KASPERSKY LAB

Kaspersky® Administration Kit versión 6.0

Primeros pasos

KASPERSKY® ADMINISTRATION KIT
VERSION 6.0

Primeros Pasos

http://www.kaspersky.com/

Fecha de revisión: Enero de 2007

Contenidos

CAPÍTULO 1. INTRODUCCIÓN

Este documento describe los primeros pasos que debe dar un administrador de seguridad de una red para instalar, de forma rápida y eficiente, un sistema de protección antivirus basado en aplicaciones Kaspersky Lab en una red corporativa usando **Kaspersky Administration Kit**.

Este documento muestra un escenario simple en el que la protección antivirus está instalada en varios equipos sin utilizar la jerarquía de los Servidores de Administración. Para realizar una instalación con éxito, los equipos deben tener instalado alguno de los siguientes sistemas operativos: Microsoft Windows 2000 con Service Pack 1 o superior; Microsoft Windows XP Professional con Service Pack 1 o superior; Microsoft Windows XP Professional x64 o superior; Microsoft Windows Server 2003 o superior; Microsoft Windows Server 2003 x64 o superior; Microsoft Windows NT4 con Service Pack 6a o superior.

Este documento también describe el proceso de actualización de aplicaciones Kaspersky Lab, de la versión 4.x a la versión 6.x.

Para una información detallada de la funcionalidad de la aplicación, consulte la Guía del Administrador y la Guía de Implementación.

Kaspersky Administration Kit 5 ha sido diseñado para la administración del sistema de protección antivirus en una red corporativa. La aplicación permite al administrador realizar las siguientes acciones:

- Crear una red lógica que garantice la protección antivirus de la red corporativa.
- Distribuir aplicaciones Kaspersky Lab a través de la red.
- Administrar, de forma remota, el sistema de protección antivirus desde una única ubicación.
- Recibir notificaciones de eventos relacionados con la protección antivirus a través de la red.
- Acumular estadísticas e informes de todas las instalaciones.

Kaspersky Administration Kit consta de los siguientes componentes:

- El **Servidor de Administración** permite a los administradores gestionar las aplicaciones Kapersky Lab instaladas en los equipos de la red desde una ubicación centralizada. El Servidor de Administración almacena

todos los datos del sistema de protección antivirus corporativo en una base de datos MSDE 2000 con Service Pack 3 o superior, SQL Server 2000 con Service Pack 3 o superior, MySQL 5.0.22 (página de códigos predeterminada UTF-8), Microsoft SQL 2005 o superior o Microsoft SQL 2005 Express o superior. Las bases de datos deben estar en funcionamiento en la red corporativa antes del comienzo de la instalación y del funcionamiento del Servidor de Administración. MSDE 2000 con Service Pack 3 puede ser instalado con Kaspersky Administration Kit 5.0. Con este fin, su equipo debe tener instalado Microsoft Data Access Components (MDAC) 2.8 o superior.

- El **Agente de Red** se instala en los equipos protegidos por aplicaciones Kaspersky Lab que soportan la administración a través de **Kaspersky Administration Kit**. Este componente coordina la interacción entre las aplicaciones Kaspersky Lab, que se ejecutan en equipos cliente, y el Servidor de Administración. El Agente de Red recibe instrucciones del Servidor de Administración y envía información sobre el estado de protección de los equipos cliente.

- La **Consola de Administración** proporciona una interfaz de usuario para los servicios de administración del Servidor y del Agente. Este componente se agrega en el Microsoft Management Console (MMC).

CAPÍTULO 2. PRIMEROS PASOS

Para crear un sistema de protección eficaz en su red corporativa, siga estos pasos:

1. Instale Microsoft Data Access Components (MDAC) 2.8 o superior. Esto no es necesario si este componente ya está instalado en su red corporativa.

2. Instale MSDE 2000 SP 3 (ver sección 10, página 7), Microsoft SQL 2000 SP 3, MySQL 5.0.22 (código de página predeterminado UTF-8), Microsoft SQL 2005 o superior o Microsoft SQL Express o superior. Omita este paso si en su red ya está instalado uno de estos servidores de datos.

3. Instale el Servidor de Administración y la Consola de Administración (ver sección 2.2, página 8).

4. Configure los parámetros iniciales del sistema de protección antivirus mediante el Asistente de Inicio Rápido (ver sección 2.3, página 8).

5. Cree grupos de administración (ver sección 2.4, página 10) si no se han creado mediante el Asistente de Inicio Rápido. Los grupos de administración permiten administrar grupos de equipos cliente como una sola entidad aplicando directivas y tareas de grupo.

6. Instalar de forma remota el Agente de Red en equipos cliente para permitir a sus aplicaciones antivirus interactuar con el Servidor de Administración. (ver sección 2.5, página 11).

7. Instalar de forma remota en los equipos cliente seleccionados la aplicación Kaspersky Lab que garantice la protección antivirus de la red corporativa y soporte la administración a través de Kaspersky Administration Kit (ver sección 7, página 12). Si estas aplicaciones ya están instaladas, este paso no es necesario.

8. Configure las actualizaciones de descargas de la base antivirus, a través de Internet, mediante el Servidor de Administración y compruebe el éxito de la operación. Compruebe que las bases de datos están actualizadas en los equipos cliente (ver sección 2, página 13).

9. Configure las opciones de notificación al administrador sobre eventos relacionados con virus en equipos cliente.

10. Ejecute un análisis a petición en equipos cliente y compruebe la tarea de notificación ejecutada en equipos cliente (ver sección 3, página 15).

11. Vea un informe sobre protección antivirus en los equipos cliente y el número de virus detectados por las aplicaciones Kaspersky Lab (ver sección 2, página 16).

