

KASPERSKY LAB

Kaspersky[®] Administration Kit 6.0

Guía de Implementación

KASPERSKY® ADMINISTRATION KIT 6.0

Guía de Implementación

Kaspersky Lab Ltd.

Visite nuestro sitio Web: <http://www.kaspersky.com/>

Fecha de revisión: Enero de 2007.

Contenidos

CAPÍTULO 1. KASPERSKY® ADMINISTRATION KIT	5
1.1. Objetivo, estructura y funciones principales	5
1.2. Requisitos software y hardware	7
1.3. Kit de Distribución.....	8
1.4. Servicio de soporte para usuarios registrados	8
1.5. Objetivo de este documento	9
1.6. Convenciones.....	9
CAPÍTULO 2. ESQUEMAS CONVENCIONALES DE DISTRIBUCIÓN DE LA PROTECCIÓN ANTIVIRUS	11
2.1. Esquemas de distribución de la protección antivirus en los equipos de la red lógica	11
2.2. Construir un sistema centralizado de administración de protección antivirus...	12
CAPÍTULO 3. INSTALACIÓN DE KASPERSKY ADMINISTRATION KIT.....	14
3.1. Instalar MSDE desde el paquete de distribución de Kaspersky Administration Kit	14
3.2. Instalar el Servidor de Administración y la Consola de Administración	16
3.3. Eliminar los componentes de Kaspersky Administration Kit.....	33
3.4. Actualizar la versión de la aplicación	34
CAPÍTULO 4. INSTALAR Y ELIMINAR EL SOFTWARE DE LOS EQUIPOS.....	35
4.1. Instalación remota de software	36
4.1.1. Crear un paquete de instalación.	37
4.1.2. Revisar y configurar los parámetros del paquete de instalación	40
4.1.3. Crear y configurar el paquete de instalación del Agente de Red	44
4.1.4. Crear una tarea para la distribución del paquete de instalación en los Servidores de Administración esclavo	47
4.1.5. Distribuir de los paquetes de instalación en un grupo mediante los agentes de red	49
4.1.6. Crear una tarea de instalación remota.....	53
4.1.7. Configurar la tarea de distribución	65

4.1.8. Eliminación remota de software	67
4.2. Asistente de distribución	68
4.3. Instalación local de software	73
4.3.1. Instalación de la ubicación del Agente de Red.....	74
4.3.2. Instalación local del complemento de administración de la aplicación.....	79
4.3.3. Instalar aplicaciones en modo no interactivo.....	80
APÉNDICE A. GLOSARIO	81
APÉNDICE B. KASPERSKY LAB LTD	89
A.1. Otros productos Kaspersky Lab	90
A.2. Cómo contactar con nosotros	96

CAPÍTULO 1. KASPERSKY® ADMINISTRATION KIT

1.1. Objetivo, estructura y funciones principales.

Kaspersky® Administration Kit ha sido diseñado para proporcionar una solución centralizada para las principales tareas administrativas asociadas con el sistema de seguridad antivirus de la red corporativa basándose en las aplicaciones Anti-Virus Business Optimal y Kaspersky Anti-Virus Corporate Suite. Kaspersky Administration Kit es compatible con todas las configuraciones de red que utilicen el protocolo TCP/IP.

Kaspersky Administration Kit es una herramienta dirigida a los administradores de redes corporativas y operadores de seguridad antivirus.

La aplicación permite al administrador:

- Distribuir o eliminar las aplicaciones Kaspersky Lab a través de una conexión de red a equipos de la red. Esta característica permite al administrador copiar el conjunto necesario de aplicaciones Kaspersky Lab a un equipo seleccionado e instalar estas aplicaciones en los de equipos de la red.
- Administrar licencias. Esta característica le permite instalar, de forma centralizada, claves de licencia para todas las aplicaciones Kaspersky Lab, supervisar la correspondencia entre el número de usuarios con licencia y las aplicaciones Kaspersky Lab instaladas en su red, así como controlar las fechas de caducidad de las licencias.
- Asegurar la administración centralizada remota de las aplicaciones Kaspersky Lab. Esta característica permite al administrador crear un sistema de protección antivirus multinivel y administrar su funcionamiento desde un único puesto de administrador. Esto es especialmente importante en grandes organizaciones que tienen una red local con un gran número de equipos distribuidos en varios edificios u oficinas separadas. Esta característica permite al administrador:
 - Agrupar equipos en *grupos de administración* según las funciones que realicen y las aplicaciones instaladas en estos.
 - Configurar las propiedades de la aplicación de forma centralizada mediante la creación y aplicación de *directivas de grupo*;

- Configurar parámetros individuales de aplicación para necesidades de equipos individuales, mediante los *parámetros de aplicación*;
- Administrar el funcionamiento de las aplicaciones de forma centralizada mediante la creación y ejecución de *tareas de grupo y globales*;
- Crear patrones individuales de funcionamiento de la aplicación mediante la creación y ejecución de un conjunto de equipos de diferentes grupos de administración.
- Actualizar automáticamente la base antivirus y los módulos de aplicación en los equipos. Estas funcionalidades permiten actualizar la base antivirus de forma centralizada para todas las aplicaciones, sin tener que conectar directamente cada equipo a los servidores de Kaspersky Lab. La actualización puede ser realizada, de forma automática, de acuerdo con la planificación establecida por el administrador. El administrador puede supervisar la instalación de actualizaciones en los equipos cliente.
- Recibir informes mediante un sistema dedicado. Esta funcionalidad permite un grupo centralizado de información estadística sobre el funcionamiento de todas las aplicaciones Kaspersky Lab instaladas, la supervisión de la corrección del funcionamiento de estas aplicaciones y la creación de informes en base a la información obtenida. El administrador puede crear un informe de red agrupado sobre el funcionamiento de una aplicación o informes sobre el funcionamiento de aplicaciones instaladas en cada equipo.
- Usar un sistema de notificación de eventos Sistema de envío de notificaciones por Correo. Esta característica permite al administrador crear una lista de eventos sobre las aplicaciones sobre las que recibirá notificaciones. Estos eventos producidos durante el funcionamiento de la aplicación pueden corresponder, por ejemplo, a la detección de un virus, a un fallo en la actualización o a la detección de un nuevo equipo en la red.

Kaspersky Administration Kit utiliza tres componentes principales:

- **El Servidor de Administración** es un almacén centralizado de información sobre las aplicaciones Kaspersky Lab instaladas en la red local de la organización y sobre la administración de dichas aplicaciones.
- **El Agente de Red** coordina la interacción entre el Servidor de Administración y las aplicaciones Kaspersky Lab instaladas en un puesto de red determinado (una estación de trabajo o servidor). Este componente soporta todas las aplicaciones incluidas en Kaspersky Anti-Virus Business Optimal y en Kaspersky Corporate Suites.

- **La Consola de Administración** proporciona una interfaz de usuario a los servicios de administración del Servidor de Administración y del Agente de Red. El módulo de administración está implementado como una extensión de Microsoft Management Console (MMC).

1.2. Requisitos software y hardware

Servidor de administración

- Requisitos software
 - Microsoft Data Access Components (MDAC) versión 2.8 o superior.
 - MSDE 2000 SP 3 o MS SQL Server 2000 SP 3 o superior o MySQL versión 5.0.22 (página de códigos predeterminada UTF-8) o MS SQL 2--5 o superior o MS SQL 2005 Express o superior;
 - Microsoft Windows 2000 SP 1 o superior; Microsoft Windows XP Professional SP 1 o superior; Microsoft Windows XP Professional x64 y superior, Microsoft Windows Server 2003 o superior; Microsoft Windows Server 2003 x64 o superior Microsoft Windows NT4 SP 6a o superior.
- Requisitos hardware:
 - Procesador Intel Pentium III, 800 MHz o superior
 - 128 Mb RAM
 - 400 Mb disponibles en el disco duro

Consola de Administración

- Requisitos software:
 - Microsoft Windows 2000 SP 1 o superior; Microsoft Windows XP Professional SP 1 o superior; Microsoft Windows XP Home Edition SP1 o superior; Microsoft Windows XP Professional x64 o superior. Microsoft Windows Server 2003 o superior; Microsoft Windows Server 2003 x64 o superior, Microsoft Windows NT 4 SP 6a o superior;
 - Microsoft Management Console versión 1.2 o superior
- Requisitos hardware:
 - Procesador Intel Pentium II, 400 MHz o superior
 - Al menos 64 Mb de RAM
 - 10 Mb disponibles en el disco duro

Agente de Red

- Requisitos software:
 - Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 SP 1 o superior; Microsoft Windows NT4 SP 6a o superior; Microsoft Windows XP Professional SP 1 o superior, Microsoft Windows XP Professional x64 o superior, Windows Server 2003 o superior; Microsoft Windows Server 2003 x64 o superior
- Requisitos hardware:
 - Procesador Intel Pentium, 233 MHz o superior
 - 32 Mb RAM
 - 10 Mb disponibles en el disco duro

1.3. Kit de Distribución

Este producto de software se proporciona, de forma gratuita, con una aplicación Kaspersky Lab incluida en el paquete de Kaspersky Anti-Virus Business Optimal y Kaspersky Corporate Suite (versión comercial) y también se encuentra disponible para su descarga del sitio Web Kaspersky Lab en www.kaspersky.com.

1.4. Servicio de soporte para usuarios registrados

Kaspersky Lab ofrece a sus usuarios registrados un amplio conjunto de servicios, que les permite disfrutar de todas las características disponibles de los productos Kaspersky Lab.

Cuando adquiera una licencia para cualquier producto Kaspersky Lab, incluido en Kaspersky Anti-Virus Business Optimal o Kaspersky Corporate Suite, se convertirá en un usuario registrado de Kaspersky Administration Kit. A continuación, recibirá los siguientes servicios durante el periodo de su licencia:

- Nuevas versiones de la aplicación de software antivirus;
- Consultas sobre problemas relativos a la instalación, configuración o funcionamiento de la aplicación antivirus por teléfono o a partir de solicitudes enviadas mediante un formulario Web;

Al enviar una solicitud al Servicio de Soporte Técnico, asegúrese de especificar la información sobre la licencia de la aplicación Kaspersky Lab utilizada con Kaspersky Administration Kit.

- Información sobre nuevas aplicaciones Kaspersky Lab y nuevos virus (para suscriptores del boletín de noticias de Kaspersky Lab).

Kaspersky Lab no proporciona información relativa al funcionamiento y el uso de sistemas operativos, u otras tecnologías.

1.5. Objetivo de este documento

Esta Guía contiene una descripción de la instalación de Kaspersky Administration Kit y de la instalación remota de aplicaciones en una red de configuración elemental.

Los conceptos generales y el esquema de funcionamiento de la aplicación se proporcionan en la Guía del Administrador de Kaspersky Administration Kit; en el Libro de Referencia de Kaspersky Administration Kit, se proporciona una descripción, paso a paso, de las acciones a realizar para la utilización de la aplicación.

Para examinar las cuestiones que nuestros usuarios preguntan más a menudo, a los especialistas de soporte de Kaspersky Lab, visite nuestra Web y siga el enlace **Services → Knowledge base**. Esta sección contiene información sobre la instalación, configuración y funcionamiento de las aplicaciones Kaspersky Lab así como sobre la eliminación de los virus más comúnmente propagados y la desinfección de archivos infectados.

1.6. Convenciones

Este documento utiliza diferentes iconos y tipos de formato en función del propósito y del significado del texto. La siguiente tabla enumera las convenciones usadas en el texto.

Convención	Significado
Texto en negrita	Títulos de menús, comandos, nombres de ventanas, elementos de diálogo, etc.
Nota	Información adicional, notas.
Alerta	Información a la que debe prestar especial atención.

Convención	Significado
<i>Para realizar una acción::</i> 1. Paso 1. 2. ...	Descripción de los pasos sucesivos del usuario y de las posibles acciones
[modificador] – nombre del modificador.	Modificador de línea de comandos
Mensajes de información y texto de la línea de comandos	Texto de archivos de configuración, mensajes de información y línea de comandos

CAPÍTULO 2. ESQUEMAS CONVENCIONALES DE DISTRIBUCIÓN DE LA PROTECCIÓN ANTIVIRUS

2.1. Esquemas de distribución de la protección antivirus en los equipos de la red lógica

Hay dos escenarios típicos que muestran cómo se puede distribuir la protección antivirus con Kaspersky Administration Kit:

- Puede instalar, de forma remota, las aplicaciones en los equipos cliente de la red lógica, desde un único equipo. La instalación y conexión al sistema de administración remota se realiza automáticamente, sin intervención del administrador y permite instalar el software antivirus en cualquier número de equipos cliente.
- Puede instalar localmente las aplicaciones en cada equipo de la red. En este caso, todos los componentes necesarios y el equipo administrador son instalados de forma manual. Los parámetros de conexión se establecen durante la instalación del Agente de Red. Este escenario de puesta en funcionamiento se utiliza sólo si la distribución centralizada no es posible.

La instalación remota puede ser usada para la instalación de cualquier aplicación seleccionada por el usuario.

Sin embargo, tenga en cuenta que Kaspersky Administration Kit soporta únicamente la administración de aplicaciones Kaspersky Lab cuyo paquete de distribución incluya un componente especializado - el complemento de administración de la aplicación.

2.2. Construir un sistema centralizado de administración de protección antivirus.

El primer paso para crear un sistema de administración centralizado en una red corporativa con Kaspersky Administration Kit es el diseño de una red lógica. En este punto, es necesario que tome las decisiones siguientes:

1. Seleccionar las secciones aisladas de la red y determinar el número de Servidores de Administración que deben ser instalados. El uso de una jerarquía de Servidores de Administración permitirá disminuir considerablemente la carga en los canales de comunicación y aumentar la fiabilidad del sistema.
2. Establecer qué equipos de la estructura de red corporativa van a funcionar como Servidor de Administración principal, Servidores administrador de los Servidores esclavo y equipos cliente. Obsérvese que todos los equipos en los que se encuentren instaladas aplicaciones Kaspersky Lab se comportarán como equipos cliente.
3. Establecer qué criterios se usarán para organizar los equipos cliente en grupos Decidir cómo va a ser la jerarquía de grupos.
4. Qué escenario de distribución va a utilizar: ¿instalación remota o local?

En la siguiente fase, el administrador debe construir una red lógica, es decir, instalar los componentes Kaspersky Administration Kit en los equipos de la red, es decir:

1. Instalar Servidores de Administración en equipos incluidos en la red corporativa.
2. Instalar la Consola de Administración en equipos desde los que se proporcionará la administración.
3. Tomar decisiones respecto a la asignación de los administradores de la red lógica, determinar qué otras categorías de usuario interactúan con el sistema y asignar una lista de funciones que podrá realizar cada categoría.
4. Crear listas de usuarios y conceder a cada grupo los permisos de acceso necesarios para realizar las funciones asignadas a ese grupo.

A continuación, es necesario crear una jerarquía de Servidores de Administración y, para cada Servidor, crear una estructura de red lógica de la

siguiente manera: crear una jerarquía de grupos de administración y distribuir los equipos entre los correspondientes grupos.

En la siguiente fase, instale el Agente de Red y las aplicaciones Kaspersky Lab seleccionadas en los equipos cliente, e instale los módulos de administración correspondientes en el equipo administrador.

Si va a utilizar la opción de instalación remota, el Agente de red debe ser instalado junto con cualquier aplicación, en este caso, se requiere no separar la instalación del Agente de Red.

Durante la etapa final, debe configurar las aplicaciones instaladas asignando y aplicando directivas de grupo y creando tareas.

Mediante el Asistente de Inicio Rápido, el administrador puede construir fácilmente un sistema de protección antivirus para su red y llevar a cabo la configuración mínima. El hecho de configurar brevemente el sistema de protección antivirus supone crear una red lógica idéntica a la estructura del dominio de la red Windows, y distribuir el sistema de protección a partir de las versiones 5.0 y 6.0 de Kaspersky Anti-Virus 5.0 for Windows Workstations.

CAPÍTULO 3. INSTALACIÓN DE KASPERSKY ADMINISTRATION KIT

Antes de iniciar la instalación, asegúrese de que su equipo cumpla con los requisitos hardware y software del Servidor de Administración y del equipo administrador (ver sección 1.3, página 8).

MSDE (Microsoft Data Engine), MySQL server o Microsoft SQL server son utilizados para almacenar información del Servidor de Administración. Si no se encuentra instalado MSDE o SQL Server, debe instalar uno de ellos antes de instalar el Servidor de Administración. Con este fin, puede usar los paquetes de distribución que tiene. Para instalar MSDE, puede también usar el paquete de distribución de Kaspersky Administration Kit. El procedimiento de instalación de MSDE a partir de Kaspersky Administration Kit se describe a continuación (ver sección 3.1, página 14).

Para la instalación de Kaspersky Administration Kit, son necesarios los permisos del administrador local en el equipo en el que se realiza la instalación.

El asistente de instalación le pedirá que instale los componentes de la aplicación de Kaspersky Administration Kit (el Servidor de Administración y la Consola de Administración) en el equipo en el que se ejecuta el asistente de instalación. Se recomienda esta configuración en la etapa inicial de creación del sistema de administración centralizado.

3.1. Instalar MSDE desde el paquete de distribución de Kaspersky Administration Kit

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).

La instalación de MSDE en un equipo desde el paquete de distribución de Kaspersky Administration Kit se realiza de forma local.

Para instalar MSDE:

1. Ejecute el archivo ejecutable que se encuentra en la carpeta **MSDE2KSP3**, del CD de instalación de Kaspersky Administration Kit 5.0. El Asistente de instalación le propondrá que configure los parámetros y ejecute la aplicación. Siga las instrucciones de instalación del asistente.
2. Los primeros pasos son los habituales e incluyen la extracción y la copia, al disco duro de su equipo, de los archivos requeridos del paquete de distribución, la verificación del software, la aceptación del contrato de licencia y la recogida de información sobre el usuario y la compañía.
3. A continuación, en el cuadro de diálogo **Carpeta de Instalación**, defina lo siguiente:
 - En el campo **Módulos de aplicación** – la carpeta para la instalación de los archivos de la aplicación MSDE. La carpeta predeterminada es: **<Disco:\Archivos de Programa\Microsoft SQL Server**. Si la carpeta no existe, el programa la creará automáticamente.
 - En el campo **Base de datos** – una carpeta se usará para almacenar la base de datos del servidor MSDE. La carpeta predeterminada es también **<Disco:\Archivos de Programa\Microsoft SQL Server**.

Para seleccionar las carpetas utilice el botón **Examinar**.

4. A continuación, en el cuadro de diálogo del **nombre del servidor SQL** (ver Figura 1. Seleccionar el nombre del servidor) especifique el nombre que se asignará al servidor.

De forma predeterminada, no se crea el nombre, y para direccionar el servidor se utiliza el nombre del equipo en el que está instalado el servidor.

Si desea asignar un nombre distinto, desmarque la casilla **Predeterminado** e introduzca un nuevo nombre en el **Nombre del servidor SQL**.

Después de que haya configurado los parámetros, puede revisarlos e iniciar la instalación. Una vez que la instalación haya concluido con éxito, se instalará MSDE en su equipo.

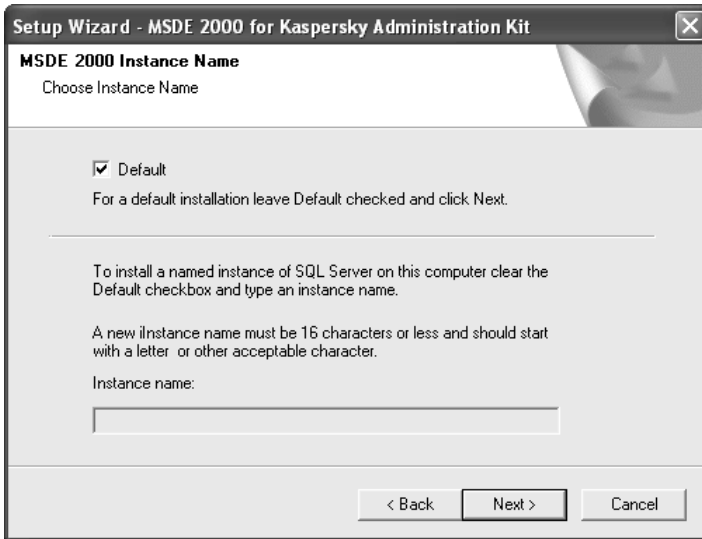


Figura 1. Seleccionar el nombre del servidor

3.2. Instalar el Servidor de Administración y la Consola de Administración

Para instalar el Servidor de Administración y/ o la Consola de Administración:

1. Ejecute el archivo **setup.exe** del CD de instalación. El asistente de instalación le indicará que configure los parámetros siguiendo las instrucciones del asistente de instalación.
2. En primer lugar el asistente extraerá y copiará, al disco duro de su equipo, los archivos requeridos del paquete de distribución, le ofrecerá que acepte la aceptación del contrato de licencia y la recogida de información sobre el usuario y la compañía.
3. A continuación defina la carpeta que se utilizará para instalar los componentes. La carpeta predeterminada es: **<Disco:\Archivos de Programa\Kaspersky Lab\Kaspersky Administration Kit**. Si la carpeta no existe, el programa la creará automáticamente. Para cambiar la carpeta, utilice el botón **Examinar**.

