrece a todos los empleados de una organización acceso seguro a Internet, y la eliminación automática del software dañino o de riesgo en los datos entrantes por HTTP/FTP. Esta solución incluye:

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

Sus características incluyen:

- Protección segura contra programas malignos o potencialmente peligrosos;
- Análisis del tráfico Internet (HTTP/FTP) en tiempo real;
- Filtra el tráfico Internet mediante una lista de servidores de confianza, tipos de objetos y grupos de usuarios;
- Cuarentena de objetos sospechosos;
- Sencillo sistema administrador;
- Generación de informes de actividad del programa;
- Soporte para servidores proxy hardware;
- Escalabilidad del paquete software dentro de los límites de disponibilidad de los recursos del sistema;
- Actualizaciones automáticas de bases de datos.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam es una suite de software avanzado diseñada para ayudar a las organizaciones con redes de tamaño pequeño o mediano a luchar contra la invasión de correos no solicitados (spam). El producto combina una tecnología revolucionaria de análisis lingüístico con todos los métodos modernos de filtrado del correo (incluyendo listas negras de DNS y funciones de análisis formal de los mensajes). Su combinación única de servicios permite a los usuarios identificar y destruir hasta un 95% del tráfico no deseado.

Kaspersky® Anti-Spam actúa como un filtro instalado a la entrada de la red, desde donde comprueba el tráfico entrante de mensajes, en busca de objetos identificados como correo no solicitado. La aplicación es compatible con cualquier sistema de mensajería existente en las instalaciones del cliente, en un servidor de correo existente o dedicado.

Kaspersky® Anti-Spam obtiene sus altas prestaciones gracias a actualizaciones diarias de la base de contenidos filtrados, a partir de las muestras proporcionadas por los especialistas del laboratorio lingüístico. Las bases se actualizan cada 20 minutos.

Kaspersky Anti-Virus® for MIMESweeper

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

El programa es un complemento software que actúa como antivirus y procesa el tráfico de correo entrante y saliente en tiempo real.

A.2. Cómo encontrarnos

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

Soporte técnico	Encontrará información de asistencia técnica en la dirección http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
Información	WWW: http://www.kaspersky.com http://www.viruslist.com Correo: info@kaspersky.com

ANEXO B. CONTRATO DE LICENCIA

Contrato estándar de licencia de usuario final

IMPORTANTE PARA TODOS LOS USUARIOS: LEA ATENTAMENTE EL SIGUIENTE CONTRATO DE LICENCIA ("CONTRATO") PARA KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION ("SOFTWARE") FABRICADO POR KASPERSKY LAB ("KASPERSKY LAB").

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

SI HA COMPRADO ESTE SOFTWARE EN UN MEDIO FÍSICO, Y HA ROTO EL ESTUCHE DEL CD, USTED ("UN INDIVIDUO O UNA ENTIDAD") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. SI NO ACEPTA TODOS LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO NO ABRA EL ESTUCHE DEL CD NI DESCARGUE, INSTALE O UTILICE ESTE SOFTWARE.

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

EL SOFTWARE KASPERSKY DIRIGIDO A CONSUMIDORES INDIVIDUALES QUE NO HA SIDO ADQUIRIDO POR INTERNET NO PODRÁ SER DEVUELTO NI CAMBIADO, SALVO CLÁUSULAS CONTRARIAS DEL DISTRIBUIDOR QUE VENDIÓ EL PRODUCTO. EN ESTE CASO, KASPERSKY LAB NO SE HARÁ RESPONSABLE DE LAS CONDICIONES DE DICHO DISTRIBUIDOR.

EL DERECHO A DEVOLUCIÓN Y REINTEGRO SÓLO SE EXTIENDE AL COMPRADOR ORIGINAL.

De aquí en adelante en todas las referencias al "Software" se considerará que éste incluye el código de activación de software proporcionado por Kaspersky Lab como parte de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

1. *Contrato de licencia.* Si los gastos de licencia han sido pagados, y de acuerdo con los términos y condiciones de este Contrato, Kaspersky Lab le concede por el presente Contrato un derecho de uso no exclusivo y no transferible de una copia de la versión especificada del Software y documentación que la acompaña ("Documentación") únicamente para sus propios fines de negocio. Puede instalar una sola copia del Software en un sólo equipo.

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

1.1.1 El Software está "en uso" en un equipo cuando está cargado en la memoria temporal (es decir, memoria de acceso-aleatorio o RAM) o instalado en la memoria permanente (es decir, el disco duro, un CDROM u otro dispositivo de almacenamiento) del equipo. Esta licencia sólo le autoriza a reproducir las copias adicionales del Software que sean necesarias para su uso legítimo, y sólo para producir copias de seguridad, a condición de que todas las copias contengan toda la información de propiedad del Software. Deberá mantener un registro con el número y ubicación de todas las copias del Software y Documentación y tomará las precauciones razonables para impedir que el Software sea copiado o utilizado sin autorización.