Si completó con éxito el paso anterior, es el momento de crear un sistema de protección antivirus seguro para su red corporativa.

Las siguientes secciones describen estos pasos detalladamente.

2.1. Instalar MSDE 2000

Omita este paso si MSDE 2000 SP 3, Microsoft SQL 2000 SP 3, MySQL 5.0.22 (código de página predeterminado UTF-8), Microsoft SQL 2005 o superior o Microsoft SQL Express o superior está instalado en la red corporativa
Antes de instalar MSDE, debe instalar Microsoft Data Access Components (MDAC) 2.8 o superior (el paquete de distribución está disponible en el sitio Web de Microsoft).

Para instalar MSDE 2000 desde el paquete incluido en Kaspersky Administration Kit:

1. Seleccione un equipo donde instalar la base de datos del Servidor de Administración. Normalmente, éste es el mismo equipo donde se instalará el Servidor de Administración.

2. Ejecute localmente el archivo **setup.exe**, que se encuentra en la carpeta **MSDE2KSP3**, del CD de instalación de Kaspersky Administration Kit 5.0.

3. Siga las instrucciones de instalación del asistente.

Una vez que haya realizado todos los pasos de la instalación, se instalará la aplicación MSDE 2000 SP.3 en el equipo seleccionado. MSDE 2000 SP 3 no necesita administración.

El Servidor de Administración utiliza MSDE 2000 SP 3 o SQL Server 2000 SP 3 para almacenar los datos de la protección antivirus en una base de datos centralizada.

La aplicación **klbackup** incluida en el paquete de distribución de Kaspersky Administration Kit crea copias de seguridad de los datos del Servidor de Administración. Para más información sobre esta utilidad, consulte la Guía del Administrador.

2.2. Instalación del Servidor de Administración y de la Consola de Administración

Durante la instalación, puede seleccionar la instalación del Servidor de Administración y la Consola de Administración o sólo la Consola de Administración. El Servidor de Administración no puede ser instalado sin la Consola. La opción por defecto es la instalación de ambos componentes.

Si es necesario, la Consola de Administración puede ser instalada en otro equipo y administrar el Servidor de Administración a través de la red.

Para instalar el Servidor de Administración y/ o la consola de administración:

1. Seleccione un equipo donde instalar los componentes. Si en su red existe una estructura de dominio de Windows, es aconsejable que instale el Servidor de Administración en un miembro del dominio.

   Puede instalar el Servidor de Administración 6.x en el mismo equipo en el que funciona el Servidor de Administración 4.x. Los Servidores de Administración de las versiones 6.x y 4.x son independientes el uno del otro y pueden funcionar simultáneamente en el mismo equipo sin problemas de compatibilidad.

   Es aconsejable que posea permisos de administrador del dominio cuando instale el producto. Esto le permitirá crear automáticamente grupos **KLAdmins** y **KLOperators** y proporcionar una identidad necesaria a la cuenta bajo la que el Servidor de Administración funcionará.

2. Ejecute el archivo setup.exe del CD de instalación de Kaspersky Administration Kit 5.

3. Siga las instrucciones del asistente.

   Seleccione la cuenta del administrador del dominio como la cuenta de servicio desde la que iniciará el Servidor de Administración en este equipo.

2.3. Asistente de inicio rápido

Para realizar la configuración inicial de los parámetros de la protección antivirus:

1. Ejecute la Consola de Administración haciendo clic en **Inicio → Programas → Kaspersky Administration Kit → Kaspersky Administration Kit**.

2. Conéctese al Servidor de Administración haciendo clic en el nodo **Servidor de Administración** del árbol de consola. Acepte el certificado del servidor.

3. Abra el menú contextual y seleccione **Asistente de Inicio Rápido**.

4. Espere hasta que el Servidor de Administración finalice la búsqueda y detecte todos los equipos de su red.

5. Cree grupos de administración mediante uno de los siguientes métodos:

   - Si sólo está probando con varios equipos, seleccione la opción **Manual** para agregar manualmente equipos cliente de prueba al grupo.

   - Si distribuye el sistema de protección antivirus en toda la red corporativa, seleccione uno de los siguientes métodos de creación automática de redes lógicas:

     - **Agregar equipos a un grupo usando la red de Windows**. En este caso, la red lógica estará basada en la estructura de dominios de Windows y grupos de usuarios (los grupos de administración coincidirán con los dominios de Windows y los grupos de usuario).

     - **Agregar equipos a un grupo usando la estructura de la versión anterior de Kaspersky Administration Kit**. En este caso, la red lógica estará basada en la red de Kaspersky Administration Kit 4.x.

6. Especifique opciones para el envío de notificaciones por correo electrónico generadas por las aplicaciones Kaspersky Lab. Estos valores pueden ser editados en las propiedades del Servidor de Administración. Para más información, consulte la Guía del Administrador.

7. Ejecute un proceso para crear directivas de aplicaciones antivirus y tareas múltiples que deban configurar el correcto funcionamiento del sistema de protección antivirus en la red corporativa. Kaspersky Administration Kit 5 usa directivas de grupo para aplicar configuraciones uniformes a todos los equipos de un grupo. Las tareas son acciones realizadas por el software antivirus en todos los equipos de un grupo.

   Se crearán los siguientes objetos:

   - Directivas de nivel superior para Kaspersky Anti-Virus for Windows Workstations 5.0 y 6.0 con parámetros predeterminados. Posteriormente, puede ver y modificar la configuración de la directiva. Para aplicar los cambios que haya realizado en la directiva a los equipos cliente e impedir que el usuario modifique estos valores, use el símbolo  .

   - Una tarea global para la actualización del Servidor de Administración a través de Internet.