4. A continuación seleccione los componentes de Kaspersky Administration Kit que desea instalar (ver Figura 2. Seleccionar los componentes a instalar): **Consola de Administración** y/ o **Servidor de Administración**.

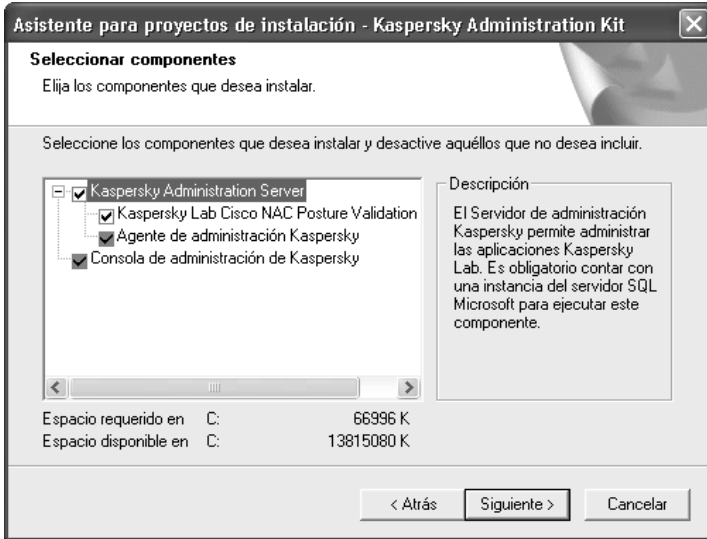


Figura 2. Seleccionar los componentes a instalar

Puede seleccionar ambos componentes o solamente la Consola de Administración. No se puede seleccionar la instalación del Servidor de Administración sin la instalación de la Consola de Administración. La opción por defecto es la instalación de ambos componentes.

Se instalará una versión servidor del Agente de Red con el Servidor de Administración. No es posible su instalación separada utilizando una versión normal del Agente de Red. Si este componente ya está instalado en su equipo, elimínelo y reinstale el Servidor de Administración.

Preste atención a la información mostrada en la ventana del asistente:

- En el campo **Descripción** en la sección de la derecha – información del componente seleccionado.
- En la sección inferior - información sobre el espacio de disco necesario para instalar los componentes seleccionados y el espacio de disco disponible en la unidad seleccionada para la instalación.

Si sólo selecciona la Consola de Administración, no necesitará realizar más pasos posteriores para configurar los parámetros de instalación y se le pedirá que pase directamente a la etapa de revisión de estos parámetros y que inicie la instalación.

5. si selecciona la instalación del Servidor de Administración, tiene que definir en el siguiente paso la cuenta bajo la que se iniciará el Servidor de Administración como un servicio en este equipo (ver Figura 3. Seleccionar la cuenta).

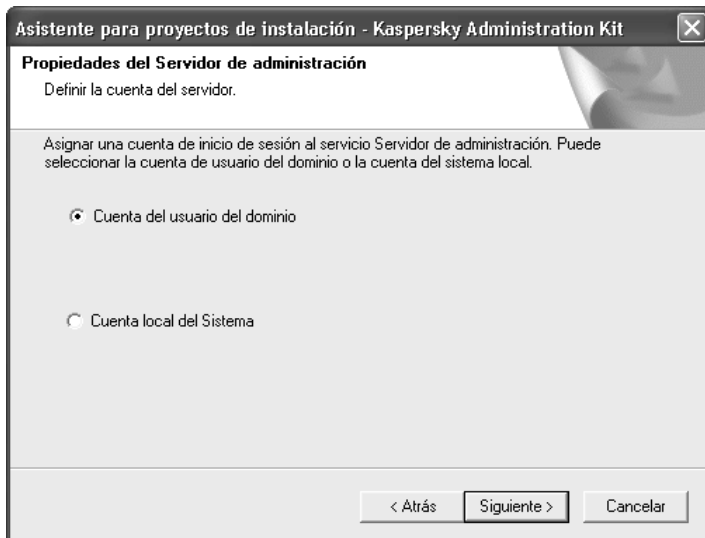


Figura 3. Seleccionar la cuenta

Puede seleccionar una de estas dos opciones:

- **Cuenta de usuario del Dominio** – El Servidor de Administración se iniciará bajo la cuenta de usuario incluida en el dominio. En este caso el Servidor de Administración iniciará todas las operaciones utilizando los permisos de esta cuenta y en el próximo paso se le pedirá que especifique el usuario cuya cuenta se utilizará.

Si se ha creado una estructura de dominios de Windows dentro de la red corporativa, le recomendamos que seleccione la cuenta del administrador del dominio para iniciar el Servidor de Administración. En el futuro, esto le permitirá evitar parámetros adicionales de configuración, por ejemplo, especificar una cuenta de un usuario con permisos de administrador del dominio cuando cree una tarea de distribución (instalación remota) (ver sección 4.1.6, página 53).

- **Cuenta Local del Sistema** - El Servidor de Administración se iniciará bajo la **Cuenta del sistema** con todos los permisos concedidos a esta cuenta. En este caso no necesita seleccionar una cuenta de usuario e irá directamente a la fase donde tiene que especificar el recurso que almacenará la base de datos de información del Servidor de Administración.

Para el correcto funcionamiento de Kaspersky Administration Kit es obligatorio que la cuenta utilizada para iniciar el Servidor de Administración tenga permisos de administrador en el medio utilizado para almacenar la base de datos de información del Servidor de Administración.

6. Si ha seleccionado una cuenta de usuario del dominio para iniciar el Servidor de administración, se le pedirá que especifique dicho usuario.

Con este fin, en el campo **Nombre de usuario** de la ventana del asistente (ver Figura 4. Seleccionar usuario:) seleccione el nombre de usuario mediante el botón **Examinar...** o introduzca este nombre de forma manual de los nombres registrados dentro del dominio actual. A continuación, introduzca la contraseña utilizada para registrar el usuario en el dominio.

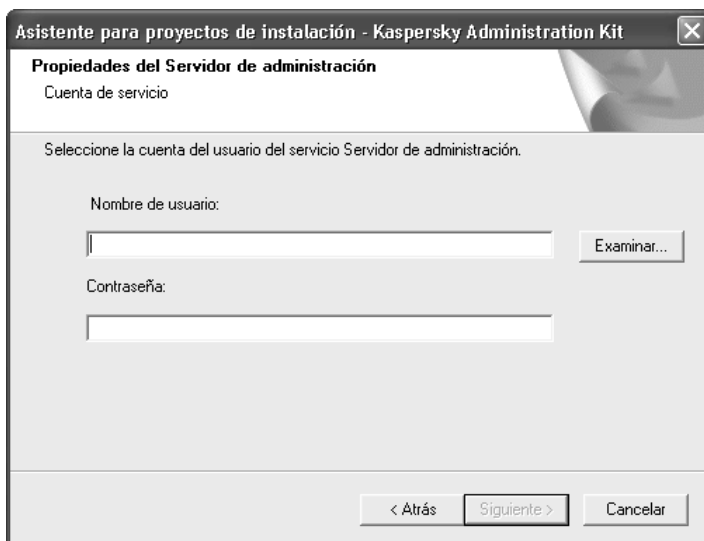


Figura 4. Seleccionar usuario:

Si ha seleccionado un usuario que no tiene permisos de administración, el Servidor de Administración se iniciará con esta cuenta, sin embargo la funcionalidad de Kaspersky Administración Kit tendrá algunas limitaciones. Por ejemplo, puede no tener los permisos necesarios para ejecutar una tarea de distribución usando un escenario de lanzamiento (ver sección 4.1.6, página 53) y para sondear algunos dominios de la red.

Para el correcto funcionamiento del Servidor de Administración, la cuenta utilizada para iniciarlo debe tener los siguientes permisos:

- Registrarse como un servicio;
- Actuar como parte del sistema operativo;
- Tener acceso a este equipo desde la red;
- Reemplazar un componente de nivel de proceso;
- Aumentar cuotas / Ajustar cuotas de memoria para un proceso.

Si el usuario que ha seleccionado es un administrador de dominio, pero no tiene los permisos enumerados arriba, estos permisos deben ser concedidos a este usuario (ver Figura 5. Mensaje sobre los permisos concedidos al usuario).

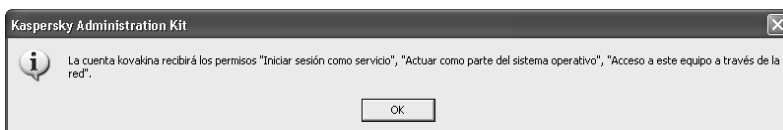
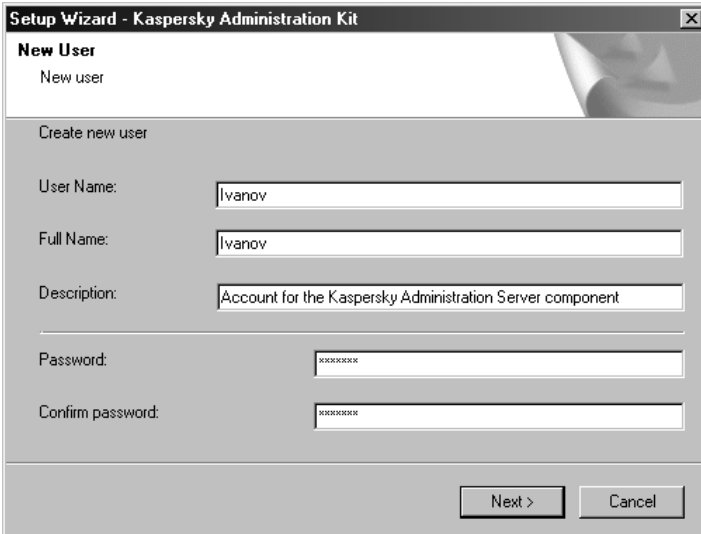


Figura 5. Mensaje sobre los permisos concedidos al usuario

Si tiene permisos de administrador del dominio, puede crear un usuario especial y usar su cuenta para iniciar el Servidor de Administración. A este usuario se le concederán permisos de administrador del dominio así como los permisos enumerados anteriormente.

Para crear un usuario especial, pulse el botón **Crear** e introduzca lo siguiente en la ventana de diálogo que se abre (ver Figura 6. Creación de un nuevo usuario):

- Nombre de usuario (obligatorio);
- Nombre de usuario completo (opcional);
- Detalles adicionales de usuario. De forma predeterminada, pondrá **Cuenta para iniciar el Servidor de Administración** (no requerido);
- Contraseña de la cuenta (obligatorio);
- Confirmación de la contraseña (obligatorio);



The screenshot shows a window titled "Setup Wizard - Kaspersky Administration Kit" with a close button in the top right corner. The window content is as follows:

- New User**
New user
- Create new user
- User Name:
- Full Name:
- Description:
- Separator line
- Password:
- Confirm password:
- Buttons: "Next >" and "Cancel"

Figura 6. Creación de un nuevo usuario

7. Durante el próximo paso tendrá que definir el recurso **Microsoft SQL server (MSDE)** o **MySQL** (ver Figura 7. Seleccionar la base de datos), que usará para almacenar la base de datos de información del Servidor de Administración.

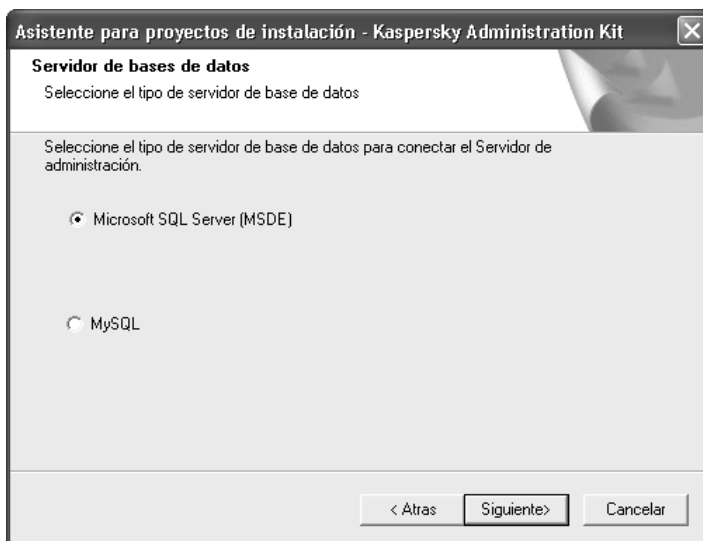


Figura 7. Seleccionar la base de datos

- Si durante el paso anterior seleccionó MSDE o Microsoft SQL server y tiene pensado utilizar un servidor instalado en la red corporativa para trabajar con Kaspersky Administration Kit, indique el nombre de ese servidor en el campo **Nombre del Servidor SQL** y especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de Administración en **Nombre del la base de datos del servidor SQL** (ver Figura 8. Seleccionar SQL server). El nombre predeterminado de la base de datos es **KAV**.

El valor **(local)** se asignará de forma automática al campo **Nombre del Servidor** si se detecta SQL Server en el equipo en el que se está instalando Kaspersky Administration Kit. Para mostrar la lista de todos los servidores Microsoft SQL Server instalados en la red, pulse el botón **Examinar...**

Si el Servidor de Administración se inicia con la cuenta del administrador local o con la cuenta del sistema, el botón **Examinar** no estará disponible.

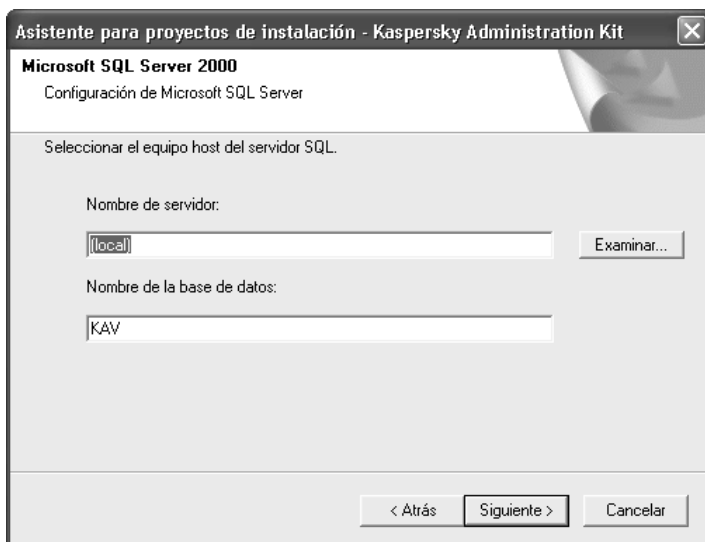


Figura 8. Seleccionar SQL server

Si durante el paso anterior seleccionó MySQL, especifique en esta ventana (ver Figura 9. Seleccionar un servidor MySQL) su nombre en el campo **nombre del servidor MySQL** (por defecto se usará la dirección IP del equipo en el que se está instalando Kaspersky Administration Kit) y especifique el puerto que se usará para la conexión en el campo **Puerto** (el puerto predeterminado es el 3306) En el campo **nombre de la base de datos del servidor MySQL** especifique el nombre de la base de datos que se creará para almacenar los datos de Servidor de Administración (de forma predeterminada la base de datos se llamará **KAV**).

Si durante la etapa anterior ha seleccionado MySQL, especifique en esta ventana

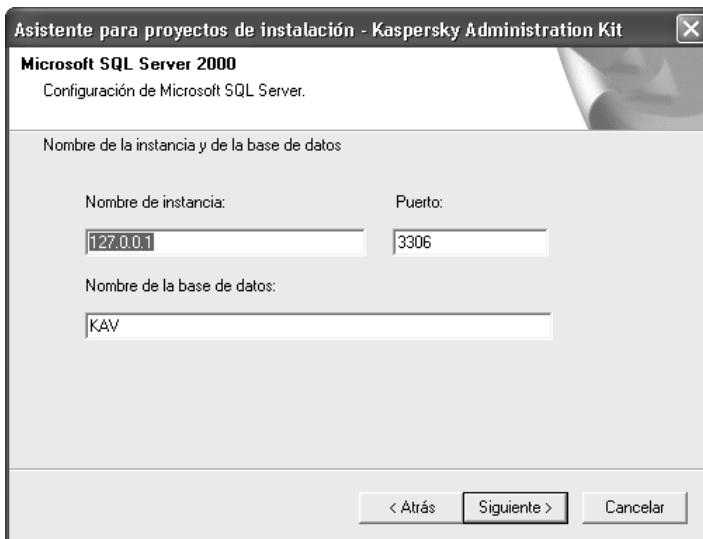


Figura 9. Seleccionar un servidor MySQL

Si no hay servidores SQL en la red y no puede utilizarlos, debe instalar uno (ver sección 3.1, página 14).

Si desea instalar un servidor SQL en el equipo desde el que está instalando Kaspersky Administration Kit, debe detener la instalación y reiniciarla después de que haya instalado el servidor SQL.

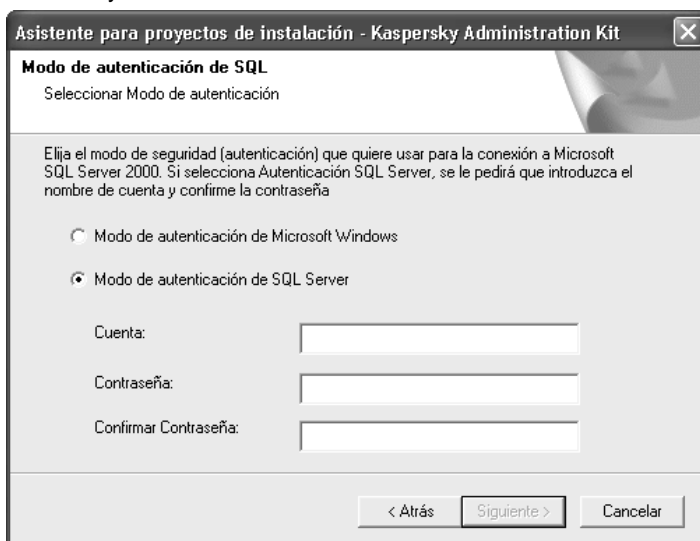
Si instala Kaspersky Administration Kit en un equipo remoto, no es necesario interrumpir el agente de instalación de Kaspersky Administration Kit. Instale el SQL Server y vuelva a la instalación de Kaspersky Administration Kit.

9. Durante esta etapa, debe definir el modo de autenticación a utilizar por el Servidor de Administración para conectar con el servidor SQL.

Para MSDE o Microsoft SQL Server puede seleccionar entre las siguientes dos opciones (ver Figura 10. Modo de autenticación de SQL Server).

- **Modo de Autenticación de Microsoft Windows** – en este caso, la cuenta utilizada para iniciar el Servidor de Administración se utilizará para verificar los permisos;
- **Modo de autenticación de SQL Server** – si selecciona esta opción, la cuenta especificada a continuación se usará para

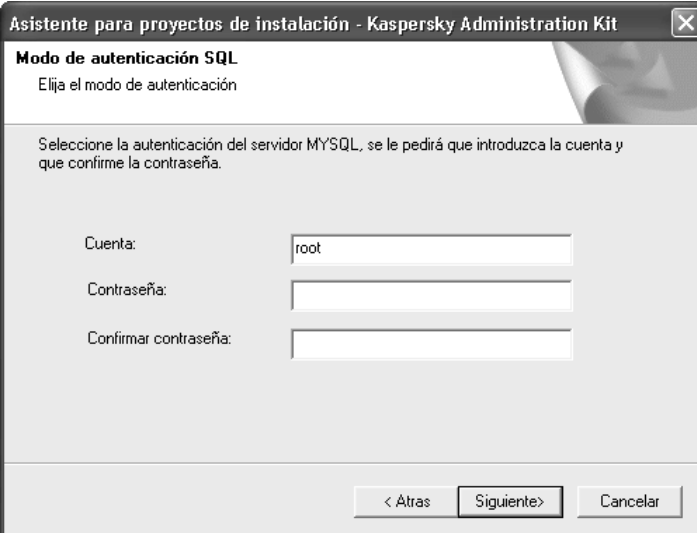
verificar los permisos. Rellene los campos **Cuenta**, **Contraseña** y **Confirmar Contraseña**.