1.1.2 El software protege el equipo contra virus y ataques de red cuyas firmas aparezcan en la base de la aplicación y de ataques de red disponible en los servidores de actualización de Kaspersky Lab.

1.1.3 En caso de que venda el equipo donde tiene instalado el software, tomará medidas previas para asegurarse de que todas las copias del Software han sido borradas.

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

1.1.5 No le está permitido a Usted, ni a terceras partes, corregir errores ni, en general, modificar, adaptar, traducir ni crear productos derivados de este Software, ni permitir a un tercero hacer copias de él (salvo que lo autorice expresamente este contrato).

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

1.1.7 No le está permitido facilitar a terceros el código de activación o el archivo llave de licencia, ni facilitar a terceros el acceso al código de activación o a la llave de licencia. El código de activación y la llave de licencia son datos confidenciales.

1.1.8 Kaspersky Lab podrá pedirle al Usuario que instale la última versión del Software (última versión y último paquete de mantenimiento).

1.1.9 No podrá utilizar este Software en herramientas automáticas, semiautomáticas o manuales diseñadas para crear firmas de identificación de virus, rutinas de detección de virus, ni cualquier otra información o código para la detección de código o de datos dañinos.

2. Soporte.

(i) Kaspersky Lab le proporcionará los servicios de soporte ("Servicios de soporte") para el periodo definido a continuación, especificados en el Archivo llave de licencia e indicados en la ventana "Servicio", a partir de la fecha de activación en los siguientes supuestos:

(a) Pago de la cuota vigente de soporte, y:

(b) Cumplimentación satisfactoria del Formulario de Suscripción a los Servicios de Soporte que acompaña este Contrato o en el sitio Internet de Kaspersky Lab, lo que requiere indicar el código de activación proporcionado por Kaspersky Lab junto con este Contrato. Si usted ha satisfecho esta condición o no para el suministro de Servicios de soporte estará a la discreción absoluta de los servicios de soporte.

El servicio de soporte estará disponible después de la activación del Software. El servicio de soporte técnico de Kaspersky Lab está también habilitado para solicitar al Usuario final datos de registro adicionales para identificarle con derecho a asistencia.

Hasta la activación del Software, o la obtención del identificador de Usuario final (Id. de cliente), el soporte técnico tan sólo facilita ayuda para la activación del software y el registro del Usuario final.

(ii) Al completar el formulario de Suscripción de los Servicios de Soporte, acepta los términos de la Política de privacidad de Kaspersky Lab disponible en la dirección www.kaspersky.com/privacy, y acepta explícitamente que sus datos sean transmitidos a otros países que el suyo, tal y como se describe en la Política de privacidad.

- (iii) Los Servicios de soporte terminarán si no los renueva anualmente pagando la cuota de Soporte anual y volviendo a rellenar el formulario de suscripción a los Servicios de soporte.
- (iv) "Servicio de soporte" significa:
 - (a) Actualizaciones horarias de la base antivirus;
 - (b) Actualizaciones de la base contra ataques de red;
 - (c) Actualizaciones de la base antispam;
 - (d) Actualizaciones gratuitas del software, incluidas actualizaciones de la versión de antivirus;
 - (e) Soporte técnico por Internet y teléfono proporcionados por el Fabricante o el Distribuidor;
 - (f) Detección de virus y actualizaciones para su desinfección en un plazo de 24 horas.
- (v) El Servicio de soporte se proporciona sólo cuando la última versión del Software (incluyendo los paquetes de mantenimiento) disponible en el sitio Internet oficial de Kaspersky Lab (www.kaspersky.com) está instalada en su equipo.

3. *Derechos de propiedad.* El Software está protegido por las leyes de derechos de autor. Kaspersky Lab y sus proveedores se reservan y retienen todos los derechos, titularidad e intereses de y sobre el Software, incluyendo todos los derechos de autor, patentes, marcas registradas y otros derechos de propiedad intelectual. Su posesión, instalación o uso del Software no le transfiere ningún título de propiedad intelectual sobre el Software: usted no adquiere ningún otro derecho sobre el Software salvo especificado en este Contrato.

4. *Confidencialidad.* Usted acepta que el Software y la Documentación, incluidos el diseño y estructura de los programas individuales, constituyen información confidencial y propietaria de Kaspersky Lab. No debe desvelar, proporcionar u ofrecer la información confidencial en cualquiera de sus formas a terceras partes sin autorización escrita de Kaspersky Lab. Deberá tomar medidas razonables de seguridad para proteger esta información confidencial y, sin que esto suponga una restricción a lo anterior, proteger lo mejor posible el código de activación.