     La aplicación descargará actualizaciones de la base antivirus y de los módulos de programa, desde los servidores de actualización Kaspersky Lab, y los guardará en la carpeta compartida especificada durante la instalación del Servidor de Administración. Los equipos cliente recuperarán las actualizaciones desde esta carpeta compartida. A continuación, para conseguir más flexibilidad cuando los equipos cliente recuperen las actualizaciones, puede distribuir las actualizaciones a los Servidores de Administración esclavo y a los Agentes de Actualización (ver detalles en la Guía del Administrador). Para configurar los parámetros de recuperación de actualizaciones desde los servidores de actualización Kaspersky Lab, haga clic en el botón **Parámetros de Actualización.**

   - Se creará una tarea de grupo de alto nivel, con parámetros por defecto, para actualizar las bases de datos antivirus en los equipos cliente. Los equipos cliente serán configurados para recuperar actualizaciones desde esta carpeta compartida.

- Se creará una tarea de análisis a petición, con parámetros por defecto, para equipos cliente.

8. Indique si la tarea para recibir actualizaciones del Servidor de Administración debe ser iniciada inmediatamente o según la planificación.

9. En la ventana final, indique si el Asistente de distribución debe iniciarse inmediatamente después de que se complete el Asistente de Inicio Rápido.

2.4. Crear un grupo de administración

Para agregar un nuevo grupo a la red lógica,

1. En el árbol de consola o la carpeta **Grupos** del panel de detalles, seleccione un grupo al que quiera agregar un nuevo grupo.
2. Abra el menú contextual y haga clic en **Nuevo → Grupo** para iniciar el Asistente de Nuevo Grupo.
3. Siga las instrucciones del asistente.
4. Mueva los equipos cliente seleccionados del grupo **Red** al nuevo grupo usando cortar y pegar o arrastrar y soltar.

> Para crear un conjunto de equipos y moverlos al grupo de administración en base a algún criterio, utilice el comando **Buscar equipo** del menú contextual (o el mismo comando del menú **Acción**). Ver detalles en la Guía del Administrador.

Los equipos cliente seleccionados pueden tener Kaspersky Lab's Anti-Virus 4.x. Los sistemas de administración de las versiones 4.x y 5.x trabajan de forma independiente uno respecto al otro. En caso de distribuir Kaspersky Anti-Virus 6.x sobre la versión 4.x, la versión 4.x será automáticamente eliminada y reemplazada por la versión 6.0.

2.5. Instalación remota del Agente de Red

Para distribuir (instalar de forma remota) el Agente de Red desde una ubicación remota:

1. Ejecute el Asistente de Distribución de Aplicaciones del menú contextual de la Consola de Administración en la Consola de Administración.

2. Seleccione el paquete de instalación del Agente de Red creado por el Asistente de Inicio Rápido. Este paquete se creará durante la instalación del Servidor de Administración y contiene la configuración utilizada por el Agente de Red para conectarse al Servidor de Administración.

3. Seleccione los equipos del grupo de administración que contiene los equipos destino en los que se instalará el Agente de Red.

4. Configure los parámetros de instalación remota.

5. Si es necesario, introduzca la cuenta de acceso a los equipos cliente. Si la cuenta del servicio del Servidor de Administración no tiene permisos de administrador para los equipos cliente seleccionados, utilice la cuenta predeterminada.

6. Durante el siguiente paso del asistente, se creará una tarea de grupo para la distribución del Agente de Red en los equipos seleccionados. En la ventana del asistente, puede ver los resultados de la ejecución de la tarea en modo de tiempo real.

7. Cuando la tarea haya finalizado, podrá ver los resultados de la tarea y salir del Asistente de Distribución de Aplicaciones.

8. Para asegurar que el Servidor de Administración pueda establecer conexiones con el Agente de Red en cualquier momento, debe abrirse el puerto UDP, número 15000, en el equipo cliente. Si no puede abrir el puerto UDP, marque la casilla **No cortar conexión con el Servidor de Administración** en la ficha **General** del cuadro de diálogo **Propiedades:<Nombre de equipo>** utilizada para configurar los parámetros de los equipos cliente.

Para marcar que la instalación finalizó con éxito, marque la opción **Propiedades** en el menú contextual de uno de los equipos en el que acabe de terminar la instalación del Agente de Red. Compruebe que la aplicación Kaspersky Network Agent muestra el estado **En Ejecución** en la ficha **Aplicaciones**.

Si la distribución de la aplicación se realizó con éxito, pero el Agente de Red no puede conectarse al Servidor de Administración, use la utilidad kinagchik.exe. Esta utilidad está incluida en el Kit de distribución del Agente de Red y ubicada en la carpeta raíz de instalación del Agente de Red después de la instalación de este componente. Cuando realice la ejecución desde la línea de comandos, esta utilidad le proporcionará diagnósticos detallados de los parámetros de conexión

del Servidor de Administración. Una descripción de acciones detallada se facilita en el Libro de Consulta.

2.6. Distribución de la Aplicación Kaspersky Anti-virus

Esta sección se centra en la instalación de Kaspersky Anti-Virus for Windows Workstations desde una instalación remota. La distribución de otras aplicaciones Kaspersky Lab es similar a lo descrito a continuación.

Algunas aplicaciones Kaspersky Lab que soportan administración a través de Kaspersky Administration Kit pueden ser instaladas únicamente de forma local (más detalles en la guía de la aplicación concreta).

Para distribuir de forma remota Kaspersky Anti-Virus for Windows Workstations en equipos conectados a la red,

1. Cree un paquete de instalación de Kaspersky Anti-Virus for Workstations mediante un asistente. El asistente se iniciará mediante la entrada **Instalación Remota** del menú contextual.