The screenshot shows a window titled "Asistente para proyectos de instalación - Kaspersky Administration Kit" with a close button in the top right corner. The main heading is "Modo de autenticación de SQL" with the subtitle "Seleccionar Modo de autenticación". Below this, there is a paragraph of instructions: "Elija el modo de seguridad (autenticación) que quiere usar para la conexión a Microsoft SQL Server 2000. Si selecciona Autenticación SQL Server, se le pedirá que introduzca el nombre de cuenta y confirme la contraseña". There are two radio button options: "Modo de autenticación de Microsoft Windows" (unselected) and "Modo de autenticación de SQL Server" (selected). Below the options are three text input fields labeled "Cuenta:", "Contraseña:", and "Confirmar Contraseña:". At the bottom of the window are three buttons: "< Atrás", "Siguiente >" (highlighted), and "Cancelar".

Figura 10. Modo de autenticación de SQL Server

Para que MySQL Server indique la cuenta y la contraseña (ver Figura 11. Modo de autenticación del servidor MySQL).



The screenshot shows a window titled "Asistente para proyectos de instalación - Kaspersky Administration Kit". The main heading is "Modo de autenticación SQL" with the instruction "Elija el modo de autenticación". Below this, it says "Seleccione la autenticación del servidor MySQL, se le pedirá que introduzca la cuenta y que confirme la contraseña." There are three input fields: "Cuenta:" with the text "root", "Contraseña:", and "Confirmar contraseña:". At the bottom, there are three buttons: "< Atras", "Siguiete>", and "Cancelar".

Figura 11. Modo de autenticación del servidor MySQL

10. A continuación, (ver Figura 12. Crear una carpeta compartida), especifique la ubicación para almacenar la carpeta compartida que se va a utilizar:

- Para almacenar archivos requeridos para la instalación remota de aplicaciones (archivos que se copiarán a los Servidores de Administración cuando se creen los paquetes de instalación);
- Para almacenar las actualizaciones copiadas desde los orígenes de actualizaciones en el Servidor de Administración.

Este recurso será público para todos los usuarios en modo de lectura.

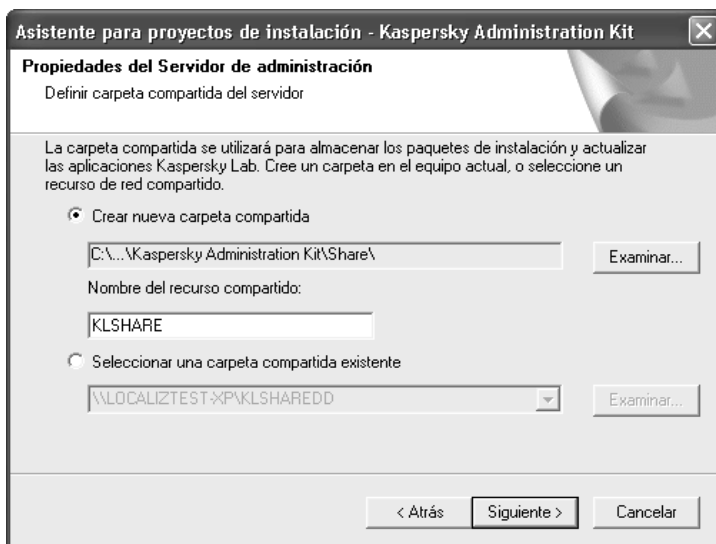


Figura 12. Crear una carpeta compartida

Puede seleccionar una de las siguientes dos opciones:

- **Crear una nueva carpeta compartida** – para crear una nueva carpeta, debe especificar la ruta a la carpeta en el siguiente campo.
- **Seleccionar una carpeta compartida existente** – con el fin de seleccionar una carpeta compartida de la lista de carpetas compartidas existentes.

Una carpeta compartida pública puede ser almacenada de forma local, en el equipo en el que se realiza la instalación o, de forma remota, en cualquiera de los equipos incluidos en la red corporativa.

Por defecto, una carpeta local **Share** se creará en la carpeta especificada para la instalación de los componentes de la aplicación Kaspersky Administration Kit.

11. A continuación, configure los parámetros a utilizar para la conexión del Servidor de Administración (ver Figura 13. Parámetros utilizados para conectar con el Servidor de Administración);
 - el número de puerto utilizado para conectar con el Servidor de Administración. De manera predeterminada, se utiliza el puerto **14000**. Si se ha asignado, puede cambiarlo.

- El número de puerto SSL que se utilizará para la conexión con el Servidor de Administración usando el protocolo SSL. De forma predeterminada, se utiliza el puerto **13000**.

Si el Servidor de Administración se ejecuta con Microsoft Windows XP SP 2, entonces, el cortafuegos interno bloqueará los puertos TCP 13000 y 14000. Por lo tanto, para asegurar el acceso del Servidor de Administración, estos puertos deben abrirse manualmente.

Asistente para proyectos de instalación - Kaspersky Administration Kit

Propiedades del Servidor de administración
Definir los puertos del servidor.

Defina el puerto del Servidor de administración. El valor debe estar entre 1-65535.

Puerto del servidor:

Defina el puerto SSL del Servidor de administración. El valor debe estar entre 1-65535.

Puerto SSL servidor:

< Atrás Siguiete > Cancelar

Figura 13. Parámetros utilizados para conectar con el Servidor de Administración

12. En esta ventana del asistente (ver Figura 14. Seleccionar el método a utilizar para recibir el certificado del Servidor de Administración), indique el método de creación del certificado a utilizar para la autenticación del Servidor de Administración que está siendo instalado.

Se proporcionan dos opciones:

- **Crear un nuevo certificado** – seleccione esta opción si está instalando un nuevo Servidor de Administración. Guarde una copia de seguridad del certificado de manera que, más tarde, si fuera necesario, sea más fácil para usted restaurar la fecha y la estructura de la red lógica de este Servidor. Con este fin, marque la casilla **Crear una copia de seguridad del certificado**.

- **Restaurar certificado** – seleccione esta opción si está restaurando el Servidor de Administración sin ninguna copia de seguridad disponible. En este caso, puede restaurar los datos y la estructura de la red lógica del Servidor de Administración anterior.

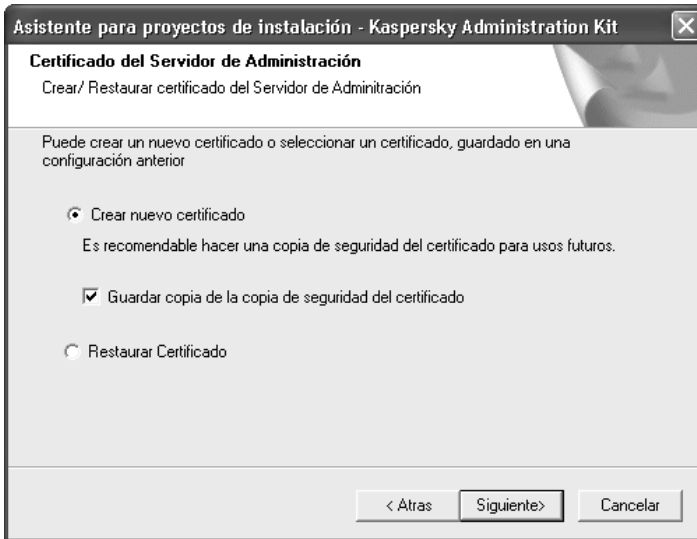
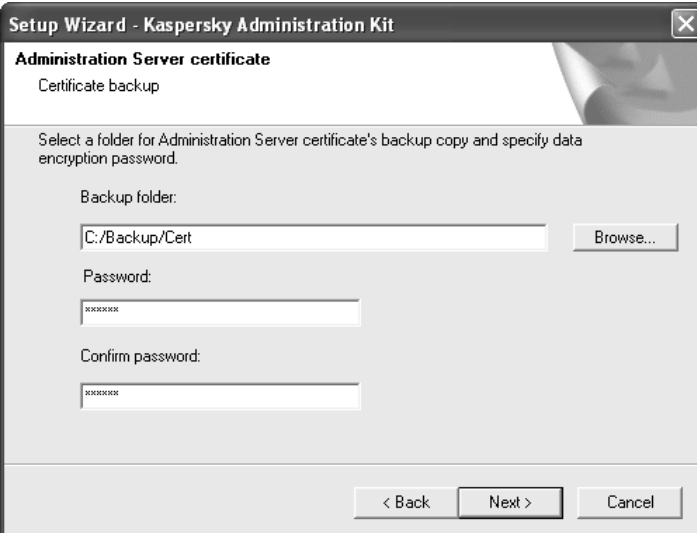


Figura 14. Seleccionar el método a utilizar para recibir el certificado del Servidor de Administración

13. Si durante la etapa anterior ha seleccionado la creación de un nuevo certificado y ha guardado su copia de seguridad, especifique lo siguiente en la ventana correspondiente (ver Figura 15. Seleccionar carpeta para guardar la copia de seguridad del certificado;):
 - Carpeta para guardar la copia de seguridad del archivo del certificado;
 - Contraseña a utilizar para el cifrado cuando se cree un nuevo certificado y para su descifrado durante su restauración desde una copia de seguridad;
 - Confirmación de contraseña.

Para restaurar los datos del Servidor de Administración más tarde, debe guardar el certificado del Servidor.

Al restaurar el certificado debe introducir la misma contraseña utilizada para la copia de seguridad. Si la contraseña es incorrecta, el certificado no se restaurará.



Setup Wizard - Kaspersky Administration Kit

Administration Server certificate

Certificate backup

Select a folder for Administration Server certificate's backup copy and specify data encryption password.

Backup folder:
C:/Backup/Cert

Password:
XXXXXXXX

Confirm password:
XXXXXXXX

< Back

Figura 15. Seleccionar carpeta para guardar la copia de seguridad del certificado;

Si durante la etapa anterior ha seleccionado la opción de restaurar el certificado de una copia de seguridad, especifique lo siguiente en la ventana correspondiente (ver Figura 16. Seleccionar carpeta para almacenar la copia de seguridad del certificado;):

- Carpeta en la que se ha guardado la copia de seguridad del archivo del certificado;
- Contraseña utilizada para el cifrado durante la creación de una copia de seguridad del certificado.

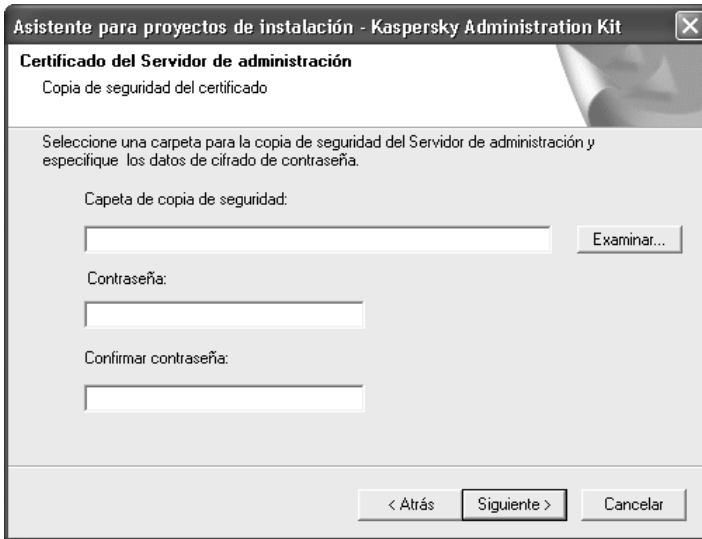


Figura 16. Seleccionar carpeta para almacenar la copia de seguridad del certificado;

Cuando haya terminado de configurar los parámetros de instalación de Kaspersky Administration Kit, puede revisarlos e iniciar la instalación.

Después de la instalación de la Consola de Administración, aparecerá un icono en el menú **Inicio**→ **Programas**→ **Kaspersky Administration Kit** de su equipo. Este icono puede utilizarse para iniciar la Consola.

El Servidor de Administración se instalará en el equipo como un servicio con el conjunto de características siguiente:

- Nombre de servicio (**CSAdminServer**);
- Con el nombre **Kaspersky Administration Server**;
- Inicio automático en la carga del sistema operativo
- **Sistema Local** de cuenta o una cuenta de usuario en función de la elección realizada

Se instalará una versión servidor del Agente de Red en el equipo con el Servidor de Administración. Está incluido en la estructura del componente del Servidor de Administración y se instala o se elimina, de forma conjunta a éste, y sólo puede interactuar con el Servidor de Administración local instalado. No necesita configurar los parámetros utilizados por el Agente para conectar con el Servidor de Administración, puesto que, mediante programación, esta conexión se ejecuta en el supuesto de que estos componentes estén instalados en el mismo

equipo. Este tipo de configuración permite evitar una configuración adicional y los posibles conflictos en el funcionamiento de los componentes, si están instalados de forma separada.

Una versión servidor del Agente de Red se instala con las mismas características y realiza las mismas funciones de administración de aplicaciones que el Agente de Red estándar. Funcionará a partir de la directiva de grupo en la que se incluye el servidor de Administración como equipo cliente, todas las tareas proporcionadas por el Agente de Red se crearán, con la excepción de la tarea de cambio del Servidor.

No se requiere una instalación separada del Agente de Red en el Servidor de Administración. Sus funciones serán realizadas por la versión del servidor.

Puede revisar las propiedades del servicio **Servidor de Administración Kaspersky** y controlar su funcionamiento mediante las herramientas de administración de Windows estándar **Administración de equipo** → **Servicios**. Se registra y se guarda información sobre el funcionamiento del servicio **Kaspersky Administration Server** en el registro del sistema de Windows del equipo en el que se ha instalado el Servidor de Administración, en una rama separada denominada **Kaspersky Event Log**.

Asimismo, los grupos de usuarios locales **KLAdmins** y **KLOperators** se crearán en el equipo en el que se ha instalado el Servidor de Administración. Si el Servidor de Administración se ejecuta bajo una cuenta de usuario asignada al dominio, entonces, los grupos **KLAdmins** y **KLOperators** se agregarán a la lista de grupos de usuarios del dominio. El cambio de la lista de los grupos se realiza usando herramientas de administración estándar de Windows.

3.3. Eliminar los componentes de Kaspersky Administration Kit

Puede eliminar Kaspersky Administration Kit mediante la aplicación de Windows estándar **Agregar/ Eliminar Programas**. Esto desinstalará la Consola de Administración, el Servidor de Administración y la versión servidor del Agente de Red de su equipo.

Cuando desinstale los programas, se le ofrecerá que guarde una copia de seguridad en el Servidor de Administración.

3.4. Actualizar la versión de la aplicación

Para actualizar la versión 4.x de Kaspersky Administration Kit a la versión 6.0, deberá desinstalar la versión anterior e instalar una nueva, tal y como se describe en esta Guía.

Cuando actualiza la versión 6.0 a una versión más reciente, por ejemplo, SP 1 a SP 2, le recomendamos que siga el procedimiento descrito a continuación:

La restauración de datos durante la actualización a una versión posterior de la aplicación está permitida si ésta se inicia con Kaspersky Administration Kit, versión 5.0 Maintenance Pack 3

1. Haga una copia de seguridad de los datos del Servidor de Administración mediante la utilidad **klbackup.exe**. Esta utilidad está incluida en el paquete de distribución de Kaspersky Administration Kit y después de la instalación del Servidor de Administración, ésta puede ser localizada en el directorio raíz de la instalación. Obsérvese que para poder restaurar completamente los datos del Servidor de Administración debe guardar el certificado del Servidor. Este es un parámetro obligatorio para la utilidad **klbackup.exe**.
2. Ejecute la instalación de la nueva versión de Kaspersky Administration Kit 6,0 en el equipo en el que está instalada la versión anterior. Actualice el componente. En el transcurso de la actualización, toda la información de la versión anterior del Servidor de Administración se guardará y se pondrá a disposición de la nueva versión. El programa soporta la compatibilidad hacia atrás entre las versiones nueva y anterior del Servidor de Administración.
3. Para actualizar a la nueva versión del Agente de Red instalado en la Red, cree un grupo o una tarea de instalación global de la nueva versión del componente. Ejecute la tarea manualmente o de acuerdo a la planificación. Una vez que la tarea se complete con éxito, la nueva versión del Agente de red estará instalada.

Si encuentra cualquier problema durante la instalación, puede restaurar la versión anterior de Kaspersky Administration Kit usando la copia de seguridad de los datos del Servidor de Administración creados antes de la actualización.

CAPÍTULO 4. INSTALAR Y ELIMINAR EL SOFTWARE DE LOS EQUIPOS

Antes de iniciar la instalación, debe asegurarse de que el software y el hardware de los equipos cumplen los requisitos necesarios (ver sección 1.3, página 8)

Kaspersky Administration Kit permite la instalación y la eliminación de aplicaciones Kaspersky Lab usando los métodos siguientes:

- De forma remota, de una forma centralizada, a través de la Consola de Administración;
- De forma local, individualmente en cada equipo.

La conexión del Servidor de Administración con los equipos cliente se asegura por el componente Agente de Red. Por consiguiente, este componente debe estar instalado en cada equipo que será conectado al sistema de administración centralizada antes de la instalación de las aplicaciones antivirus. Si utiliza el método centralizado para instalar las aplicaciones mediante la Consola de Administración, el Agente de Red podrá instalarse junto con una de las aplicaciones.

En el equipo en el que está instalado el Servidor de Administración, sólo se puede utilizar la versión servidor del Agente de Red. Está incluida en la estructura del Servidor de Administración y es instalado y eliminado, de forma conjunta, con el Servidor de Administración (ver sección 3.2, página 16). No necesita instalar el Agente de Red en este equipo.

El Agente de Red se instala de la misma forma que las aplicaciones – de forma remota o local.

Los Agentes de Red pueden variar en función de las aplicaciones Kaspersky Lab para las que fueron instalados. En algunos casos, sólo es posible la instalación local del Agente de Red (para más detalles, ver las Guías de las aplicaciones correspondientes). El Agente de Red se instala en el equipo cliente sólo una vez.

La interfaz de administración de la aplicación de Kaspersky Administration Kit se implementa por los correspondientes complementos de administración. Por lo tanto, para de acceder a la interfaz de administración de la aplicación, el complemento correspondiente debe ser instalado en el equipo administrador. En caso del método de instalación remota, se instala automáticamente cuando se crea el primer paquete de instalación para la aplicación correspondiente. En

caso de instalación local en el equipo cliente, el complemento de administración debe ser instalado, de forma manual, por el administrador.

4.1. Instalación remota de software

La instalación remota de software puede realizarse desde el equipo administrador en la ventana principal de la aplicación Kaspersky Administration Kit.

Algunas aplicaciones de Kaspersky Lab pueden instalarse sólo en equipos cliente de forma local (para más detalles, ver las Guías de las aplicaciones correspondientes). Sin embargo, la administración remota de estas aplicaciones está disponible usando Kaspersky Administration Kit.

Con el fin de realizar la instalación remota del software:

1. Cree un paquete de instalación (ver sección 4.1.6, página 53). La estructura de este paquete incluirá los archivos requeridos para instalar la aplicación y los archivos que contienen la configuración del paquete de instalación.

El paquete de instalación contiene el archivo setup.exe con el que se realiza la instalación local de la aplicación en modo no interactivo.

2. Cree una tarea de instalación remota (ver sección 4.1.6, página 53).

Para instalar la aplicación en todos los equipos de la red lógica, en varios grupos de administración o en equipos específicos desde varios grupos, debe crear una tarea de distribución global (instalación remota).

Para instalar la aplicación en todos los equipos de un grupo de administración (incluidos todos los grupos anidados y servidores esclavo), debe crear una tarea de distribución de grupo (instalación remota).

Puede utilizar el asistente de distribución (ver sección 4.2, página 68) para crear un grupo o una tarea global.

La tarea que ha creado se ejecutará de acuerdo a la programación. Los parámetros de funcionamiento de la aplicación en cada equipo cliente se configurarán en función de la directiva de grupo y de los parámetros predeterminados de la aplicación.