5. *Garantía limitada.*

- (i) Kaspersky Lab le garantiza que durante seis (6) meses desde la primera descarga o instalación del Software adquirido en un soporte físico, su funcionamiento responderá esencialmente a lo descrito por la Documentación, si se ejecuta de forma apropiada y de la manera especificada en la Documentación.
- (ii) Al seleccionar este software, usted acepta toda la responsabilidad derivada de la satisfacción de sus necesidades. Kaspersky Lab no

- garantiza que el Software y/o la Documentación son adecuados para sus necesidades, funcionarán de forma ininterrumpida ni que estén libres de errores;
- (iii) Kaspersky Lab no garantiza que este Software identifique todos los virus ni todos los correos indeseados, ni que el Software no detecte erróneamente en ocasiones un virus en un archivo no infectado por ese virus;
 - (iv) Su único recurso y la entera responsabilidad de Kaspersky Lab por la ruptura de la garantía mencionada en el párrafo (i) será, según la decisión de Kaspersky Lab, reparación, reemplazo o reembolso del Software si ha informado de esto a Kaspersky Lab o sus proveedores durante el período de la garantía. Debe proporcionar toda la información que pueda ser necesaria para ayudar al Proveedor a determinar el elemento defectuoso;
 - (v) (v) La garantía mencionada en (i) no se aplicará si usted (a) realiza o causa cualquier modificación a este Software sin autorización de Kaspersky Lab, (b) utiliza el Software de una manera no prevista, o (c) de manera no autorizada por este Contrato;
 - (vi) Las garantías y condiciones especificadas en este Contrato sustituyen todas las otras condiciones, garantías u otros términos acerca de las prestaciones o prestación prevista, ausencia o tardanza en las prestaciones del Software o la Documentación que puedan tener efecto entre Kaspersky Lab y usted, excepto en los casos especificados en este párrafo (vi), o estuvieren implícitas o incorporadas a este Contrato o cualquier contrato colateral, por normativa legal, derecho común o cualquier otra razón, que quedan todas excluidas (incluidas, sin limitación alguna, a condiciones implícitas, garantías u otros términos relativos a niveles razonables de calidad, conveniencia, capacidad y cuidados necesarios).

6. *Limitación de responsabilidad.*

- (i) Nada en este Contrato excluirá o limitará la responsabilidad de Kaspersky Lab por (a) acto delictuoso de engaño, (b) muerte o daños personales debidos al incumplimiento de obligaciones relativas a la salud o por violación negligente de este Contrato o (c) cualquier responsabilidad que no quede excluida por ley.
- (ii) De acuerdo con el párrafo (i) anterior, el Proveedor no será responsable (por contrato, daño, restitución o cualquier otra forma) por las siguientes pérdidas o daños (si tales pérdidas o daños estaban previstas, eran previsibles, o conocidas de cualquier otra forma):
 - (a) Pérdida de ingresos;

- (b) Pérdida de beneficios reales o anticipados (incluyendo la pérdida de beneficios en contratos);
 - (c) Pérdida del uso de dinero;
 - (d) Pérdida de ahorros anticipados;
 - (e) Pérdida de negocios;
 - (f) Pérdida de oportunidad;
 - (g) Pérdida de buena fe;
 - (h) Pérdida de reputación;
 - (i) Pérdida, daños o corrupción de datos, o:
 - (j) Cualquier otra pérdida o daño incidental o consecuente causado de cualquier forma (incluyendo, para eliminar cualquier duda, pérdida o daño del tipo especificado en los párrafos (ii), (a) - (ii), (i).
- (iii) De acuerdo con el párrafo (i), la responsabilidad de Kaspersky Lab (por contrato, daño, restitución o cualquier otra forma) que es resultado de o está conectada con la entrega del Software, estará en cualquier circunstancias limitada a una cantidad no mayor que la pagada por el Software.

7. Este contrato contiene el pleno conocimiento de las partes en cuanto a su contenido y reemplaza todos y cualquier declaración, acuerdo o compromiso entre Usted y Kaspersky Lab, tanto oral o como por escrito o formulado en negociaciones entre nosotros o con nuestros representantes antes de este Acuerdo y para los contratos entre las partes respecto a las cuestiones antedichos que cesan a partir del momento en que este Contrato entre en vigor.

El uso de la versión de demostración del Software no le da acceso al Soporte técnico descrito en la cláusula 2 de este CLUF, ni le autoriza a vender a terceros la copia en su posesión.

Está autorizado a utilizar el Software con fines de demostración durante el periodo especificado en el archivo llave de licencia, a contar del momento de la activación (puede ver dicho periodo en la ventana Servicio de la interfaz del programa).