   El archivo .**kpd** requerido para crear el paquete de instalación está ubicado en la raíz del archivo de distribución de Kaspersky Anti-Virus for Workstations. La archivo de clave de licencia para Kaspersky Anti-Virus for Workstations está localizado también en el directorio raíz. Especifique la clave de licencia utilizada para el funcionamiento de Kaspersky Anti-Virus Windows Workstations.

   Si fuera necesario, configure los parámetros del paquete de instalación Es aconsejable, por ejemplo, que permita el reinicio automático de los equipos cliente.

2. Ejecute el Asistente de Distribución de Aplicaciones del menú contextual del Servidor de Administración.

3. Instale Kaspersky Anti-Virus for Workstations desde el paquete de instalación, de la misma manera que el Agente de Red (ver sección 0, página 11). También puede instalar el Agente de Red junto a Kaspersky Anti-Virus for Windows Workstation.

   Puede instalar Kaspersky Anti-Virus 5.x en equipos con aplicaciones 4.x instaladas. En este caso, las aplicaciones 4.x serán sobrescritas automáticamente por la última versión 6.x.

Para verificar que la instalación ha sido correcta, seleccione un equipo cliente en el que acabe de instalar la aplicación y abra su ventana de **Propiedades**. Abra la ficha **Aplicaciones** y compruebe que la aplicación Kaspersky Anti-Virus for Workstations 5 tiene el estado **En ejecución**. La ficha **Tareas** debe mostrar la tarea de protección en tiempo real ejecutada por Kaspersky Anti-Virus for Workstations 5.

2.7. Comprobación del funcionamiento de la tarea de actualización

Para comprobar que los equipos cliente recuperan correctamente las actualizaciones:

1. Ejecute la tarea de actualización del Servidor de Administración en el nodo Tarea del nivel superior del árbol de consola. Esta tarea se crea automáticamente por el Asistente de Inicio Rápido. La aplicación descargará actualizaciones desde los servidores de actualización de Kaspersky Lab y las guardará en la carpeta compartida especificada durante la instalación del Servidor de Administración. Espere hasta que se complete la tarea.

   Haga clic en el botón **Historial** para ver el resultado de las tareas.

   Para ver la lista de actualizaciones descargadas, haga clic en el nodo **Actualizaciones** del árbol de consola.

   Los detalles del procedimiento de actualización están disponibles en la Web de Kaspersky Lab (http://www.kaspersky.ru/avupdates).

2. Ejecute la tarea de actualización de grupo en equipos cliente. Esta tarea se crea por el Asistente de Inicio Rápido y se almacena en la carpeta **Tareas** del nodo **Grupo**. Espere hasta que se complete la tarea.

   Haga clic en el botón **Historial** para ver el resultado de las tareas.

La tarea, creada por el Asistente de Inicio Rápido, actualiza equipos cliente usando la conexión entre el Agente de Red y el Servidor de Administración. Son también válidos los siguientes métodos de actualización de equipos:

- Desde la carpeta compartida en el Servidor de Administración;

- Desde la carpeta compartida en el Servidor de Administración principal (si se usa jerarquía de Servidor).
- Desde los servidores de actualización de Kaspersky Lab.
- Mediante un Servidor FTP o HTTP;

Copiar las últimas actualizaciones desde la carpeta compartida, para ello los equipos cliente deben tener permiso de lectura sobre esa carpeta. SI por alguna razón esto no es posible, puede utilizarse un servidor FTP o HTTP para distribuir las actualizaciones a los equipos cliente. Crear un directorio FTP o HTTP enlazado a la subcarpeta **Actualizaciones**, en la carpeta compartida en la que el Servidor de Administración guardará las actualizaciones descargadas (por ejemplo, ftp://admserver/actualizaciones). Especificar esta carpeta (ftp://admserver/updates) como el origen de actualizaciones de la tarea de actualización ejecutada en equipos cliente.

2.8. Configuración de Notificaciones

Para configurar notificaciones sobre eventos relacionados con la protección antivirus,

1. Abra la ficha **Procesamiento de Eventos** desde las propiedades de la directiva de nivel superior para una aplicación antivirus (por ejemplo, Kaspersky Anti-Virus for Workstations).

2. En esta ficha, especifique los eventos sobre los que quiere ser notificado y seleccione la forma de envío de estas notificaciones.

   Para probar el sistema de notificación (ver sección 3 en página 15), es suficiente con configurar una notificación para el evento **Virus encontrado**.

3. Use el símbolo  para todos los valores que configure con el fin de extenderlos a todos los equipos cliente. Para aplicar cambios, pulse el botón **Aplicar**.

4. Puede comprobar los parámetros que ha configurando mediante el envío de un mensaje de forma manual. Con este fin, pulse el botón **Probar**. Se abrirá una ventana de notificación de prueba. En caso de error, se mostrará información detallada sobre ello.

2.9. Comprobación del sistema de notificación y la tarea de análisis a petición

Para comprobar el sistema de notificación y la tarea de análisis a petición

1. Intente copiar el test de virus **Eicar** a un equipo protegido. La copia fallará si la tarea de protección en tiempo real esta en ejecución. Debería recibir una notificación de que el virus ha sido detectado y además, este evento debe ser registrado en el nodo **Eventos** del árbol de consola.

   El "test de virus" Eicar no es realmente un virus, ya que no contiene código que pueda causar daños a su equipo. Sin embargo, la mayoría de los productos antivirus marcan este archivo como un virus. Puede descargar el "test de virus" desde la Web oficial de la organización EICAR en http://www.eicar.org/anti_virus_test_file.htm.

2. Detenga la tarea de protección en tiempo real en el equipo cliente. Copie el test de virus **Eicar** en el equipo cliente y habilite la protección en tiempo real nuevamente.

3. Ejecute la tarea de grupo de análisis a petición para un grupo de equipos cliente. Como resultado, la aplicación debería detectar el archivo eicar.com y enviar la notificación correspondiente. Debe aparecer un registro de este evento en el nodo **Eventos** del árbol de consola.