Puede detener el proceso de instalación mediante la interrupción manual de la ejecución de la tarea.

Todos los paquetes de instalación creados para el Servidor de Administración se ubicarán en el árbol de consola en un contenedor especial **Instalación remota**.

En el Servidor de Administración, estos paquetes de instalación se almacenarán en la carpeta compartida especificada en la carpeta de servicio **Paquetes**.

Puede revisar las propiedades del paquete de instalación, cambiar su nombre y parámetros usando la ventana **Propiedades: <Nombre del paquete>** (ver Figura 20. Ventana de revisión de propiedades del paquete de instalación La ficha **General**). Esta ventana se abre mediante el comando del menú contextual **Propiedades** o el elemento análogo del menú **Acción**.

Los paquetes de instalación creados pueden ser distribuidos en los Servidores de Administración esclavo (ver sección 4.1.4, página 47) y en los equipos de un grupo mediante los agentes de actualización (ver sección 4.1.5, página 49).

Un paquete de instalación puede ser reutilizado varias veces para crear tareas de distribución.

4.1.1. Crear un paquete de instalación.

Para crear un paquete de instalación:

1. Conecte al Servidor de administración que necesita.
2. Seleccione el nodo **Instalación remota** en el árbol de consola, abra el menú contextual y seleccione el comando **Crear** → **Paquete de Instalación** o utilice el elemento análogo desde el menú **Acción**. Se iniciará el asistente. Siga sus instrucciones.
3. Especifique el nombre del paquete de instalación y especifique la aplicación a instalar durante la siguiente etapa (ver Figura 17. Crear un paquete de instalación. Seleccionar la aplicación a instalar).

Si está instalando una aplicación que soporta la administración remota a través de Kaspersky Administration Kit, debe seleccionar la opción **Crear el paquete de instalación para la aplicación Kaspersky Lab** desde la lista desplegable. Mediante el botón **Examinar...**, seleccione el archivo que contenga la descripción de la aplicación (archivo con la extensión **.kdp** y que está incluido en el paquete de distribución de todas las aplicaciones Kaspersky Lab que soportan la administración remota) o un archivo auto-extraíble de la aplicación Kaspersky Lab (archivo con la extensión **.exe** y que puede descargarse del sitio Web Kaspersky Lab). Como resultado, se rellenarán automáticamente los campos con el nombre de aplicación y el número de versión.

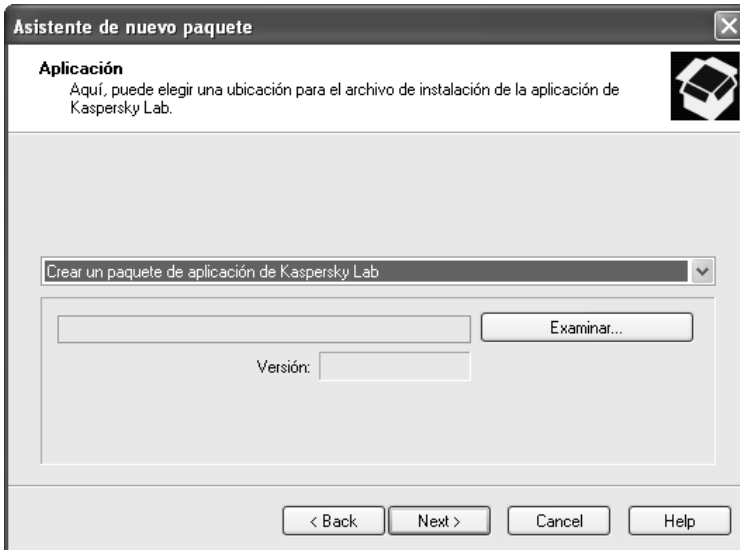


Figura 17. Crear un paquete de instalación. Seleccionar la aplicación a instalar

La configuración del paquete de instalación se creará de manera predeterminada y corresponderá con la aplicación seleccionada para ser instalada. Puede cambiar la configuración después de la creación del paquete mediante la ventana de revisión de propiedades del paquete (ver sección 4.1.2, página 40).

Si crea un paquete de instalación para instalar otras aplicaciones (ver Figura 18. Paquete de instalación y de creación para instalar la aplicación especificada por el usuario.):

- Seleccione **Crear un paquete de instalación para la aplicación especificada por el usuario** en la lista desplegable;
- Especifique la ruta al paquete de distribución de la aplicación mediante el botón **Examinar...**
- marque la casilla **Copiar toda la carpeta en el paquete de instalación**, si el paquete debe contener todo el contenido de la carpeta en la que está ubicado el archivo de distribución;
- Especifique los parámetros utilizados para ejecutar el archivo ejecutable en la línea de entrada proporcionada si este tipo de parámetros se requieren para instalar la aplicación (por ejemplo, ejecución en modo no interactivo).

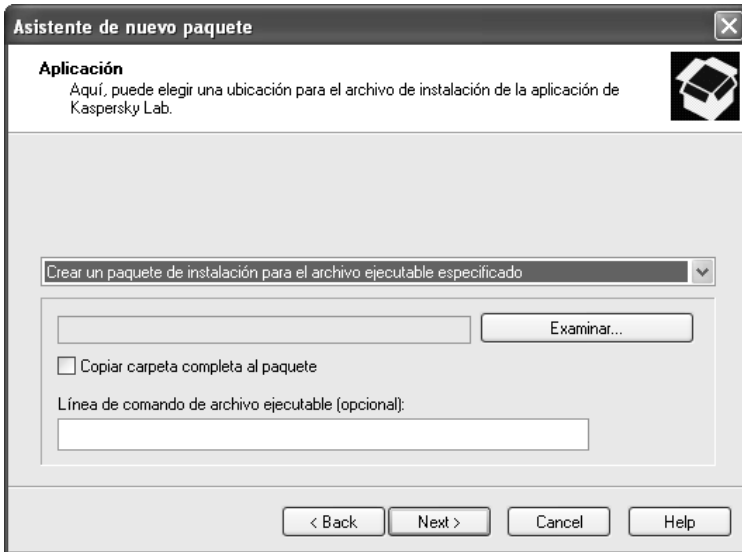


Figura 18. Paquete de instalación y de creación para instalar la aplicación especificada por el usuario.

4. En la siguiente ventana del asistente (ver Figura 19. Crear un paquete de instalación. Seleccionar la clave de licencia), puede especificar la clave de licencia que será incluida en el paquete de instalación. Con este fin, pulse el botón **Examinar...** y seleccione el archivo requerido de la clave de licencia (archivo sin extensión **.key**)

Si no desea incluir la clave de licencia en la instalación, simplemente pulse el botón **Siguiente>**.

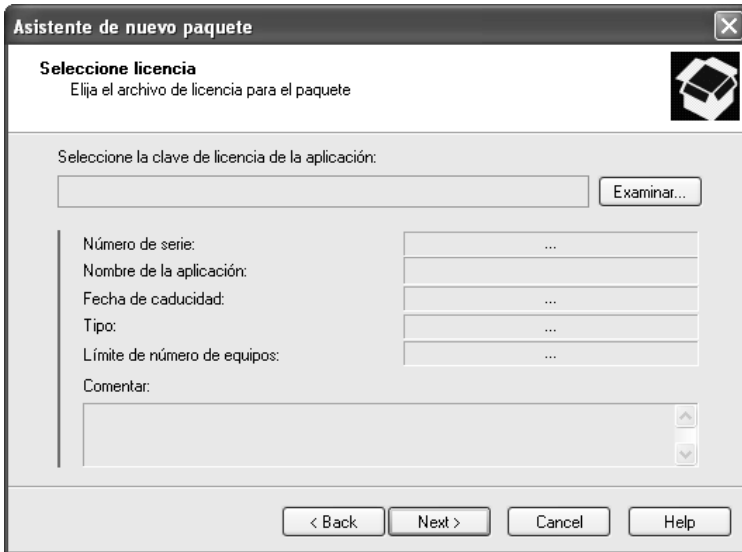


Figura 19. Crear un paquete de instalación. Seleccionar la clave de licencia

5. A continuación, el conjunto de archivos requerido para la instalación de la aplicación especificada en los equipos cliente se descargarán de la carpeta compartida del Servidor de Administración y se realizará una comprobación de si el complemento de administración de la aplicación seleccionada está instalado en el equipo administrador. Si este complemento no está instalado o su versión es anterior a la versión incluida en el paquete de distribución, el nuevo complemento será instalado y el antiguo complemento será remplazado.

Tras la finalización del asistente, el paquete de instalación creado será agregado al nodo **Instalación remota** y se mostrará en el panel de resultados.

4.1.2. Revisar y configurar los parámetros del paquete de instalación

Para revisar las propiedades del paquete de instalación, cambie su nombre y parámetros:

En el nodo **Instalación Remota** en el árbol de consola, seleccione el paquete de instalación requerido en el panel de resultados y utilice el

comando **Propiedades** del menú contextual o del comando análogo del menú **Acción**.

Se abrirá la ventana **Propiedades <Nombre del paquete de instalación>** ver Figura 20. Ventana de revisión de propiedades del paquete de instalación La ficha **General**) que consiste en las fichas **General, Parámetros, Licencias y Reinicio del sistema operativo**.



Figura 20. Ventana de revisión de propiedades del paquete de instalación La ficha **General**

La ficha **General** (ver Figura 20. Ventana de revisión de propiedades del paquete de instalación La ficha **General**) incluye información general sobre el paquete:

- Nombre del paquete;
- Nombre y versión de la aplicación para cuya instalación se ha creado el paquete;
- Tamaño del paquete;
- Fecha de creación.

La ficha **Propiedades** (ver Figura 21. Ventana de revisión de propiedades del paquete de instalación de propiedades del paquete de instalación La ficha **Parámetros**) contiene los parámetros del paquete de instalación para la aplicación para cuya instalación se ha creado el paquete. Estos parámetros se crean de forma predeterminada durante la creación del paquete y, si es necesario, puede modificarlos.



Figura 21. Ventana de revisión de propiedades del paquete de instalación
La ficha **Parámetros**

La ficha **Licencia** (ver Figura 22. Ventana de revisión de propiedades del paquete de licencia de instalación de licencia de instalación La ficha **Licencia**) contiene información general sobre la licencia de la aplicación para cuya instalación se creó el paquete.

La ficha **Licencia** no está disponible en las propiedades del paquete de instalación del Agente de Red.

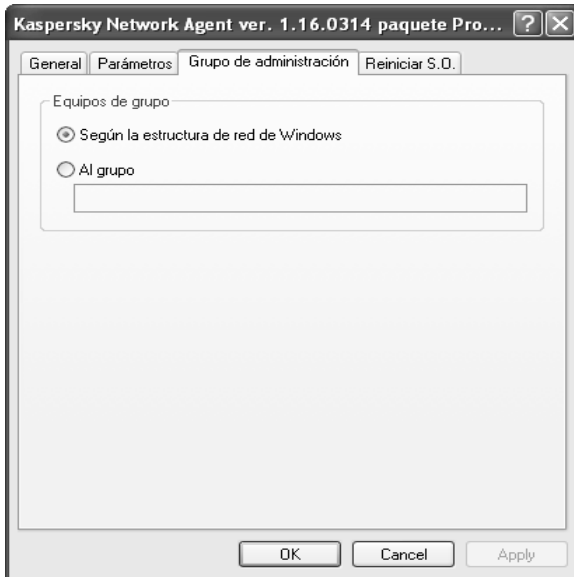


Figura 22. Ventana de revisión de propiedades del paquete de instalación
La ficha **Licencia**

En la ficha **Reinicio del SO** Figura 23. Ventana de revisión de propiedades del paquete de instalación (La ficha **Reinicio del Sistema Operativo**) puede determinar las acciones a realizar si el equipo debe ser reiniciado después de la instalación de la aplicación. Puede seleccionar una de las siguientes opciones:

- **No reiniciar el sistema operativo**
- **Reiniciar el sistema operativo automáticamente**
- **Solicitar al usuario una acción** - si se selecciona esta opción, puede:
 - Crear un mensaje de información que será mostrado para notificar al usuario que el sistema operativo debe ser reiniciado, en el campo de entrada establecido.
 - Especificar una frecuencia de notificaciones sobre el reinicio del sistema operativo si el usuario ha cancelado el reinicio, marcando la casilla **repetir solicitud cada (min.)** y especificando el intervalo en el que se mostrará el mensaje.
 - Especificar el reinicio automático del sistema operativo del equipo si no lo realiza el usuario en un intervalo de tiempo

específico desde el momento de la instalación de la aplicación. Con este fin, marque la casilla **Forzar el reinicio después de (min.)** y especifique el intervalo de tiempo.



Figura 23. Ventana de revisión de propiedades del paquete de instalación
La ficha **Reinicio del Sistema Operativo**

4.1.3. Crear y configurar el paquete de instalación del Agente de Red

El paquete de instalación de la instalación remota del Agente de Red no necesita crearse de forma manual. Se crea automáticamente durante la instalación de Kaspersky Administration Kit y se ubica en el nodo **Instalación Remota**.

Si el paquete para la instalación remota del Agente de Red ha sido eliminado, entonces, para crearlo de nuevo, seleccione el archivo **kinagent.kpd** ubicado en la carpeta NetAgent del paquete de distribución Kaspersky Administration Kit para utilizarlo como el archivo que contiene la descripción.

Los parámetros de instalación del Agente de Red contienen un conjunto mínimo de parámetros requeridos para asegurar el funcionamiento del componente inmediatamente después de su instalación. Los valores de los parámetros

corresponden con los valores de los parámetros predeterminados de la aplicación. Si fuera necesario, puede cambiarlos en las fichas Parámetros de la ventana de revisión de propiedades del paquete de instalación (ver Figura 21. Ventana de revisión de propiedades del paquete de instalación La ficha **Parámetros**).

El grupo de campos **Conexión al Servidor de Administración** contiene los parámetros utilizados por el Agente de Red, después de su instalación en los equipos cliente, para conectar con el Servidor de Administración (por defecto, los valores del servidor actual se utilizarán durante la creación).

- Dirección del equipo donde se ejecuta el Servidor de Administración.
- Número de puerto utilizado para la conexión no segura con el Servidor de Administración. De manera predeterminada, se utiliza el puerto **14000**. Si este puerto está ocupado, puede cambiarlo.
- Número de puerto utilizado para la conexión segura con el Servidor de Administración usando el protocolo SSL. De manera predeterminada, se utiliza el puerto **13000**.

Únicamente se permite notación decimal.

- Archivo de certificado para la autenticación de acceso al Servidor de Administración. El valor de este parámetro está determinado por la casilla **Usar el certificado del servidor**.

Si no se marca esta casilla por defecto, el archivo del certificado se obtendrá automáticamente desde el Servidor de Administración cuando el Agente se conecta a éste por primera vez.

Si la casilla **Usar certificado del servidor** está marcada, la autenticación se realizará en función del archivo del certificado especificado usando el botón **Examinar**. El archivo tiene la extensión **.cer** y está ubicado en la carpeta **Cert** de la carpeta de instalación de Kaspersky Administration Kit. Puede cambiar el archivo del certificado seleccionando el archivo que necesite usando el botón **Examinar**.

- El puerto que utilizará el Agente de Red para conectar con el Servidor: Simple o seguro. El valor de este parámetro está determinado por la casilla **Usar conexión SSL**. Si la casilla está marcada, la conexión se realizará a través de un puerto seguro usando el protocolo SSL, si la casilla no está marcada, la conexión se realiza a través de un puerto no seguro.
- Los parámetros de conexión del servidor Proxy. Si un servidor Proxy es utilizado por el Agente de Red para conectar con el Servidor, marque la casilla **Usar servidor Proxy**. A continuación, pulse el botón **Parámetros** y en la ventana que se abre introduzca la dirección del servidor Proxy, nombre de usuario y contraseña.

Tras la instalación del Agente de Red, puede cambiar los valores de los parámetros utilizados para conectar con el Servidor de Administración usando la directiva y los parámetros de la aplicación.

Si reinstala de forma remota el Agente de Red en el equipo cliente, los valores de los parámetros utilizados para conectar con el Servidor y con el certificado del Servidor de Administración se reemplazarán por unos nuevos.

En el grupo de campos **Asignar equipos a grupos** se define un subgrupo del grupo **red** en el que se agregan los equipos después de que el Agente de Red haya sido instalado en ellos. Puede seleccionar las siguientes opciones:

- Agregar equipos a las carpetas **Correspondientes con la posición del equipo en la red de Windows**: Dominio o grupo de trabajo (esta opción está seleccionada por defecto);
- Agregar todos los equipos **Al grupo** especificado en el campo de entrada. Si selecciona esta opción, introduzca el nombre de la carpeta en el siguiente campo. Si el grupo **Red** no contiene esa carpeta, se creará (también puede especificar el nombre de una carpeta existente del grupo **Red**).

Esta carpeta se utilizará para almacenar sólo los equipos recientemente detectados en la red, si el equipo no ha sido detectado por el Servidor de Administración y puesto en la carpeta correspondiente a su posición en la red antes de la instalación del Agente de Red. Los equipos detectados en la red antes de la instalación del Agente de Red permanecerán en sus antiguas ubicaciones en el grupo **Red**.

Después de la instalación del Agente de Red, puede no cambiar la carpeta para almacenar los equipos en el grupo **Red** ya que este parámetro no está incluido en la directiva y en los parámetros de aplicación.

El Agente de Red se instala, en el equipo, como un servicio que tiene el siguiente conjunto de características:

- Nombre de servicio **KLNAgent**;
- Con el nombre **Kaspersky Network Agent**;
- Inicio automático en la carga del sistema operativo;
- Con la cuenta **Local system**.

Puede revisar las propiedades del servicio **Agente de Red Kaspersky** y controlar su funcionamiento mediante las herramientas de administración estándar de Windows **Administración de equipos** → **Servicios**.

4.1.4. Crear una tarea para la distribución del paquete de instalación en los Servidores de Administración esclavo

Para crear la tarea para la distribución del paquete de instalación en los Servidores de Administración esclavo

1. Conecte al Servidor de administración que necesita.
2. Seleccione la entrada **Tareas Globales** en el árbol de consola, abra el menú contextual y seleccione el comando **Nueva→ Tarea** o utilice el elemento análogo desde el menú **Acción**. Se iniciará el asistente. Siga sus instrucciones.
3. Para la aplicación Kaspersky Administration Kit, seleccione el tipo de tarea **Distribución del paquete de instalación**.
4. En la siguiente ventana del asistente (ver Figura 24. Crear un conjunto de paquetes de instalación), seleccione qué paquetes de instalación deben ser distribuidos. Seleccione una de las opciones siguientes:
 - Todos los paquetes de instalación.
 - Paquetes de instalación seleccionados En este caso, marque las casillas junto a los nombres de los paquetes de instalación requeridos en la siguiente tabla.

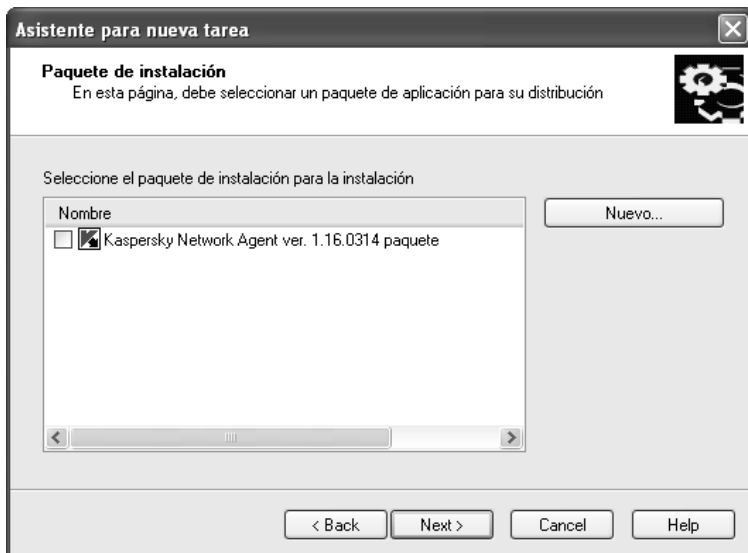


Figura 24. Crear un conjunto de paquetes de instalación

Especifique el valor requerido en el campo **número máximo de instalaciones compartidas**.

5. En la siguiente ventana del asistente (ver Figura 25. Seleccionar Servidores de Administración esclavo), marque las casillas junto a los nombres de los Servidores de Administración esclavo a los que se deben distribuir los paquetes de instalación.