2.10. Generación de Informes

A partir de los datos del registro de eventos de Kaspersky Administration Kit almacenados en el Servidor de Administración, la aplicación puede generar informes del estado actual del estado del sistema de protección antivirus. Las plantillas predeterminadas de informes pueden verse desde el nodo **Informes** del árbol de consola.

Existen siete modelos estándar de plantillas que se corresponden con los siguientes tipos de informes:

- **Informe de la versión de las bases de datos Antivirus**
- **Informe de error**

- **Informe de licencia**
- **Informe de los equipos mas infectados**
- **Informe de protección**
- **Informe de la versión de software**
- **Informe de actividad de virus**
- **Informe sobre aplicaciones de terceros**
- **Informe sobre ataques de red.**

Por ejemplo, si crea un informe de la actividad de virus mediante el uso de la plantilla correspondiente, contendrá información sobre todas las incidencias de virus registradas por Kaspersky Administration Kit.

Si agrega un equipo que no tenga el Agente de Red a un grupo de administración, el informe de protección incluirá información acerca de que uno de los equipos del grupo no está protegido.

CAPÍTULO 3. ACTUALIZACIÓN DE 4.X A LA VERSIÓN 6.X

Esta sección describe como actualizar desde aplicaciones Kaspersky Lab 4.x a Kaspersky Anti-Virus for Workstations versión 6.x o Kaspersky Anti-Virus for Windows Servers versión 6.x. Algunos de los pasos han sido descritos anteriormente. Aquí, puede encontrar instrucciones paso a paso para una transición sin contratiempos.

Kaspersky Administration Kit 6.x funciona de forma independiente de Kaspersky Administration Kit 4.x. El sistema de administración para la versión 5.x administra únicamente aplicaciones de la versión 5.x y el sistema de administración de las versiones 6.x y 4.x administra la versión 4.x. Por lo tanto, durante la instalación, dos sistemas de administración pueden funcionar juntos en los equipos de la red.

A continuación se describe un escenario típico de transición:

1. Instale la versión 6.x del Servidor de Administración. Puede instalarlo en el mismo equipo de la versión 4.x.

2. Cree una estructura de red lógica de grupos de administración para aplicaciones 6.x. Puede importar esta estructura desde el sistema de administración 4.x.

3. Cree directivas y tareas de grupo para aplicaciones 5.x y 6.x en la red lógica. Configure los parámetros requeridos de la protección antivirus y establezca las reglas para el procesamiento de los eventos relacionados con la protección antivirus

4. Especifique qué equipos cambiarán de la versión 4.x a la versión 5.x y 6.x.

5. Cree un paquete de instalación para aplicaciones de la versión 5.x y 6.x e instale las aplicaciones 5.x y 6.x en los equipos seleccionados. En el transcurso de la instalación, las aplicaciones 4.x serán automáticamente reemplazadas por aplicaciones 5.x y 6.x.

6. Los equipos en los que instale la versión 5.x del software antivirus serán añadidos a la red lógica del Servidor de Administración 5.x. El resto de

equipos continúa siendo administrado por el Sistema de Administración 4.x.

De esta forma, el sistema de protección antivirus de su empresa, basado en la versión anterior, transferirá, de forma gradual a la versión 5.x y 6.x, las aplicaciones administradas por la versión del sistema de administración 6.x.

CAPÍTULO 4. CONCLUSIÓN

Kaspersky Administration Kit 5 ofrece una variedad de características administrativas, que se extienden más allá de las mencionadas en este documento. Este documento le introduce en Kaspersky Administration Kit 5 para mostrarle como comenzar a usar la aplicación, y distribuir el sistema de protección antivirus a los equipos de la red. Este guión simple se ocupa de las cuestiones básicas relacionadas con la construcción de un sistema de protección permitiendo al administrador:

- Distribuir y configurar el sistema de administración de la protección antivirus.
- Distribuir aplicaciones antivirus en equipos cliente desde una única ubicación
- Definir la directiva de protección antivirus
- Crear y probar la viabilidad de operación de la tarea de actualización en equipos cliente
- Poner a prueba el funcionamiento de la tarea de protección en tiempo real
- Crear y poner a prueba la tarea de análisis a petición en equipos cliente
- Establecer reglas para el envío de notificaciones después de eventos críticos
- Generar y visualizar informes creados por el sistema de protección antivirus.

APPENDIX 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 todo tipo de programas dañinos, correo no solicitado o indeseable, y ataques de red.

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

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

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

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

Los clientes de Kaspersky Lab se benefician de un amplio abanico de servicios adicionales que garantizan no sólo un funcionamiento estable de nuestros productos sino también la compatibilidad con cualquier necesidad específica de negocios. La base antivirus de Kaspersky Lab se actualiza en tiempo real cada 3 horas. Nuestra organización ofrece a sus usuarios un servicio de asistencia técnica de 24 horas, disponible en numerosos idiomas, capaz de adaptarse a su clientela internacional.

A.1. Otros productos Kaspersky Lab

Kaspersky Anti-Virus® Personal

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

- **Protección antivirus en tiempo real**: análisis antivirus de todos los objetos que son ejecutados, abiertos o guardados dentro del equipo protegido.

- **Análisis a petición**: análisis y desinfección del equipo completo o de discos, archivos o carpetas seleccionados. El análisis a petición puede ser iniciado manualmente desde la interfaz de usuario o automáticamente, de acuerdo con una planificación.

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

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

Kaspersky Anti-Virus Personal reconoce más de 700 formatos de archivos comprimidos y datos archivados, analiza automáticamente el contenido y elimina el código dañino de archivos **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** e **ICE.**

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

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

Kaspersky Anti-Virus® Personal Pro

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

Características de Kaspersky Anti-Virus® Personal Pro:

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

Kaspersky® Anti-Hacker

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

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

La tecnología **SmartStealth**™ impide que los piratas puedan detectar su equipo desde el exterior. En este modo invisible, la aplicación funciona de forma transparente para mantener su equipo protegido mientras navega por el Web. La aplicación ofrece toda la transparencia y facilidad de acceso a la información que pueda esperar.

Kaspersky Anti-Hacker bloquea los ataques maliciosos más frecuentes y monitoriza las tentativas de análisis de puertos de su equipo.

La configuración de la aplicación se reduce a elegir entre 5 niveles de seguridad. De forma predeterminada, la aplicación se inicia en modo aprendizaje, que configura automáticamente su sistema de seguridad, en función de sus respuestas a diferentes eventos. De este modo, la protección se ajusta a sus preferencias específicas y a sus necesidades particulares.

Kaspersky® Security para PDA

Kaspersky® Personal Security Suite es un programa diseñado para la organización de la protección completa de equipos personales Windows. La suite evita que los programas peligrosos y potencialmente engañosos penetren en cualquier origen de datos y le proteja de los intentos inautorizados de acceder a los datos de su equipo, al igual que bloquea el correo no deseado.

Kaspersky Personal Security Suite tiene las siguientes características:

- Protección antivirus de datos guardados en su equipo;
- Protección de usuarios de Microsoft Outlook y Microsoft Outlook Express ante los correos no deseados;
- Protección de su equipo ante el acceso no autorizado, y también ante los ataques externos a través de la red desde su LAN o Internet.

Kaspersky® OnLine Scanner

Este programa es un servicio gratuito disponible para los visitantes del sitio Web de la compañía para realizar análisis eficaces de su equipo y desinfectar online los archivos infectados. Kaspersky OnLine Scanner se ejecuta en el navegador mediante la tecnología ActiveX® de Microsoft. Los usuarios pueden recibir rápidamente una respuesta de su interés relativa a la infección con software malicioso. Durante el análisis, el usuario puede:

- excluir archivos y bases de datos de correo del alcance del análisis.
- seleccionar una base antivirus estándar o extendida a usar para el análisis.
- guardar informes con el resultado del análisis en formato txt y html.

Kaspersky® OnLine Scanner Pro

Este programa es un servicio de suscripción disponible para los visitantes del sitio Web de la compañía para realizar análisis eficaces de su equipo y desinfectar online los archivos infectados. Kaspersky OnLine Scanner Pro se ejecuta en el navegador mediante la tecnología ActiveX® de Microsoft. Durante el análisis, el usuario puede:

- excluir archivos y bases de datos de correo del alcance del análisis.
- seleccionar una base antivirus estándar o extendida a usar para el análisis.

Guardar informes con el resultado del análisis en formato txt y html.

Kaspersky® Security para PDA

Kaspersky Security para PDA ofrece protección antivirus de los datos almacenados en equipos PDA con sistema operativo Palm o Windows CE. El paquete software incluye una combinación óptima de las herramientas antivirus siguientes:

- **analizador antivirus** para analizar a petición los datos almacenados tanto en el PDA como en una tarjeta de expansión;

- **monitor antivirus** que intercepta los virus en archivos copiados de otros portátiles o transferidos mediante la tecnología HotSync™.

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

Kaspersky Anti-Virus® Business Optimal

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

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

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

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

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

Kaspersky® Corporate Suite

Este paquete proporciona una protección antivirus completa de redes corporativas de cualquier tamaño al igual que una protección antivirus ampliada, exhaustiva y compleja. El paquete de componentes ha sido desarrollado para proteger cualquier integrante de una red corporativa, incluso en entornos mixtos. Kaspersky Corporate Suite es compatible con la mayoría de los sistemas

operativos y aplicaciones instalados en una empresa. Todos los componentes del paquete son administrados desde una consola con interfaz de usuario unificada. Kaspersky Corporate Suite ofrece un sistema de protección seguro y de alto rendimiento totalmente compatible con las necesidades de su configuración de red.

Kaspersky Corporate Suite ofrece protección antivirus completa para:

- Estaciones de trabajo con Windows 98/ME, Windows NT/2000/XP Workstation y Linux;
- Servidores de archivos y aplicaciones con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD y OpenBSD, y Linux;
- Clientes de correo: Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail y Qmail;
- Pasarelas Internet: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- Equipos portátiles (PDAs) con Microsoft Windows CE y Palm OS, y también smartphones con Windows Mobile 2003 for Smartphone y Microsoft Smartphone 2002.

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

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

Kaspersky® Anti-Spam

Kaspersky Anti-Spam es una aplicación avanzada diseñada para ayudar a las corporaciones con redes de tamaño pequeño o mediano a luchar contra la propagación de correos no deseados (spam). El producto combina una tecnología revolucionaria de análisis lingüístico con todos los métodos modernos de filtrado del correo, incluyendo lista negra 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 basura. La aplicación es compatible con cualquier sistema de mensajería existente en las instalaciones del cliente, en un servidor de correo existente o dedicado.

El alto rendimiento de Kaspersky Anti-Spam se garantiza con la actualización diaria de las bases de filtrado de contenidos, a partir de las muestras proporcionadas por los especialistas del laboratorio lingüístico. Las bases de datos se actualizan cada 20 minutos.