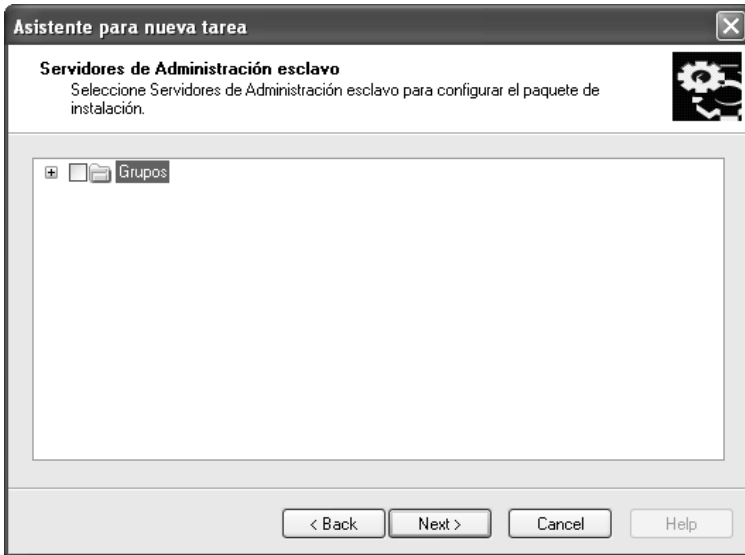


Figura 25. Seleccionar Servidores de Administración esclavo

6. A continuación, determine bajo qué cuenta se iniciará la tarea en los equipos (para más detalles, ver sección 4.1.6, página 53).
7. En la siguiente ventana del asistente, especifique la planificación de inicio de tarea (para más detalles, ver sección 4.1.6, página 53).
8. Para salir del asistente una vez que haya finalizado, pulse el botón **Finalizar**.

4.1.5. Distribuir de los paquetes de instalación en un grupo mediante los agentes de red

Para distribuir los paquetes de instalación en un grupo, puede usar los agentes de actualización. Los agentes de actualización reciben paquetes de instalación y actualizaciones desde el Servidor de Administración y los guardan en la carpeta de instalación de la aplicación Kaspersky Lab.

La ubicación de la carpeta que contiene las actualizaciones y los paquetes de instalación no puede cambiarse, su tamaño no puede limitarse.

A continuación, los paquetes de instalación serán distribuidos a los equipos cliente usando la entrega multi-dirección. La entrega de los nuevos paquetes de instalación en un grupo sólo se realiza una vez. Si en el momento de la entrega, un equipo cliente se desconecta de la red lógica corporativa, entonces, cuando la tarea de instalación se ejecute, el Agente de Red descargará automáticamente el paquete de instalación requerido desde el agente de actualización.

Para crear una lista de agentes de actualización y configurarlos para distribuir los paquetes de instalación en los equipos de un grupo,

1. Conéctese al Servidor de administración requerido.
2. Seleccione el grupo requerido en el árbol de consola, abra el menú contextual y seleccione el comando **Propiedades** o utilice un elemento análogo desde el menú **Acción**.
3. En la ventana de propiedades de grupo que se abrirá, en la ficha **Agentes de Actualización** (ver Figura 26. La ventana propiedades de grupo. La ficha **Agente de Actualización**), cree la lista de equipos que actuarán como agentes de actualización en el grupo, usando los botones **Agregar** y **Eliminar**.

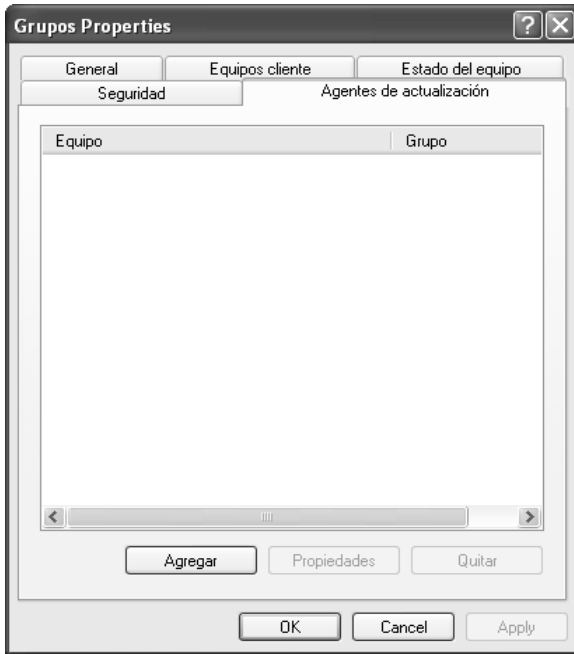


Figura 26. La ventana propiedades de grupo.
La ficha **Agente de Actualización**

4. Modifique los parámetros del agente de actualización. Con este fin, seleccione el agente en la lista y pulse el botón **Propiedades**. En la ventana <Actualizar nombre del agente> propiedades que se abrirá (ver Figura 27.) Haga lo siguiente:
 - Especifique el número del puerto utilizado por el equipo cliente para conectar con el agente de actualización. El número de puerto predeterminado es el **14001**. Si este puerto ya está en uso, puede cambiarlo.
 - Especifique el número de puerto utilizado por el equipo cliente para conectar de forma segura con el agente de actualización usando el protocolo SSL. El número de puerto predeterminado es 13001.
 - Marque la casilla **Usar entrega multi-dirección IP** y rellene los campos **Dirección IP de entrega** y **Número de puerto MULTICAST-IP**.
5. Pulse el botón **Aplicar** o **Aceptar**.



Figura 27. Ventana Propiedades del Agente de actualización

4.1.6. Crear una tarea de instalación remota

Cuando se ejecuta esta tarea, la instalación remota de software en los equipos cliente se realiza usando uno de los siguientes métodos: **Instalación forzada o instalación usando el escenario de inicio.**

La **Instalación forzada** permite llevar a cabo la instalación remota de software en los equipos cliente especificados en la red lógica. Cuando se ejecuta la tarea, el Servidor de Administración copiará de la carpeta compartida un conjunto de archivos requeridos para instalar la aplicación en cada equipo cliente en el archivo temporal e inicia la aplicación de instalación en cada equipo. Para realizar con éxito la tarea de instalación forzada, el Servidor de Administración debe tener los permisos del administrador local en los equipos cliente de la red lógica. Se aconseja este método para instalar aplicaciones en equipos con Microsoft Windows NT/2000/2003/XP que permiten esta funcionalidad o en equipos con Microsoft Windows 98/Me en los que esté instalado el Agente de Red.

Si la conexión entre el Servidor de Administración y un equipo cliente se establece a través de Internet o si está protegida por un cortafuegos, las carpetas compartidas no pueden utilizarse para transferir datos. En este caso, los archivos requeridos para instalar la aplicación en el equipo cliente pueden ser entregados por el Agente de Red. El Agente de Red se instala en estos equipos de forma local.

El segundo método – **instalación usando el escenario de inicio** – permite asignar una tarea de instalación remota para una cuenta de un usuario específico (o de varios usuarios). Como resultado de la tarea de ejecución, se introducirá un registro de los usuarios seleccionados sobre el inicio de la aplicación del instalador en el escenario de inicio. La aplicación del instalador está ubicada en la carpeta compartida en el Servidor de Administración. Para asegurar una ejecución de tarea adecuada, la cuenta bajo la que se ejecuta el Servidor de Administración deben tener permiso para modificar los escenarios de inicio en la base de datos del controlador de dominio. Como resultado del registro del usuario con el dominio, se realizará un intento de instalación de la aplicación en el equipo cliente desde el que se ha registrado el usuario. Se recomienda este método para la instalación de las aplicaciones Kaspersky Lab en equipos con MS Windows 98/Me.

Para asegurar una ejecución, con éxito, de la tarea de instalación remota usando el escenario de inicio, los usuarios para los que se realizan los cambios en los escenarios deben tener permisos del administrador local en sus correspondientes equipos.

Las tareas de grupo para la instalación remota de software en los equipos cliente se ejecutan usando solamente el método de instalación forzada. Al crear una tarea global, puede seleccionar el método que requiera: La instalación forzada o la instalación usando el escenario de inicio.

Para crear una tarea global para la instalación remota usando el método de instalación forzada:

Conéctese al Servidor de administración requerido.

1. Seleccione la entrada **Tarea Global** en el árbol de consola, abra el menú contextual y seleccione el comando **Nueva/Tarea** o utilice el elemento análogo desde el menú **Acción**. Se iniciará la tarea de creación del asistente. Siga sus instrucciones.
2. Especifique el nombre de la tarea.
3. Al seleccionar la aplicación y el tipo de tarea (ver Figura 28. Especificar el tipo de tarea), especifique los valores de **Kaspersky Administration Kit** e **Instalación remota de la aplicación** respectivamente.

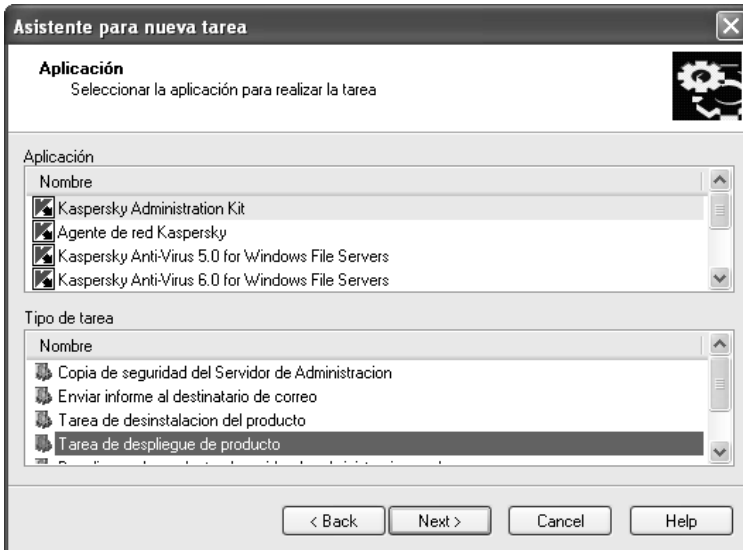


Figura 28. Especificar el tipo de tarea

4. A continuación, especifique el paquete de instalación que se instalará durante la ejecución de esta tarea (ver Figura 29. Seleccionar el paquete de instalación para la instalación). Seleccione el paquete requerido de entre los paquetes creados para el Servidor de Administración o genere uno nuevo mediante el botón **Nuevo...**

Algunas aplicaciones que soportan la administración a través de Kaspersky Administration Kit pueden instalarse en los equipos cliente, sólo de forma local. Para más información, consulte las Guías de las aplicaciones correspondientes.

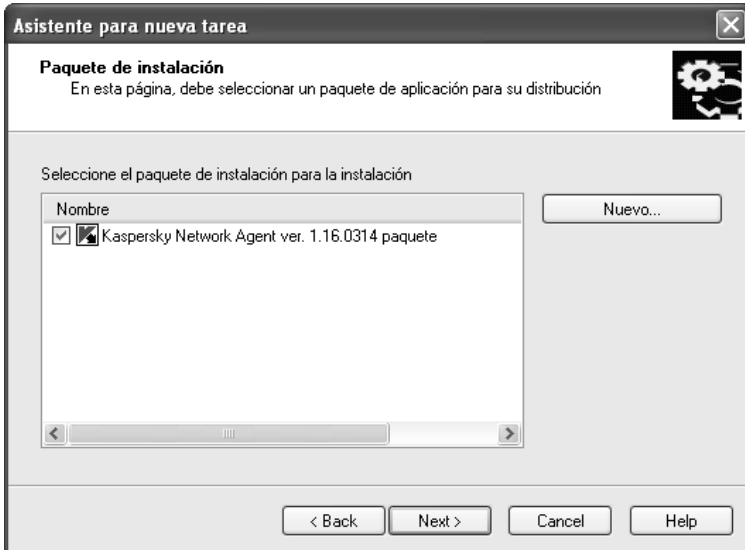


Figura 29. Seleccionar el paquete de instalación para la instalación

5. Durante esta etapa, seleccione la opción **Instalación de inserción** (ver Figura 30. Seleccionar el método de instalación)

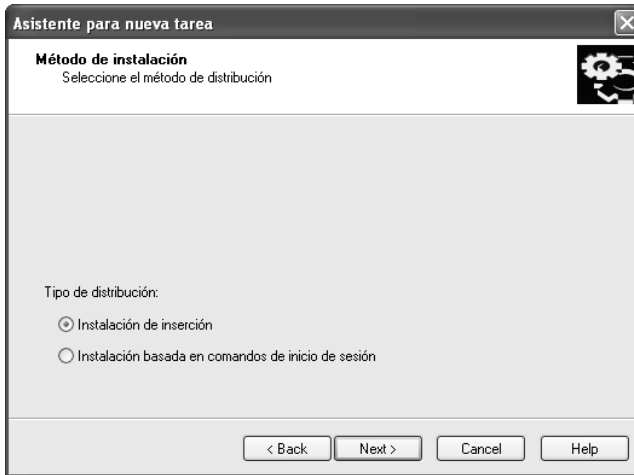


Figura 30. Seleccionar el método de instalación

6. En esta ventana del asistente (ver Figura 31. Parámetros de instalación adicionales) se le ofrecerá determinar unos parámetros de instalación adicionales.
- Si la aplicación debe ser reinstalada en caso de que ya se haya instalado en el equipo.

Marque la casilla **No instalar la aplicación si ya está instalada** para evitar repetir la instalación (esta casilla está marcada de forma predeterminada). En caso de equipos en los que la aplicación esté instalada de forma local o sea el resultado de un inicio planificado anterior de la tarea de instalación remota, la tarea no se iniciará.

Si la casilla está desmarcada, la tarea de instalación remota se iniciará mediante planificación hasta que se alcance el número máximo de intentos de instalación de la aplicación.

- Para especificar el método de entrega de los archivos requeridos para instalar la aplicación en los equipos cliente.

Con este fin, realice lo siguiente en el grupo de campos **Descargar el paquete de instalación:**

- Marque la casilla **Usar los recursos de Microsoft Windows desde la carpeta de acceso público** si desea que la transferencia de los archivos requeridos para la

instalación de la aplicación en los equipos cliente se realice mediante las herramientas de Windows y las carpetas compartidas (esta casilla está marcada de forma predeterminada).

- o Marque la casilla **Usar Agente de Administración** de manera que el Agente de Red instalado en cada equipo entregue los archivos a los equipos cliente (esta casilla está marcada por defecto).
- o En el campo **El número máximo de descargas simultáneas** especifique el número máximo de equipos cliente que pueden descargar información desde el Servidor de Administración.
- Especifique el número de intentos para realizar la instalación en caso de tarea planificada iniciada al introducir el valor en el campo **Número de intentos**. Se realizan diferentes intentos en caso de error durante la ejecución en el transcurso de la instalación anterior.

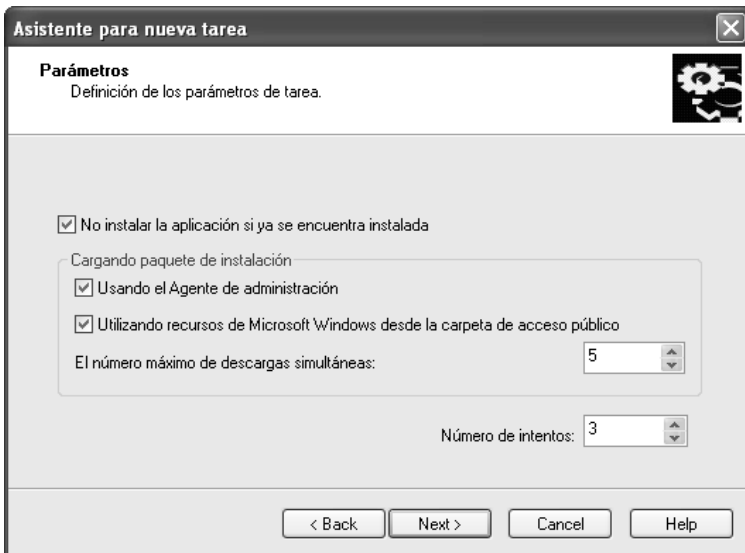


Figura 31. Parámetros de instalación adicionales

7. Durante esta etapa (ver Figura 32. Seleccionar instalación conjunta con el Agente de Red) se le ofrecerá instalar el Agente de Red con la aplicación.

Le recomendamos que use la instalación conjunta con el fin de reducir la carga en el Servidor de Administración. Con este fin, marque la casilla **Instalar con el Agente de Administración** y marque la casilla junto al nombre del paquete de instalación requerido. Si fuera necesario, cree un nuevo paquete de instalación usando el botón **Crear**.

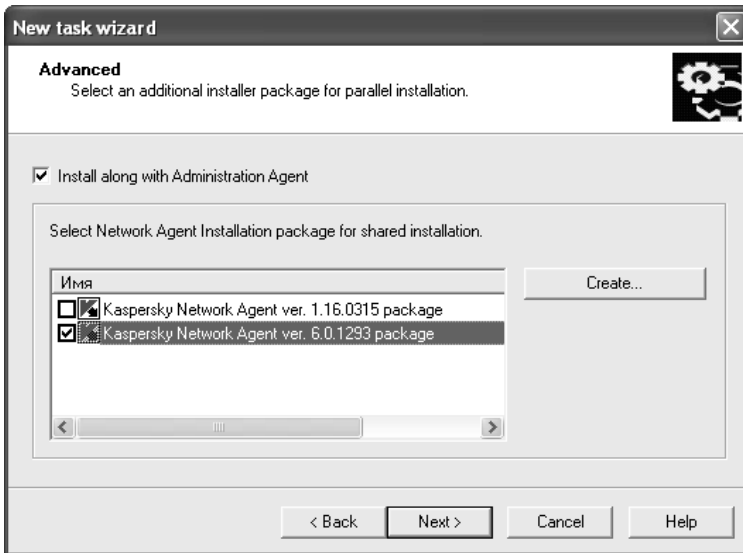


Figura 32. Seleccionar instalación conjunta con el Agente de Red

Determine el método para seleccionar los equipos en los que se creará la tarea (ver Figura 33. Seleccionar el método a utilizar para seleccionar los equipos cliente):

- **Quiero seleccionar equipos mediante la red de Windows.** En este caso, se seleccionarán los equipos para la instalación en base a los datos recibidos por el Servidor de Administración en función del sondeo de red corporativa de Windows.
- **Quiero definir direcciones IP para los equipos.** En este caso, los equipos de la instalación se seleccionarán manualmente.

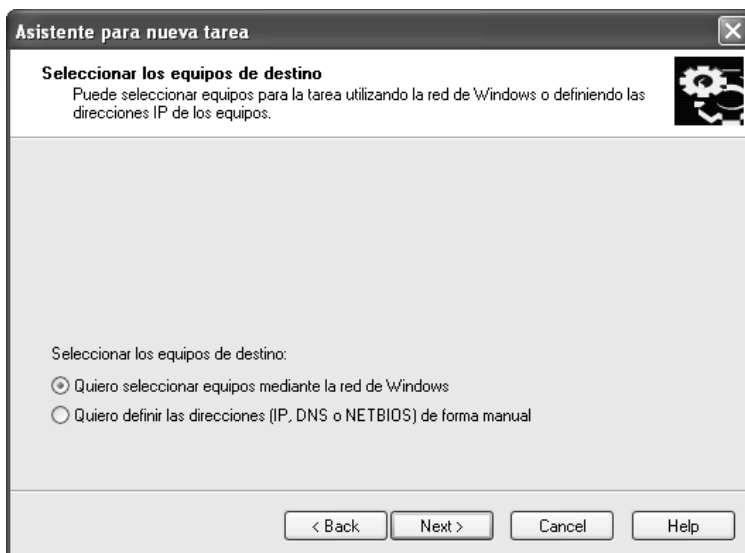


Figura 33. Seleccionar el método a utilizar para seleccionar los equipos cliente

Si los equipos son seleccionados en función de los datos recibidos como resultado de un sondeo de red de Windows, la lista se creará en la ventana del asistente (ver Figura 34. Crear la lista de equipos para la instalación en función de los datos de la red de Windows) y se realizará de la misma forma que al agregar equipos a la red lógica (para más detalles, ver el Libro de Consulta de Kaspersky Administration Kit). Puede seleccionar los equipos de la red lógica (la carpeta **Grupos**) o los equipos que todavía no se han incluido en la red lógica (la carpeta **Red**).

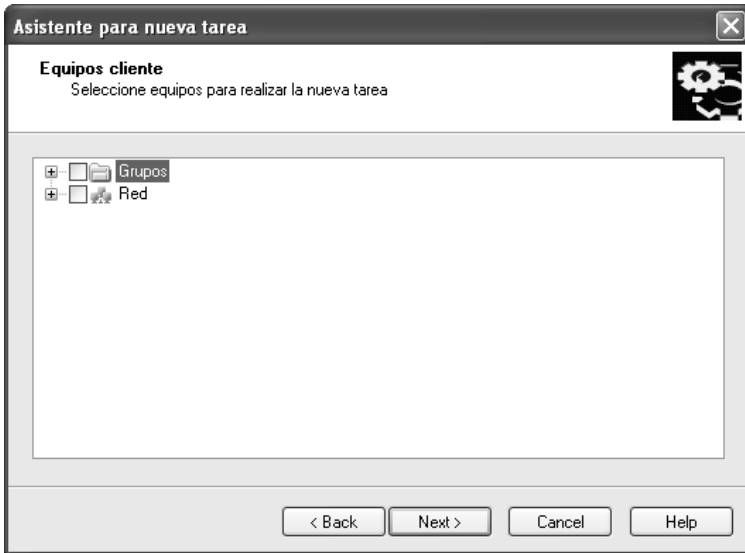


Figura 34. Crear la lista de equipos para la instalación en función de los datos de la red de Windows

Si selecciona los equipos manualmente, entonces, la lista se crea introduciendo los nombres NETBIOS o DNS, las direcciones IP (o un rango de direcciones IP) de los equipos o importando la lista desde un archivo de *.txt* en el que cada dirección debe introducirse en una nueva línea (ver Figura 35. Crear la lista de equipos para la instalación en función de las direcciones IP).

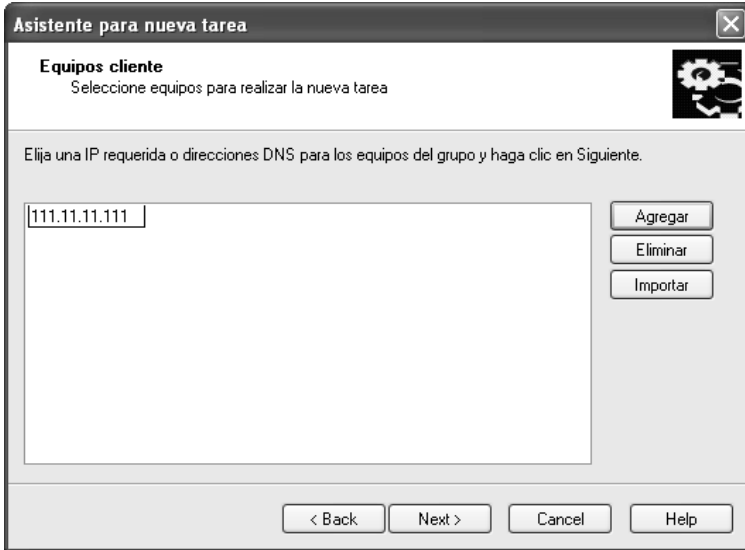


Figura 35. Crear la lista de equipos para la instalación en función de las direcciones IP

8. En la siguiente ventana del asistente, especifique la cuenta bajo la cual se iniciará la tarea de distribución en los equipos (ver Figura 36. Seleccionar la cuenta).

La cuenta debe tener permisos del administrador para todos los equipos en los que pretende realizar la instalación remota de software.

Al instalar el software en los equipos incluidos en diferentes dominios, debe existir una relación de confianza entre este tipo de dominios y el dominio en el que el Servidor de Administración está trabajando.

Seleccione una de las opciones siguientes:

- **Cuenta predeterminada** – si el Servidor de Administración se ejecuta bajo la cuenta de usuario del dominio (ver sección 3.2, página 16) y esta cuenta tiene los permisos requeridos para la instalación del software.
- **Cuenta especificada** – si el Servidor de Administración se ejecuta bajo la cuenta del sistema o si la cuenta del Servidor de Administración no tiene los permisos requeridos para iniciar la tarea de distribución.

Para instalar de forma remota el software en los equipos no incluidos en el dominio, inicie la tarea de instalación remota bajo la cuenta de un usuario que tiene los permisos de acceso de estos equipos.

En los campos proporcionados a continuación, especifique las características del usuario cuya cuenta cumple las condiciones requeridas.

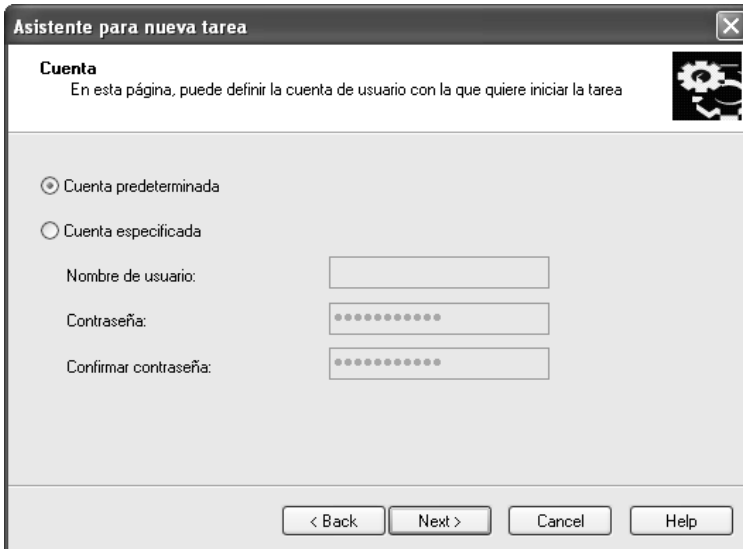


Figura 36. Seleccionar la cuenta

9. A continuación, cree la planificación para iniciar la tarea (ver Figura 37. Inicio de la tarea diaria).
 - Seleccione el modo de inicio de la tarea requerida desde la lista desplegable **Inicio planificado**.
 - **Manualmente**
 - **Cada N hora(s)**
 - **Diario**
 - **Semanal**
 - **Mensual**

- o **Una vez** (en este caso, la tarea de distribución se ejecutará sólo una vez en el equipo, independientemente del resultado de su ejecución).
- o **Ahora** (inmediatamente después de la creación de la tarea y de la finalización del asistente)
- Configure los parámetros de planificación en el grupo de campos, en función del modo seleccionado (ver detalles en la Guía de Referencia de Kaspersky Administration Kit)

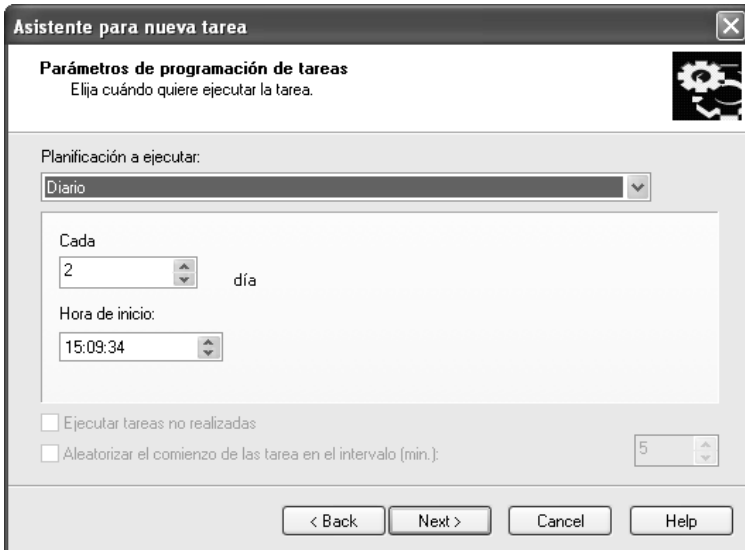


Figura 37. Inicio de la tarea diaria

Para crear una tarea de distribución global mediante el escenario de inicio:

1. Conéctese al Servidor de administración requerido.
2. Seleccione el nodo **Tarea Global** en el árbol de consola, abra el menú contextual y seleccione el comando **Nueva/Tarea** o utilice el elemento análogo desde el menú **Acción**. Se iniciará la tarea de creación del asistente. Siga sus instrucciones.
3. Especifique el nombre de la tarea.
4. Al seleccionar la aplicación y el tipo de tarea (ver Figura 28. Especificar el tipo de tarea), seleccione **Kaspersky**

Administration Kit e Instalación remota de la aplicación respectivamente.

5. En la siguiente ventana (ver Figura 29. Seleccionar el paquete de instalación para la instalación) especifica el paquete a utilizar para la instalación. Esto se realiza de la misma forma que el método de instalación forzada (ver arriba).
6. A continuación, seleccione la opción **Instalación usando el escenario de inicio** (ver Figura 30. Seleccionar el método de instalación)
7. En la siguiente ventana del asistente (ver Figura 35. Crear la lista de equipos para la instalación en función de las direcciones IP) seleccione las cuentas de usuarios para las que se deben cambiar el escenario de inicio.

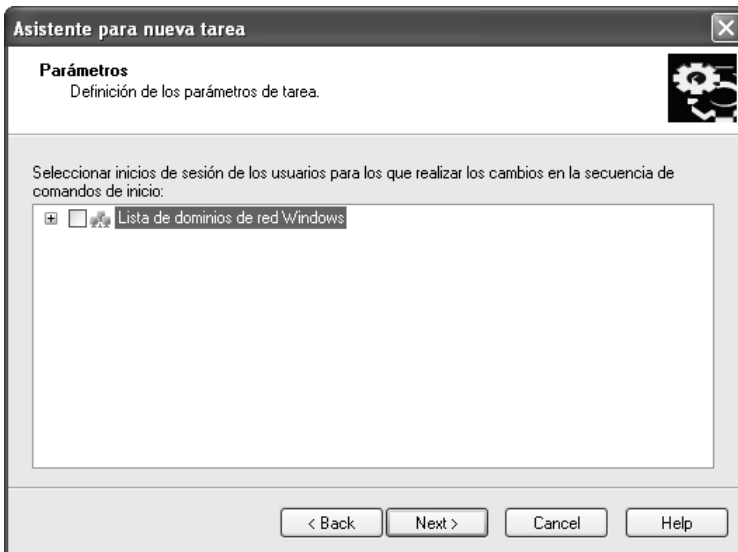


Figura 38. Seleccionar cuentas

8. Durante la siguiente etapa del asistente (ver Figura 36. Seleccionar la cuenta), de forma similar al uso del método de instalación forzada (ver arriba),
9. En la planificación de inicio de **Task** (ver Figura 37. Inicio de la tarea diaria) cree una planificación de la misma forma que se crea si se utiliza el método de instalación forzada (ver arriba).

Tras la finalización del asistente, la tarea de distribución que ha creado se agregará al nodo **Tareas globales** y se mostrará en el panel de resultados. Si fuera necesario, puede modificar los parámetros de tarea (para más detalles, ver sección 4.1.7, página 65).

Con este fin:

Seleccione el nodo **Instalación remota** en el árbol de consola, seleccione el paquete de instalación requerido en el panel de resultados, abra el menú contextual y seleccione el comando **Instalar** o utilice el comando análogo del menú **Acción**. Se iniciará el asistente de creación de tarea de distribución, anteriormente descrito, sin embargo, este asistente no incluirá el tipo de tarea y los pasos de selección del paquete de instalación. Siga sus instrucciones.

De forma alternativa, puede iniciar el asistente de creación de tarea de distribución de grupo.

Con este fin:

Seleccione el nodo **Grupos** en el árbol de consola, abra el menú contextual y utilice el comando **Instalar** o utilice el elemento análogo desde el menú **Acción**. Se iniciará el asistente de creación de tarea de distribución, anteriormente descrito, sin embargo, este asistente no incluirá el tipo de tarea ni los pasos de selección del grupo del equipo. Siga sus instrucciones.

4.1.7. Configurar la tarea de distribución

Las tareas de distribución se configuran de la misma forma que cualquier tarea (para más detalles, ver Libro de Referencia de Kaspersky Administration Kit). A continuación, se enumera una relación de parámetros para este tipo de tareas proporcionada en la ficha **Propiedades**.

Si está modificando una tarea que realizará una instalación forzada (ver Figura Figura 39. Configurar una tarea de distribución Método de instalación forzada), puede:

- Determinar si necesita reinstalar la aplicación si ésta ya ha sido instalada en el equipo cliente;
- Especificar el método a utilizar para la entrega de los archivos requeridos para instalar la aplicación en el equipo cliente y especificar el número máximo de conexiones simultáneas;
- Especificar el número de intentos de realización de la instalación si la tarea se ejecuta en función de una planificación.

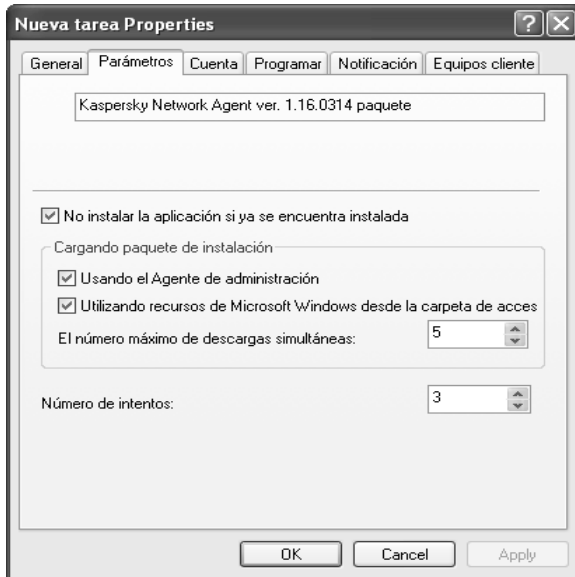


Figura 39. Configurar una tarea de distribución
Método de instalación forzada

Al configurar una tarea de distribución usando un escenario de inicio, puede utilizar la ficha **Parámetros** para cambiar la lista de cuentas de usuarios a los que se va a modificar el escenario de inicio (ver Figura 40. Configurar una tarea de distribución usando el escenario de inicio.). Para modificar la lista, utilice los botones **Agregar** y **Eliminar**.



Figura 40. Configurar una tarea de distribución usando el escenario de inicio.

4.1.8. Eliminación remota de software

Para la eliminación remota de software:

Cree una tarea de forma similar a la creación de una tarea de distribución (ver sección 4.1.6, página 53); seleccione **Eliminación remota de la aplicación** como tipo de tarea y seleccione la aplicación Kaspersky Lab requerida desde la lista desplegable **Aplicación a eliminar** en la ventana **Aplicación** (ver Figura 41. Seleccionar una aplicación a eliminar). Para eliminar una aplicación de terceros, marque **Aplicación de terceros** y seleccione la aplicación a eliminar.

La lista desplegable contiene la lista de aplicaciones detectadas en los equipos de las redes lógicas después de que se haya instalado el Agente de Red en estos equipos.

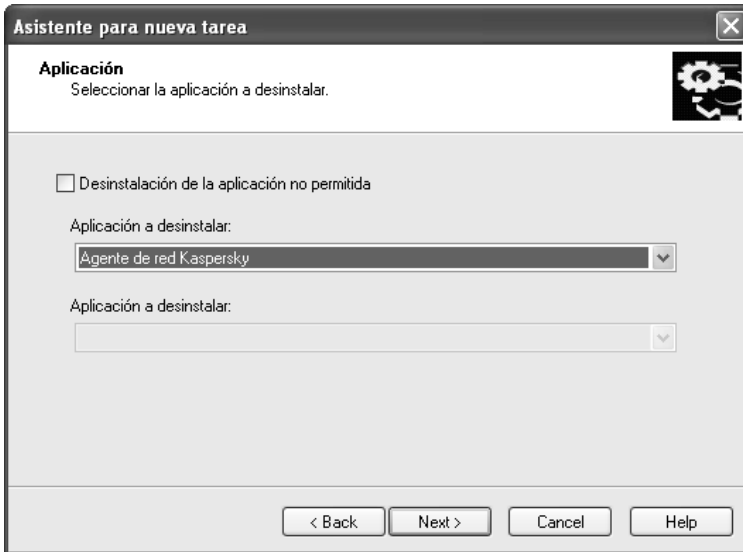


Figura 41. Seleccionar una aplicación a eliminar

La tarea que ha creado se ejecutará de acuerdo con la planificación.

4.2. Asistente de distribución

Puede utilizar el asistente de distribución para instalar las aplicaciones Kaspersky Lab. Este asistente permite la realización de la distribución de la aplicación usando el método de instalación forzada mediante el paquete de instalación creado o directamente desde el paquete de distribución.

El asistente realiza lo siguiente:

- Crea un paquete de instalación para instalar la aplicación (si el paquete todavía no ha sido instalado). El paquete se almacena en el nodo **Instalación Remota** con el nombre que corresponda con el nombre y la versión de la aplicación y puede utilizarse para instalar la aplicación más tarde.
- Crea e inicia tareas de distribución globales y de grupo. La tarea creada se ubicará en la carpeta **Tareas globales** o **Tareas de grupo** del grupo para el que se ha creado la tarea, y se podrá ejecutar más tarde. El nombre de la tarea corresponde con el nombre del paquete de la instalación de la aplicación: **Instalación <Nombre del paquete de instalación seleccionado>**.

Para instalar la aplicación usando el asistente de distribución:

1. Conéctese al Servidor de administración requerido.
2. En el árbol de consola de la ventana de aplicación principal de Kaspersky Administration Kit, seleccione el nodo correspondiente al Servidor de Administración requerido, abra el menú contextual y seleccione el comando **Asistente de distribución** o utilice el comando análogo del menú **Acción**. Se iniciará el asistente. Siga sus instrucciones.
3. En la ventana que se abrirá (ver Figura 42. Seleccionar un paquete de instalación) especifique el paquete de instalación que será instalado. Si está instalando una aplicación desde el paquete de distribución y/o el paquete de instalación no ha sido creado, genere un nuevo paquete de instalación. Con este fin, pulse el botón **Nuevo...** y se abrirá el asistente de creación del paquete de instalación (ver sección 4.1.1, página 37).

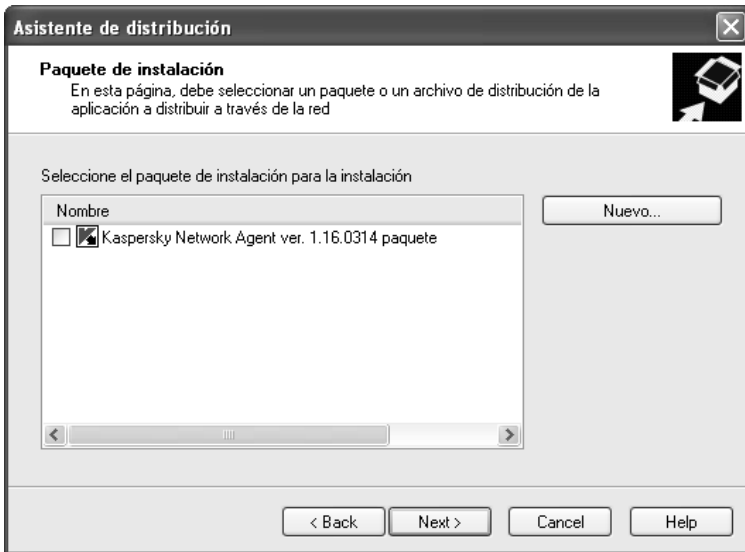


Figura 42. Seleccionar un paquete de instalación

4. En la siguiente ventana del asistente, si fuera necesario, especifique el paquete de instalación del Agente de Red que se instalará de forma conjunta (para más detalles, ver sección 4.1.6, página 53).

5. En la ventana del asistente (ver Figura 43. Seleccionar un tipo de tarea), determina en qué equipos se instalará la aplicación. Con este fin, seleccione una de las opciones:
 - **Instalar la aplicación en los equipos seleccionados**, si selecciona esta opción, entonces, una vez que se finalice el asistente, se creará una tarea de distribución global de la aplicación.
 - **Instalar la aplicación en los equipos del grupo de administración** - Se creará una tarea de grupo como resultado del funcionamiento del asistente.