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix es una solución diseñada para el procesamiento del correo electrónico enviado a través de SMTP contra los virus. La aplicación contiene un número de herramientas adicionales para filtrar el tráfico de correo electrónico por el nombre y tipo MIME de documentos adjuntos y una serie de herramientas que reduce la carga en el sistema de correo y previene contra los ataques externos. El soporte de Lista negra DNS proporciona protección de correos electrónicos provenientes de servidores introducidos en estas listas como orígenes para la distribución de correos electrónicos.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange realiza un análisis antivirus de los mensajes de correo entrantes y salientes al igual que de todos los mensajes almacenados en el servidor, incluidos los mensajes almacenados en carpetas públicas y correspondencia de filtros no solicitados mediante las tecnologías de anti-spam “inteligente” en combinación con las tecnologías de Microsoft. La aplicación analiza todos los mensajes que llegan al Servidor de Intercambio a través del protocolo SMTP para detectar la presencia de virus, mediante las tecnologías antivirus de Kaspersky Lab y contra la presencia de características de SPAM, filtrado de spam mediante los atributos convencionales (dirección de correo, dirección IP, tamaño de la carta, título) y analizando el contenido de la carta y de sus documentos adjuntos mediante la tecnología "inteligente" que incluye las firmas gráficas únicas para la identificación gráfica de SPAM. El análisis incluye tanto el cuerpo del mensaje como los archivos adjuntos.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway es una solución completa que proporciona una protección total a los usuarios del sistema de correo. Esta aplicación instalada entre la red corporativa e Internet analiza todos los componentes de los mensajes de correo electrónico contra la presencia de virus y otros elementos maliciosos (Spyware, Adware, etc.) y realiza un filtrado anti-spam centralizado del flujo de mensajes. Esta solución también incluye algunas características adicionales de filtrado de tráfico de correos.

A.2. Cómo contactar con nosotros

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
Información general	WWW http://www.kaspersky.com/ http://www.viruslist.com Correo electrónico: sales@kaspersky.com

APPENDIX B. CONTRATO DE LICENCIA

Contrato licencia de usuario final IMPORTANTE PARA TODOS LOS USUARIOS: LEA ATENTAMENTE EL SIGUIENTE CONTRATO DE LICENCIA ("CONTRATO") PARA EL SOFTWARE ESPECIFICADO ("SOFTWARE") FABRICADO POR KASPERSKY LAB (“KASPERSKY LAB”).

SI HA ADQUIRIDO ESTE SOFTWARE POR INTERNET HACIENDO CLIC SOBRE EL BOTÓN ACEPTAR, USTED ("UN INDIVIDUO O ENTIDAD JURÍDICA") ACEPTA LAS OBLIGACIONES DE ESTE CONTRATO. I 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 TERMINOS Y CONDICIONES DE ESTE CONTRATO NO ABRA EL ESTUCHE DEL CD NI DESCARGUE, INSTALE O UTILICE ESTE SOFTWARE. SI HA ROTO LA FUNDA DEL CD O HA ABIERTO EL PAQUETE, NO PODRÁ SOLICITAR LA DEVOLUCIÓN DEL IMPORTE DEL SOFTWARE. EL SOFTWARE KASPERSKY DIRIGIDO A CONSUMIDORES INDIVIDUALES (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) 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. NO SE DEVOLVERÁ EL IMPORTE DEL RESTO DE PRODUCTOS. EL DERECHO A DEVOLUCIÓN Y REINTEGRO SÓLO SE EXTIENDE AL COMPRADOR ORIGINAL.

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

1. 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 copia del Software en un equipo, puesto de trabajo, agenda personal u otro dispositivo electrónico para el que el Software ha sido diseñado (cada uno es un "Sistema cliente"). Si la licencia del Software contempla un conjunto compuesto por varios productos, esta licencia se aplicará a todos los productos de este Software, de acuerdo con todas las limitaciones o condiciones de uso descritas en la lista de precios correspondiente o en el paquete de cada uno de estos productos del Software.

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

1.1.1 El Software está "en uso" en un Sistema cliente cuando está cargado en la memoria temporal (es decir, memoria de acceso-aleatorio o RAM) o instalado en la memoria permanente) por ej.: disco duro, CDROM, u otro dispositivo de almacenamiento) de ese Sistema cliente. Esta licencia sólo le autoriza a reproducir las copias adicionales del Software que sean necesarias para su uso legítimo, y sólo para producir copias de seguridad, a condición de que todas las copias contengan toda la información de propiedad del Software. 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 Si vende el Sistema cliente en que el Software está instalado, se asegurará que se han borrado previamente todas las copias del Software.

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

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

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

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

1.2 Uso en Modo Servidor. Sólo puede usar el Software en un Sistema cliente o en un Servidor ("Servidor") dentro de un entorno multiusuario o en red ("Modo Servidor") si tal uso está autorizado en la lista de precios o en el embalaje del Software. Se requiere una licencia separada para cada Sistema cliente o "Terminal" que puedan conectarse al Servidor en un momento dado; esta obligación no depende de si tales Sistemas Clientes o "terminales" autorizados se conectan simultáneamente, ni si acceden y usan el Software realmente. La utilización de herramientas software o hardware para reducir el número de Sistemas Cliente o "Terminales" que acceden o utilizan el Software directamente (por ejemplo, "multiplexación" o "agrupación" de software o hardware) no reduce el número de licencias requeridas, es decir: el número requerido de licencias será igual al número de entradas distintas del software o hardware multiplexado o agrupado. Si el número de Sistemas Cliente o "Terminales" que puedan conectarse al Software supera el número de licencias adquiridas, debe disponer de un mecanismo razonable para garantizar que el uso del Software cumple con las limitaciones especificadas para la licencia obtenida. Esta licencia le autoriza a crear e instalar copias autorizadas de la Documentación para cada Sistema cliente o Terminal que lo necesite para su uso legítimo, con la condición de que en cada copia aparezcan todos los anuncios relativos a la propiedad de la Documentación.