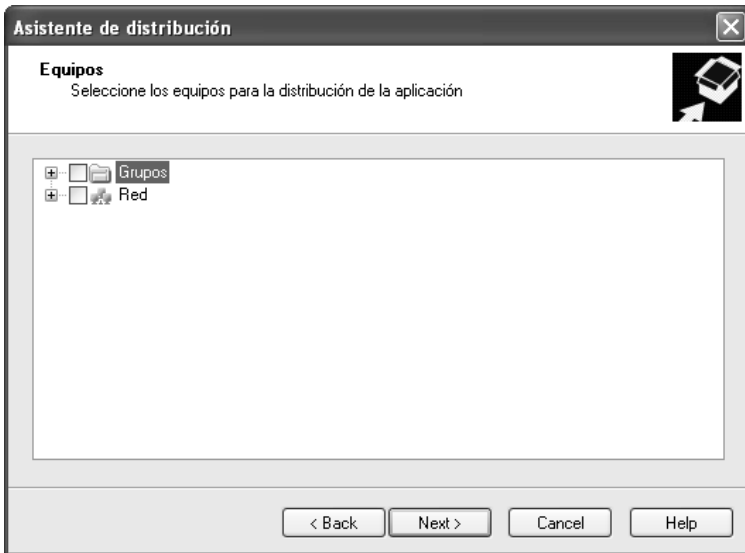


Figura 43. Seleccionar un tipo de tarea

6. A continuación, si está creando una tarea de grupo, especifique un grupo en cuyos equipos se instalará la aplicación de forma remota (ver Figura 44. Seleccionar un grupo), o seleccione los equipos para la instalación. Si la aplicación debe instalarse en todos los equipos cliente de la red lógica, seleccione el grupo **Grupos**.

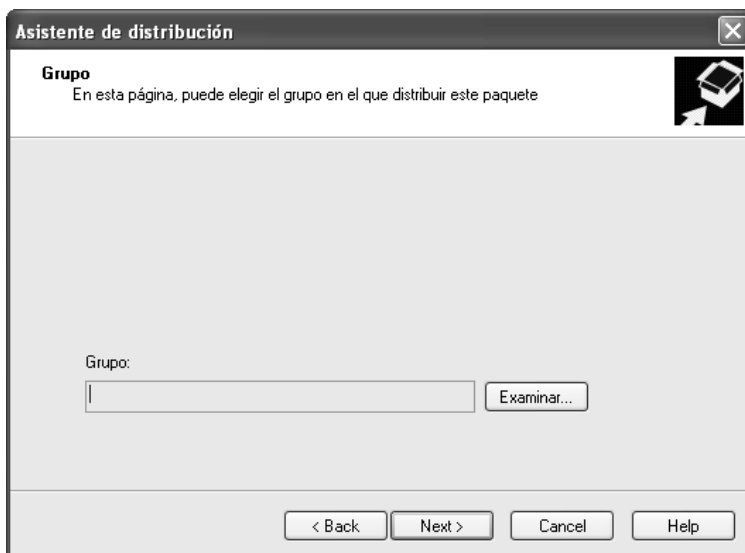
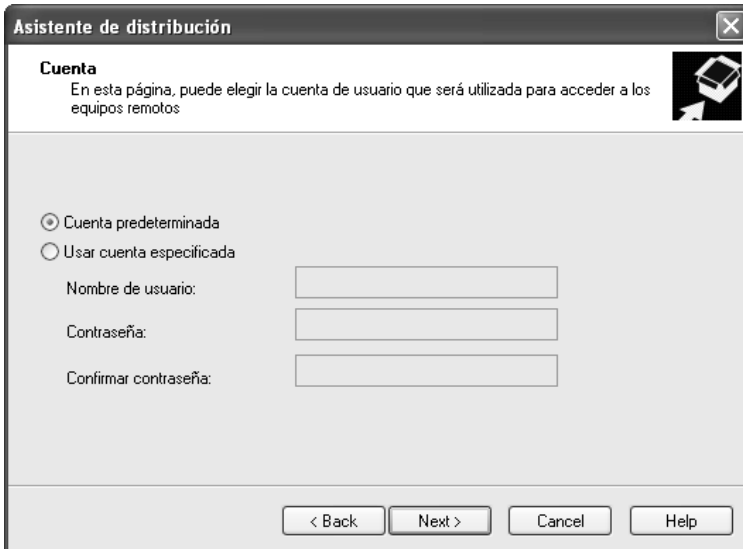


Figura 44. Seleccionar un grupo

7. A continuación, determine bajo qué cuenta se ejecutará la tarea de distribución en los equipos (para más detalles, ver sección 4.1.6, página 53).



The screenshot shows a window titled "Asistente de distribución" (Distribution Assistant) with a close button in the top right corner. The main heading is "Cuenta" (Account). Below the heading is a sub-heading "Cuenta" and a descriptive text: "En esta página, puede elegir la cuenta de usuario que será utilizada para acceder a los equipos remotos" (On this page, you can choose the user account that will be used to access the remote computers). To the right of the text is a small icon of a computer monitor. Below the text are two radio button options: "Cuenta predeterminada" (Predefined account) which is selected, and "Usar cuenta especificada" (Use specified account). Under the second option are three text input fields labeled "Nombre de usuario:" (Username), "Contraseña:" (Password), and "Confirmar contraseña:" (Confirm password). At the bottom of the window are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figura 45. Seleccionar una cuenta de usuario

8. A continuación, se abrirá una ventana que mostrará el proceso de distribución y de ejecución de la tarea de distribución en los equipos del grupo seleccionado (ver Figura 46. Ejecutar la tarea de distribución). Puede saltar a la ventana final del asistente sin esperar que finalice el proceso. Con este fin, pulse el botón **Siguiente**. Puede ver información detallada sobre los resultados de la ejecución de la tarea de cada equipo mediante el botón **Historial**.

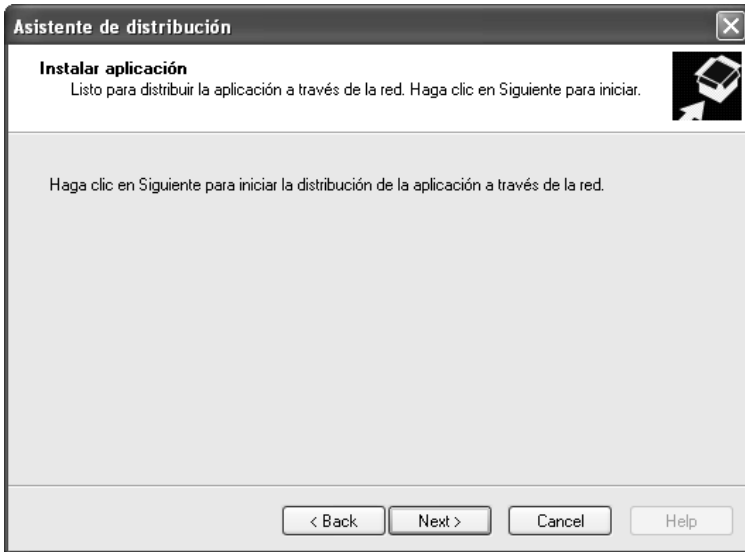


Figura 46. Ejecutar la tarea de distribución

4.3. Instalación local de software

La instalación local se ejecuta individualmente en cada equipo. Con el fin de realizar una instalación local, debe tener permisos del administrador del equipo local.

Algunas aplicaciones que permiten la administración a través de Kaspersky Administration Kit pueden instalarse en los equipos cliente, sólo de forma local. Para más información, consulte las Guías de las aplicaciones correspondientes.

El procedimiento general para la instalación de software durante la distribución local del sistema de protección antivirus puede realizarse de la siguiente forma:

- Instale el Agente de Red y configure la conexión entre el equipo cliente y el Servidor de Administración (ver sección 4.3.1, página 74);
- Instale las aplicaciones requeridas en el equipo que se incluirá en el sistema de protección antivirus, de acuerdo con la descripción de las Guías correspondientes;

- Instale el complemento de administración para cada una de las aplicaciones Kaspersky Lab instaladas en el equipo administrador (ver sección 4.3.2, página 79).

Kaspersky Administration Kit permite la instalación de la aplicación local en un modo no interactivo en función de los archivos creados durante la creación del paquete de instalación (ver sección 4.3.3, página 80).

4.3.1. Instalación de la ubicación del Agente de Red

Para instalar de forma local el Agente de Red en el equipo:

1. Ejecute el archivo **setup.exe** (o **setup.msi**) ubicado en el CD de distribución de la aplicación Kaspersky Administration Kit, en la carpeta **NetAgent**. El asistente facilita el proceso de instalación. El asistente le ofrecerá que configure los parámetros de instalación. Siga sus instrucciones.
2. Los primeros pasos del proceso de instalación son los habituales e implican la extracción de los archivos requeridos del paquete de distribución y su copia en el disco duro de su equipo, la aceptación del contrato de licencia y la recogida de información sobre el usuario y la compañía.
3. A continuación, debe definir la carpeta de instalación del Agente de Red. La carpeta de instalación predeterminada es **Archivos de programa\Kaspersky Lab\Agente de Red**. Si esta carpeta no existe, el programa la creará automáticamente. Para cambiar la carpeta, utilice el botón **Examinar...**
4. En la ventana del asistente (ver Figura 47. Configurar los parámetros utilizados para conectar con el Servidor de Administración), deberá configurar los parámetros utilizados por el Agente de Red para conectar con el Servidor de Administración. Con este fin, defina lo siguiente:
 - La Dirección del equipo donde está o estará instalado el Servidor de Administración. La dirección IP del equipo o su nombre en la red de Windows puede utilizarse como la dirección del equipo. De forma alternativa, puede seleccionar el equipo mediante el botón **Examinar**.
 - El número de puerto con el que el Agente de Red se conectará al Servidor de Administración. De manera predeterminada, se

utiliza el puerto **14000**. Si se ha asignado, puede cambiarlo. Únicamente se permite notación decimal.

- El número de puerto SSL que se utilizará para la conexión segura al Servidor de Administración usando el protocolo SSL. De forma predeterminada, se utiliza el puerto **13000**. Si se ha asignado, puede cambiarlo. Únicamente se permite notación decimal. Para asegurarse de que la conexión está utilizando un puerto seguro (mediante protocolo SSL), marque la casilla **Usar SSL para conectar con el servidor**.

Asistente para proyectos de instalación - Agente de red Kaspersky

Servidor de administración

Seleccionar el servidor de administración

Seleccione el equipo donde va a instalar Kaspersky Administration Server.

Dirección de servidor:

Permitir nombre de servicio NetBIOS en Anti-Hacker

Defina el puerto del servidor de administración. El valor debe estar entre 1-65535.

Puerto del servidor:

Puerto SSL servidor:

Usar SSL para conectar al servidor

< Atrás Siguiente > Cancelar

Figura 47. Configurar los parámetros utilizados para conectar con el Servidor de Administración

5. Si el Agente de Red se conecta al Servidor a través de un servidor Proxy (ver Figura 48. Configurar los parámetros de conexión a través de un servidor Proxy), configure los parámetros de conexión correspondientes:
 - Marque la casilla **Usar un servidor Proxy para conectar con el servidor del Administration Kit** e introduzca la dirección y el nombre del puerto para conectar con el servidor Proxy. Sólo se permite notación decimal (por ejemplo: Dirección Proxy: proxy.test.com; Puerto: 8080).
 - Si se utiliza una contraseña para acceder al servidor proxy, rellene los campos **Usuario Proxy** y **Contraseña proxy**.

- Si no se utiliza un servidor Proxy, salte este paso pulsando el botón **Siguiente**.



Figura 48. Configurar los parámetros de conexión a través de un servidor Proxy

6. A continuación, determine qué carpeta del grupo **Red** debe agregarse al equipo después de que sea detectado por el Servidor de Administración durante el sondeo de red de Windows. Seleccione una de las opciones siguientes: (ver Figura 49. Seleccionar el grupo en la carpeta **Red** para almacenar los equipos):
 - **Nombre de grupo predeterminado** – el equipo se agregará a la carpeta que corresponde con su posición en la red de Windows: dominio o grupo de trabajo (es la opción predeterminada).
 - **Definir el nombre del grupo** - el equipo se agregará a la carpeta especificada en el campo **Nombre del grupo**. Si selecciona esta opción, introduzca el nombre de la carpeta. Si esta carpeta no existe en el grupo **Red**, se creará (puede especificar el nombre de cualquier carpeta existente en el grupo **Red**).

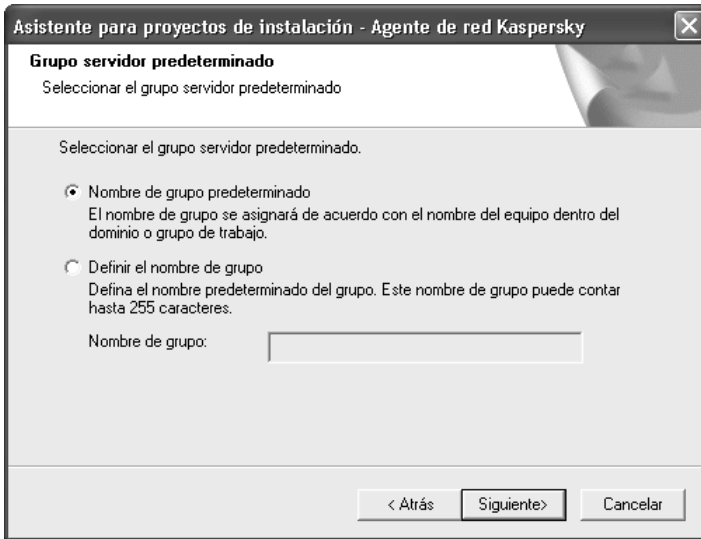


Figura 49. Seleccionar el grupo en la carpeta **Red** para almacenar los equipos

7. Durante la siguiente etapa (ver Figura 50. Seleccionar el método a utilizar para recibir el certificado del Servidor de Administración) tiene que especificar el método que quiere utilizar para recibir el certificado del Servidor de Administración al que se conectará el Agente de Red. Seleccione una de las opciones siguientes:

- **Certificado predeterminado** – El certificado del Servidor de Administración se recibirá cuando el Agente de Red se conecte a éste por primera vez (esta es la opción predeterminada);
- **Seleccionar el archivo de certificado** – La autenticación del Servidor de Administración se realizará en función del certificado especificado por el administrador. Si selecciona esta opción, especifique el archivo del certificado del Servidor de Administración a utilizar.

El archivo del certificado tiene la extensión **.cer** y está ubicado en la carpeta **Cert** de la carpeta de instalación de Kaspersky Administration Kit.

Puede copiar el archivo del certificado en la carpeta compartida o en un disco y usar una copia del archivo para instalar el Agente de Red.

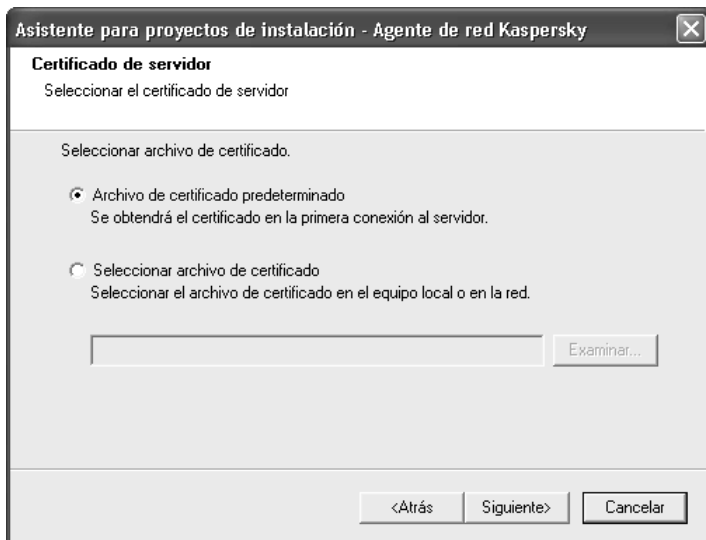


Figura 50. Seleccionar el método a utilizar para recibir el certificado del Servidor de Administración

8. En la última ventana del asistente (ver Figura 51. Configurar el inicio del Agente de Red), se le ofrecerá que ejecute el Agente de Red inmediatamente después de que se finalice el asistente. Si quiere ejecutarlo más tarde, desmarque la casilla **Iniciar el Agente de Red**, marcada por defecto.

Si está planeando usar el disco duro del equipo en el que está instalado el Agente de Red para crear una imagen de disco y distribuirla en otros equipos, debe desmarcar la casilla **Iniciar Agente de Red**.

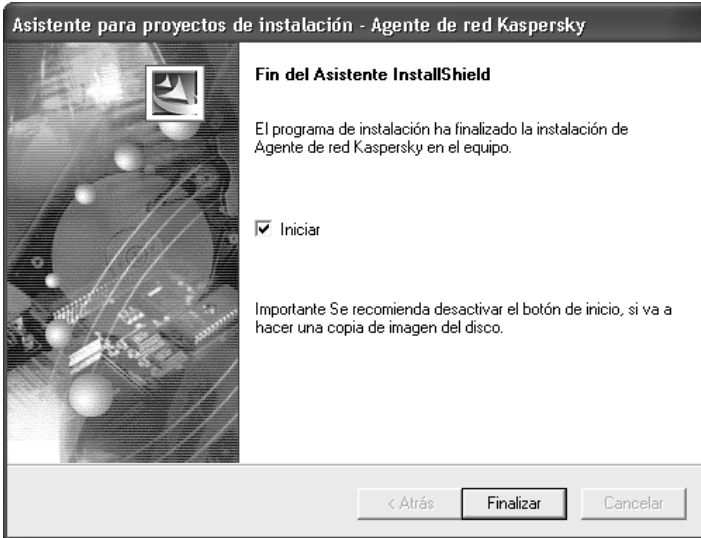


Figura 51. Configurar el inicio del Agente de Red

Después de que finalice el asistente, el Agente de Red se instalará en su equipo.

Puede revisar las propiedades del servicio **Kaspersky Network Agent** o controlar su funcionamiento mediante las herramientas de administración de Windows estándar **Administración de equipos** → **Servicios**.

4.3.2. Instalación local del complemento de administración de la aplicación

Para instalar el complemento de administración de la aplicación:

En el equipo en el que está instalada la Consola de Administración, ejecute el archivo ejecutable **klcfginst.exe**, ubicado en el CD de distribución de la aplicación. Este archivo se incluye en todas las aplicaciones que pueden administrarse a través de Kaspersky Administration Kit. El asistente facilita la instalación. Se le ofrecerá que configure los parámetros de instalación y que la inicie.

El archivo del complemento de administración del Agente de Red **klcfginst.exe** está ubicado en la carpeta **NetAgent** del paquete de distribución de Kaspersky Administration Kit.

4.3.3. Instalar aplicaciones en modo no interactivo

Para instalar una aplicación en modo no interactivo:

1. Cree el paquete de instalación requerido (ver sección 4.1.1xx), si el paquete de instalación de la instalación que quiere instalar no se ha creado.
2. Ejecutar el archivo ejecutable **setup.exe** con el modificador **/s** incluido en el paquete de distribución de la aplicación que está instalando, en el equipo en el que quiere instalar la aplicación usando un modo no interactivo.

Los paquetes de instalación se almacenan en el Servidor de Administración en la carpeta compartida especificada durante la etapa de instalación del Servidor de Administración, en la carpeta de servicio **Paquetes**.

APÉNDICE A. GLOSARIO

Esta Guía utiliza algunos términos específicos del campo de la protección antivirus. Este glosario sirve de diccionario, con definiciones de estos términos. Para mayor comodidad, el glosario se presenta en orden alfabético.

A

Actualización: Una función de Kaspersky Anti-Virus que actualiza/ agrega nuevos archivos (base antivirus o módulos de programa) recuperados de los servidores de actualización de Kaspersky Lab.

Actualizaciones disponibles: paquetes de revisión (Service Packs) con actualizaciones urgentes acumuladas durante un determinado periodo de tiempo y con las últimas modificaciones de la arquitectura de la aplicación.

Administración de una aplicación de forma centralizada: Administrar una aplicación a través de Kaspersky Administration Kit.

Administración local: Administración de una aplicación a través de una interfaz local.

Administrador de la red local: Un usuario que instala, configura y mantiene Kaspersky Administration Kit y que administra, de forma remota, las aplicaciones Kaspersky Lab instaladas en los equipos de la red lógica.

Agente de Red: Un componente de Kaspersky Administration Kit que proporciona comunicación entre el Servidor de Administración y las aplicaciones Kaspersky Lab instaladas en los nodos de red específicos (equipos o servidores). Este componente es habitual en todas las aplicaciones incluidas en Kaspersky Lab Business Optimal y Corporate Suite.

Agentes de actualización - equipos que actúan como centros intermediarios para la distribución de actualizaciones y de paquetes de instalación en los grupos de administración.

Almacenamiento de copia de seguridad: Una carpeta que contiene copias de datos del Servidor de Administración creada por la utilidad de copia de seguridad.

Análisis completo a petición: Un modo definido por el administrador que analiza todos los archivos de su equipo buscando virus y desinfecta/ elimina los objetos infectados en el momento de su detección.

Analizar archivos por extensión: En el modo de análisis, el programa considera la extensión del archivo analizado.

Analizar archivos por formato: En este modo de análisis, el programa analiza los contenidos de un archivo, particularmente el identificador de formato en el encabezamiento del archivo.

Aplicación de terceros - una aplicación antivirus de un proveedor externo o una aplicación de Kaspersky Lab que no soporta la administración a través de Kaspersky Administration Kit.

Aplicaciones, parámetros: Parámetros de aplicación específicos para todo tipo de tarea realizada por esta aplicación.

B

Base antivirus. Una base de datos creada por los especialistas de Kaspersky Lab que contiene una descripción detallada de todos los virus existentes hasta el momento, junto con los métodos de detección y desinfección utilizados. Las aplicaciones antivirus utilizan la base de datos para detectar y desinfectar virus con éxito. La base antivirus disponible en los sitios Web Kaspersky Lab se actualiza regularmente cuando aparecen nuevas amenazas de virus. Los usuarios registrados de las aplicaciones Kaspersky Lab tienen acceso a las actualizaciones de la base de datos. Para que su equipo esté constantemente protegido de virus, le recomendamos encarecidamente que descargue las actualizaciones de forma regular.

Bases de datos de correo electrónico: Bases de datos que almacenan los mensajes de correo electrónico en su equipo. Cada mensaje entrante/saliente se conserva en la base después de su recepción o envío. Estas bases de datos son analizadas en el modo de análisis a petición.

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

C

Carpeta de copia de seguridad: Un directorio que contiene las copias de seguridad u objetos desinfectados y eliminados.

Certificado del Servidor de Administración – Un certificado utilizado para autenticar el Servidor de Administración en la conexión de la Consola de Administración al servidor y en la transmisión de datos entre el servidor y los clientes. El certificado del Servidor de Administración se crea durante la instalación del Servidor de Administración. Se ubica en la carpeta **Cert** de la carpeta de instalación.

Clave de licencia actual: la clave de licencia instalada y utilizada actualmente para trabajar con la aplicación Kaspersky Lab. Esta clave determina el periodo de validez de la licencia y la directiva de licencia correspondiente al producto.

Clave de licencia de copia de seguridad: Una clave de licencia instalada, para una aplicación Kaspersky Lab, que no ha sido activada. En función de los parámetros, se activará la clave, de forma automática, con la expiración de la clave de licencia actual o de forma manual.

Clave de licencia: Un archivo con extensión **.key** que sirve de clave

personal. Este archivo es necesario para un funcionamiento correcto de las aplicaciones Kaspersky Lab. La clave de licencia viene incluida en el kit de distribución cuando adquiere su ejemplar de la aplicación en un distribuidor Kaspersky Lab. Si adquiere su producto en línea, recibirá su archivo de clave de licencia por correo electrónico. Sin la clave de licencia, Kaspersky Anti-Virus NO FUNCIONARÁ.

Complemento (gestión) de consola: Un componente especial que proporciona una interfaz para la administración remota de una aplicación a través de la Consola de Administración. Los complementos son específicos para cada aplicación y están incluidos en todas las aplicaciones Kaspersky Lab que pueden administrarse a través de Kaspersky Administration Kit.

Consola de administración: Componente de Kaspersky Administration Kit que proporciona una interfaz de usuario para los servicios de administración del Servidor de Administración y del Agente de Red.

Copia de seguridad: copia de datos del Servidor de Administración para el almacenamiento y restauración posterior llevada a cabo por la utilidad de copia de seguridad. La utilidad permite guardar:

- La base de datos del Servidor de Administración que almacena directivas, tareas, parámetros de aplicación y eventos registrados en el Servidor de Administración
- Información sobre las redes lógicas y configuraciones del cliente
- Instalación de archivos para la instalación remota de aplicaciones (contenidos de Paquetes, Desinstalación, Carpetas de actualizaciones)
- Certificado del Servidor de administración

Cuarentena: Un almacenamiento especial que aísla los objetos sospechosos e infectados.

D

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

Directiva de grupo: Un conjunto de parámetros de aplicación en un grupo de administración administrado a través de Kaspersky Administration Kit. Las directivas de grupo pueden ser diferentes para cada grupo. Las directivas de grupo son específicas para las aplicaciones individuales.

La directiva implica la configuración de todos los parámetros de las aplicaciones.

Directiva: ver Directiva de grupo

E

Eliminar un objeto: Un método de gestionar un objeto. Eliminar un objeto es eliminarlo físicamente de un equipo. Este método se recomienda para el tratamiento de objetos infectados. Si la eliminación es la primera acción que se aplica a un objeto, es necesario crear una copia de seguridad de este objeto antes de eliminarlo. Puede usar la copia de seguridad para restaurar el objeto original.

Equipo administrador – Un equipo en el que está instalada la Consola de Administración de Kaspersky Administration Kit. Usando la Consola, el administrador puede construir y administrar el sistema de protección antivirus en función de las aplicaciones Kaspersky Lab.

Estado de protección antivirus. El estado actual de la protección antivirus que caracteriza el nivel de seguridad de su equipo.

Exclusiones. Configuración personalizada que permite dejar algunos objetos fuera de la cobertura del análisis. Es posible personalizar las reglas de exclusión de la protección en tiempo real y del análisis a petición. De este modo, puede desactivar el análisis de los archivos comprimidos durante un análisis completo o excluir algunos archivos con máscaras.

G

Grupo de administración: Equipos agrupados de acuerdo con su funcionalidad y las aplicaciones Kaspersky Lab instaladas. El agrupamiento facilita considerablemente el proceso de gestión que permite que el administrador administre todos los equipos como una única entidad. Un grupo debe incluir otros grupos. Las directivas y las tareas de grupo pueden crearse para cada aplicación instalada en los miembros del grupo.

I

Instalación basada en scripts: Un método de instalación que relaciona la tarea de instalación remota con una cuenta de usuario especificada (varias cuentas). Cuando un usuario específico se conecta al dominio, la aplicación se instalará en el cliente, allí donde se ha conectado el usuario. Se recomienda este método para su uso con equipos con MS Windows 95/98/Me

Instalación de inserción: Un método de instalación remota que le permite instalar software Kaspersky Lab en los equipos especificados de su red lógica. Para realizar con éxito la tarea mediante una instalación de inserción, la cuenta utilizada para lanzar esta tarea debe tener permisos para ejecutar aplicaciones en clientes remotos. Este método es aconsejable para equipos con MS Windows NT/2000/2003/XP que

soportan esta funcionalidad o en equipos con MS Windows 98/Me en los que se haya instalado el Agente de Red.

Instalación Forzada: Un método de instalación remota que le permite instalar software Kaspersky Lab en los equipos especificados de su red lógica. Para realizar con éxito la tarea mediante una instalación forzada, la cuenta utilizada para lanzar esta tarea debe tener permisos para ejecutar aplicaciones en clientes remotos en los equipos cliente de la red lógica. Este método es aconsejable para instalar aplicaciones en equipos con Microsoft Windows NT/2000/2003/XP que soportan esta funcionalidad o en equipos con Microsoft Windows 98/Me en los que esté instalado el Agente de Red.

Instalación remota: Instalación de las aplicaciones Kaspersky Lab mediante los servicios proporcionados por Kaspersky Administration Kit.

Instalación utilizando el escenario de inicio: un método de instalación remota de aplicaciones Kaspersky Lab que permite asignar una tarea de instalación remota a una cuenta específica de un usuario (o varios usuarios). Cuando se registra un usuario en el dominio, se realiza un intento de instalación de la aplicación en el equipo cliente desde el que se registró el usuario. Se recomienda este método para la instalación de las aplicaciones Kaspersky Lab en equipos con Microsoft Windows 98/Me.

K

Kaspersky Administration Kit: Una aplicación para el control centralizado de las principales tareas administrativas. Proporciona un control completo de la directiva antivirus de la empresa basada en las aplicaciones Kaspersky Lab

N

Nivel de gravedad: Un parámetro que clasifica un evento registrado durante la ejecución de Kaspersky Anti-Virus. Existen cuatro niveles de gravedad:

- **Crítico**
- **Error**
- **Advertencia**
- **Información**

Los eventos del mismo tipo pueden tener diferentes niveles de gravedad, en función de la situación específica.

Nivel recomendado: El nivel de protección antivirus con los parámetros predeterminados recomendados por los expertos Kaspersky Lab que asegura la protección óptima de su equipo. Este nivel se establece por defecto.

O

- Objeto infectado:** Un objeto que contiene un virus. Le recomendamos dejar de trabajar con estos objetos para no arriesgar la infección de su equipo.
- Objeto OLE - :** Un objeto enlazado o integrado en otros archivos mediante el uso de tecnología OLE.
- Objeto sospechoso:** objeto que contiene código modificado de un virus conocido o que recuerda a un virus, pero no está actualmente fichado por los especialistas de Kaspersky Lab.
- Objetos de Inicio:** Un conjunto de programas necesarios para iniciar y mantener en funcionamiento el sistema operativo y otros programas instalados en su equipo. Su sistema operativo ejecuta estos objetos cada vez que arranca. Algunos virus infectan los objetos de inicio y pueden provocar un fallo de arranque.
- Operador de la red lógica:** Un usuario que controla el sistema de protección antivirus administrado por Kaspersky Administration Kit.

P

- Paquete de instalación:** Un paquete de archivos utilizado para instalar aplicaciones Kaspersky Lab en equipos remotos de una red lógica. Los paquetes de instalación se basan en un archivo especial **.kpd** incluido en el kit de distribución de la aplicación, que contiene un conjunto mínimo de parámetros, que proporciona la función básica de la aplicación, inmediatamente después de la instalación. Los valores de los parámetros son parámetros predeterminados de las aplicaciones.
- Periodo de licencia:** Un periodo durante el cual tiene derecho a utilizar la funcionalidad completa de Kaspersky Anti-Virus. El periodo de licencia viene definido por la clave de licencia y, como regla general, tiene una duración de un año a partir de la fecha de compra. Tras caducar la licencia, el producto seguirá funcionando pero no podrá actualizar la *base antivirus* ni los *módulos de aplicación*.
- Protección en tiempo real:** Un modo de análisis en el que la aplicación antivirus permanece residente en memoria. En el modo de protección en tiempo real, la aplicación analiza todos los objetos cuando los abre para su lectura, escritura o ejecución. Antes de permitir el acceso a un objeto, Kaspersky Anti-Virus lo analiza en busca de virus y, si se detecta uno, bloquea el acceso al objeto, lo desinfecta o lo elimina (en función de los parámetros definidos por el usuario).
- Protección máxima:** Un nivel de protección que asegura la protección completa pero que disminuye ligeramente las características de rendimiento.
- Puesta en cuarenta:** Un método de tratamiento de un objeto *sospechoso*. El acceso a este objeto está bloqueado y el archivo se mueve a la cuarentena para su procesamiento posterior.

R

Restauración: Restaurar los datos del Servidor de Administración usando una utilidad de copia de seguridad. La información a restaurar está disponible en el almacenamiento de copia de seguridad. La utilidad le permite restaurar:

- La base de datos del Servidor de Administración que almacena directivas, tareas, parámetros de aplicación y eventos registrados en el Servidor de Administración
- Información sobre las redes lógicas y configuraciones del cliente
- Archivos de Instalación para la instalación remota de aplicaciones (contenidos de los Paquetes, Desinstalación, Carpetas de actualizaciones)
- Certificado del Servidor de administración

S

Servidor de Administración, Cliente (o equipo cliente): un equipo, servidor o estación de trabajo en el que esté instalado el Agente de Red y administrado por aplicaciones Kaspersky Lab.

Servidor de administración: Un componente de Kaspersky Administration Kit que almacena información, de forma centralizada, sobre las aplicaciones Kaspersky Lab instaladas en los clientes y administra estas aplicaciones.

Servidores de actualizaciones Kaspersky Lab: Una lista de sitios Web Kaspersky Lab en la que puede copiar actualizaciones desde su equipo.

T

Tarea de grupo: Una tarea definida para su ejecución en todos los clientes en un grupo.

Tarea global: Una tarea definida para su ejecución en un determinado número de clientes de diferentes grupos de administración.

Tarea local: Una tarea creada para su ejecución en un único cliente.

Tarea, parámetros: Parámetros de aplicación específicos para cada tipo de tarea.

Tarea: Es una acción que tiene un nombre realizado por una aplicación Kaspersky Lab.

Tecnología IChecker: Tecnología que permite a la aplicación evitar volver a analizar objetos no modificados desde el análisis anterior. La tecnología IChecker se ha implementado mediante el uso una base de datos de sumas de control de objetos.

Tecnología iStreams™: Tecnología que permite excluir los archivos almacenados en sistemas de archivos NTFS que no han sido

modificados desde el último análisis. La tecnología IStreams ha sido implementada mediante un método de almacenamiento de sumas de control en flujos NTFS adicionales.

U

Umbral de actividad de virus: Número de virus detectados en un intervalo de tiempo específico. Cuando se excede el número, la situación se considera Foco de virus (ataque de virus). Este parámetro es importante para definir las epidemias de virus ya que la administración puede responder sin demora a las nuevas amenazas y adoptar las medidas de prevención para proteger su equipo.

Unidades virtuales (discos RAM): Una zona de memoria RAM de un ordenador personal que simula la presencia de un disco físico dentro del equipo.

V

Velocidad máxima: Un nivel de protección con la velocidad máxima de funcionamiento pero con un nivel de seguridad inferior.

Virus desconocido: virus nuevo que no aparece registrado en la *base antivirus*. En general, Kaspersky Anti-Virus detecta los virus desconocidos con el *analizador de código heurístico*: los objetos infectados por estos virus son marcados como *sospechosos*.

APÉNDICE B. KASPERSKY LAB

Fundado en 1997, Kaspersky Lab se ha convertido en un líder reconocido en tecnologías de seguridad de la información. Es fabricante de una amplia gama de productos software para la seguridad de los datos, y aporta soluciones completas de alto rendimiento para la protección de equipos y redes contra 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 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 ha sido diseñado para proporcionar protección antivirus a ordenadores personales con Microsoft Windows 98/ME o Microsoft Windows 2000/NT/XP contra todo tipo de virus conocidos, incluyendo software potencialmente peligroso. Kaspersky Anti-Virus Personal ofrece la supervisión de todos los posibles orígenes de intrusión de virus, como el correo electrónico, Internet, los CD, etc. Los virus desconocidos son detectados con eficacia y procesados mediante un sistema único de análisis de datos heurístico. Esta aplicación puede trabajar en los siguientes modos (que pueden ser utilizados de forma separada o conjunta):

- **Protección del equipo en tiempo real:** análisis antivirus de todos los objetos que son ejecutados, abiertos o guardados en el equipo del usuario.
- **Análisis a petición:** análisis y desinfección del equipo completo o de discos, archivos o carpetas seleccionados. Puede iniciar este análisis manualmente o configurar un análisis automático, de acuerdo con una planificación.

Kaspersky Anti-Virus Personal no analiza los objetos previamente 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 **incrementa considerablemente la velocidad de funcionamiento de la aplicación.**

Kaspersky Anti-Virus Personal ofrece una protección segura contra los virus que intentan penetrar en los equipos por medio de correos electrónicos. Kaspersky Anti-Virus® Personal realiza el análisis automático y desinfección de todos los mensajes de correo entrantes y salientes enviados o recibidos por los protocolos POP3 y SMTP y proporciona una gran eficiencia en la detección de virus en las bases de datos de correo.

La aplicación reconoce más de 700 formatos de archivos comprimidos y datos archivados, analiza automáticamente su contenido y elimina el código dañino de archivos **ZIP, CAB, RAR, ARJ, LHA e ICE.**

La configuración de la aplicación se realiza de forma simple e intuitiva gracias a la posibilidad de seleccionar alguno de los siguientes niveles de protección preestablecidos: **Máxima protección**, **Recomendado** y **Máxima velocidad**.

La base antivirus se actualiza cada tres horas, y la entrega de la base de datos a su equipo 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 Microsoft Windows 98/ME/2000/NT/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. Kaspersky Anti-Virus Personal incorpora muchas mejoras en la interfaz, haciendo más fácil que nunca la utilización del programa.

Kaspersky Anti-Virus® Personal Pro tiene las siguientes características:

- **Análisis a petición** de discos locales;
- **Protección en tiempo real automática** de todos los archivos a los que se accede.
- **Filtro de correo**: analiza y desinfecta automáticamente todo el correo entrante y saliente que utiliza los protocolos POP3 y SMTP y detecta eficazmente los virus en las bases de datos de correo;
- **Bloqueador de comportamiento** que proporciona la máxima protección contra virus en las aplicaciones MS Office.
- **Análisis de archivos** – Kaspersky Anti-Virus reconoce alrededor de 700 formatos de archivos comprimidos y datos archivados, y se hace cargo automáticamente del análisis del contenido y eliminación de código dañino en archivos con formato **ZIP, CAB, RAR, ARJ, LHA e ICE**.

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 desde Internet o desde la red local.

Kaspersky Anti-Hacker monitoriza la actividad de red TCP/IP de todas las aplicaciones de su equipo. Cuando detecta cualquier acción sospechosa, la aplicación bloquea el acceso a la red de la aplicación sospechosa. Esto asegura una privacidad mejorada y una seguridad del 100% en 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 la Web. La aplicación ofrece toda la transparencia y facilidad de acceso a la información.

Kaspersky Anti-Hacker bloquea los ataques maliciosos más frecuentes y controla los intentos de analizar los puertos de su equipo.

La configuración de la aplicación se reduce a elegir entre uno de los cinco niveles de seguridad. De forma predeterminada, la aplicación se inicia en modo de auto-aprendizaje, el cual 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® Personal Security Suite es un programa diseñado para la completa organización de la protección de ordenadores personales con Microsoft Windows. La suite evita que los programas peligrosos y potencialmente maliciosos penetren a través de algún origen de datos y le protege de los intentos de acceso no autorizados a los datos de su equipo, al igual que bloquea el correo no deseado (spam).

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 de los correos electrónicos no deseados (spam);
- Protección de su equipo de accesos no autorizados así como de los ataques de hackers desde su red local o desde Internet.

Este programa es un servicio gratuito disponible para los visitantes del sitio Web corporativo para realizar análisis eficientes 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 relacionada con la infección con un software malicioso. Durante el análisis, el usuario puede:

- Excluir archivos y bases de datos de correo del análisis.
- Seleccionar una base antivirus estándar o extendida para su uso en el análisis.
- Guardar informes con el resultado del análisis en formato txt y html.

Este programa es un servicio de suscripción disponible para los visitantes del sitio Web corporativo 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 análisis.
- Seleccionar una base antivirus estándar o extendida para su uso en 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.

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 Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation y Linux;
 - *Servidores de archivos y aplicaciones* con Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server,
-

Microsoft 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 2000 Standard Edition.

El kit de distribución de Kaspersky Anti-Virus Business Optimal 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.

Este paquete proporciona una protección antivirus escalable y completa de redes corporativas de cualquier tamaño y complejidad. El paquete de componentes ha sido desarrollado para todos los niveles de una red corporativa, incluso en entornos de equipos mixtos. Kaspersky Corporate Suite es compatible con la mayoría de los sistemas operativos y aplicaciones instalados en una empresa. Todos los componentes del paquete se administran desde una consola con una interfaz de usuario unificada. Kaspersky Corporate Suite ofrece un sistema de protección seguro y de alto rendimiento que además es totalmente compatible con las necesidades específicas de su configuración de red.

Kaspersky Corporate Suite le ofrece protección antivirus completa para:

- *Estaciones de trabajo* con Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstations y Linux;
- *Servidores de archivos y aplicaciones* con Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/ Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux y Samba Servers;
- *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 Microsoft 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 listas negras 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 transmitido 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 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 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 http://www.kaspersky.com/supportinter.html
Información general	WWW http://www.kaspersky.com http://www.viruslist.com Correo electrónico: sales@kaspersky.com