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

2. Duración. Este contrato es válido para el periodo especificado en el archivo llave (el archivo exclusivo necesario para activar completamente el Software: consulte el menú Ayuda/Acerca de, y para versiones Unix/Linux consulte la nota relativa a la fecha de caducidad del archivo llave) salvo por razones de finalización anticipada como se describe a continuación. Este Contrato terminará automáticamente si no respeta cualquiera de las condiciones, limitaciones u otros requisitos especificados en este contrato. Si el Contrato carecerá de vigor o expirará, debe destruir inmediatamente todas las

copias del Software y la Documentación. Puede terminar este Contrato en cualquier momento destruyendo todas las copias del Software y la Documentación.

3. Soporte.

(i) Kaspersky Lab le proporcionará los servicios de soporte ("Servicios de soporte") para un período de un año en los términos especificados a continuación:

(a) Pago de la cuota de servicio de soporte actual; y:

(b) Cumplimentación del Formulario de Suscripción para el servicio de soporte suministrado con este Contrato o disponible en el sitio Web de Kaspersky Lab que le exigirá que incluya el archivo Llave de Identificación proporcionado por Kaspersky Lab según este Contrato. Si usted cumple esta condición del suministro de Servicios de soporte, se someterá a los servicios de soporte.

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

(iii) Al completar el formulario de Suscripción de los Servicios de Soporte, acepta los términos de la Política de privacidad de Kaspersky Lab disponible en la dirección www.kapersky.com/privacy, y acepta explícitamente que los datos se transmitan a otros países que el suyo como especificado en la Política de privacidad.

(iv) "Servicio de soporte" significa:

(a) Actualizaciones diarias de bases antivirus;

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

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

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

4. Derechos de propiedad. El Software está protegido por las leyes de derechos de autor. Kaspersky Lab y sus proveedores se reservan y retienen

todos los derechos, titularidad e intereses de y sobre el Software, incluyendo todos los derechos de autor, patentes, marcas registradas y otros derechos de propiedad intelectual. Su posesión, instalación o uso del Software no le transfiere ningún título de propiedad intelectual sobre el Software: usted no adquiere ningún otro derecho sobre el Software salvo especificado en este Contrato.

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

6. Garantía limitada.

(i) Kaspersky Lab le garantiza que durante seis (6) meses desde la primera descarga o instalación del Software adquirido en un soporte físico, su funcionamiento corresponderá esencialmente de acuerdo con lo descrito por la Documentación, si se ejecuta de forma apropiada y de la manera especificada en la Documentación.

(ii) Usted acepta toda la responsabilidad por la selección de este Software para que satisfaga todas sus necesidades. Kaspersky Lab no garantiza que el Software y/o la Documentación son adecuados para sus necesidades, funcionarán de forma ininterrumpida ni que estén libres de errores;

(iii) Kaspersky Lab no garantiza que este Software identifique todos los virus conocidos, ni que no detecte ocasionalmente por error un virus en un archivo que no está infectado por ese virus;

(iv) Su único recurso y la entera responsabilidad de Kaspersky Lab por la ruptura de la garantía mencionada en el párrafo (i) será, según la decisión de Kaspersky Lab, reparación, reemplazo o reembolso del Software si ha informado de esto a Kaspersky Lab o sus proveedores durante el periodo de la garantía. Debe proporcionar toda la información que pueda ser necesaria para ayudar al Proveedor a determinar el 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) use el Software de una manera no prevista, o © utiliza el Software 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 (v) o se implicarían o se incorporarían a este Contrato o cualquier contrato colateral, si por el estatuto, derecho común o cualquier otra forma todos se excluyen por el presente (incluido, pero sin limitarse a, condiciones implícitas, garantías u otros términos acerca de la calidad satisfactoria, conveniencia o competencia y cuidado necesarios).

7. 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 de leyes sanitarias o violación negligente de este Contrato o (iv) cualquier responsabilidad que no queda 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 actuales o anticipadas (incluida pérdida de beneficios en contratos);

(c) Pérdida del uso de dinero;

(d) Pérdida de ahorros anticipados;

(e) Pérdida de negocios;

(f) Pérdida de oportunidad;

(g) Pérdida de buena fe;

(h) Pérdida de reputación;

(i) Pérdida de información, su daño o corrupción; o:

(j) Cualquier otra pérdida o daño incidental o consecuente causado de cualquier forma (incluido, para eliminar cualquier duda, pérdida o daño del tipo especificado en los párrafos (ii), (a) - (ii), (i).

(iii) Según al párrafo (i), la responsabilidad de Kaspersky Lab (en el contrato, acto delictuoso, restitución o cualquier otra forma), que es resultado de

o está conectada con la provisión del Software, se limitará en todas las circunstancias a un monto no mayor del que Usted pagó por el Software.

8. La elaboración e interpretación de este Contrato estará regido de acuerdo con la legislación de Inglaterra y Gales. Por la presente, las partes se someten a la jurisdicción de los tribunales de Inglaterra y Gales a menos que Kaspersky Lab, como demandante, inicie procedimientos en cualquier tribunal de jurisdicción competente.

9. (i) Este contrato contiene el pleno conocimiento de las partes en cuanto a su contenido y reemplaza todos y cualquier declaración, acuerdo o compromiso entre Usted y Kaspersky Lab, tanto oral o como por escrito o formulado en negociaciones entre nosotros o con nuestros representantes antes de este Acuerdo y para los contratos entre las partes respecto a las cuestiones antedichos que cesan a partir del momento en que este Contrato entre en vigor. Excepto lo especificado en los párrafos (ii) - (iii), no tendrá derecho a reembolso en caso de invocar la existencia de falsas declaraciones en el momento de firmar este Contrato ("Falseamiento") y Kaspersky Lab no será responsable por nada que se salga de los términos de este Contrato.

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

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