INFORME SOBRE: Lineamientos y procedimientos a seguir para la actualización del licenciamiento y la instalación y/o actualización de la Solución Antivirus Corporativo de ESET NOD32 a la nueva versión File Security para Servidores (versión 4.5) y ESET Endpoint Antivirus para Estaciones de Trabajo y/o Laptops (Versión 5.0.2126.6).

FECHA: 11 de Marzo de 2013

ELABORADO POR: Ing. Dubraska Peña.

OBJETIVO: Especificar los lineamientos y procedimientos a seguir por los administradores de redes para la actualización del licenciamiento y la instalación y/o actualización de la Solución Antivirus Corporativo de ESET NOD32 en Facultades, Dependencias Centrales y extramuros de la Universidad Central de Venezuela (UCV) a la nueva versión File Security para Servidores (versión 4.5) y ESET Endpoint Antivirus para Estaciones de Trabajo y/o Laptops (Versión 5.0.2126.6).

DESCRIPCIÓN:

En el marco del Proyecto de Antivirus Corporativo, liderado por la DTIC, se ha elaborado el presente documento con la finalidad de brindar a los administradores de las distintas Facultades, Dependencias Centrales y Extramuros de la UCV, la información referente a los lineamientos y procedimientos a seguir para la instalación y/o actualización de la solución de Antivirus Corporativo de ESET en las distintas Facultades, Dependencias Centrales y Extramuros.

La nueva versión de la solución de Antivirus ESET se conoce como File Security para Servidores y ESET Endpoint Antivirus para Estaciones de Trabajo y/o Laptops.

Alcance:

Está orientado a todos los administradores de las Facultades, Dependencias Centrales y Extramuros de la UCV que tienen bajo su responsabilidad la instalación, actualización y administración de la solución de Antivirus Corporativo en sus respectivas localidades.

Lineamientos:

- La solución de Antivirus Corporativo para toda la UCV mantiene su estructura jerárquica con el fin de agrupar en una consola centralizada la información de todas las estaciones de trabajo y servidores que contempla la solución en las Facultades, Dependencias Centrales y Extramuros.
  El servidor central ubicado en el Rectorado consolida el proceso de monitoreo y permite detectar cualquier eventualidad para su inmediata notificación al administrador responsable.

    - ***Actualización:*** es el proceso de la transferencia de las bases de firmas de virus al cliente instalado en el servidor, estación de trabajo y/o laptops.
    - ***Replicación:*** es el proceso de transferencia de la información concerniente al estado de las estaciones de trabajo, servidores y/o laptops que posee la solución de Antivirus Corporativo.

- El archivo de configuración (.XML) para la solución de antivirus en la Facultad o Dependencia Central tanto para estaciones de trabajo como para los servidores, debe establecer los siguientes parámetros como base:
    - ***Servidor de actualización***: es el servidor de Antivirus dedicado a las actualizaciones de la solución Antivirus de la Facultad, Dependencia Central o Extramuros.
    - ***Servidor de Administración Remota***: es el servidor Antivirus dedicado a la administración de la solución Antivirus de la Facultad, Dependencia Central o Extramuros.
    - ***Proteger parámetros de configuración***: permite crear una clave de acceso para evitar que los usuarios finales puedan realizar modificación o desinstalar la solución de antivirus residentes en las estaciones de trabajo, laptops y servidores.
    - ***Tareas programadas***: permite crear una limpieza de rutina para realizar un escaneo de los archivos contenidos en los dispositivos de almacenamiento.

Procedimientos:

El procedimiento de instalación y/o actualización de la solución de Antivirus comprende la instalación de las siguientes herramientas:

- ESET Remote Administrator Server (ERAS).
- ESET Remote Administrator Console (ERAC).
- ESET File Security (Servidores).
    - Configuración de otras herramientas (archivos de configuración (.XML), cargado de archivos de licencias (.LIC), excepciones en el Firewall de Windows, tareas programadas, entre otros).
- ESET Endpoint Antivirus (Estaciones de Trabajo y/o Laptops).
- Manejador de Base de Datos MySQL Server (No es necesario su instalación para el proceso de actualización de la solución Antivirus).
- MySQL Connector ODBC. (No es necesario su instalación para el proceso de actualización de la solución Antivirus).

A continuación se detallan los pasos de instalación de cada una de las herramientas indicadas anteriormente:

INSTALANDO ESET REMOTE ADMINISTRATOR SERVER (ERAS)

1. Para comenzar la instalación, haga doble clic en el ícono del archivo instalador (***era_server_nt323_esn***) que guardó previamente en el equipo. Si Windows le solicita Abrir/Ejecutar el archivo, **presione Abrir/Ejecutar**.

Fig. 1-1

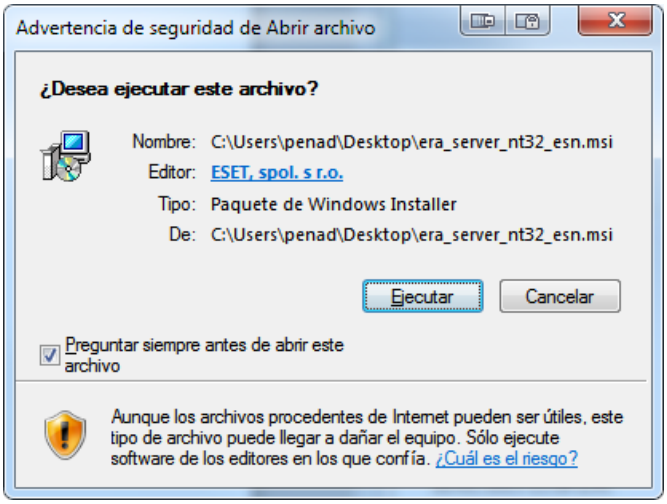

Fig. 1-2

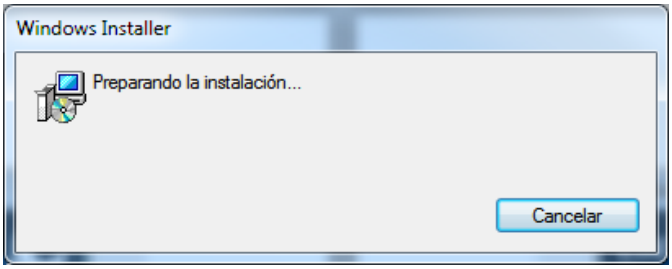

Fig. 1-3

2. En la siguiente ventana aparecerá el ***Asistente de instalación de ESET Remote Administrator Server 5.0.242.0***. .Luego presionar el botón Siguiente.

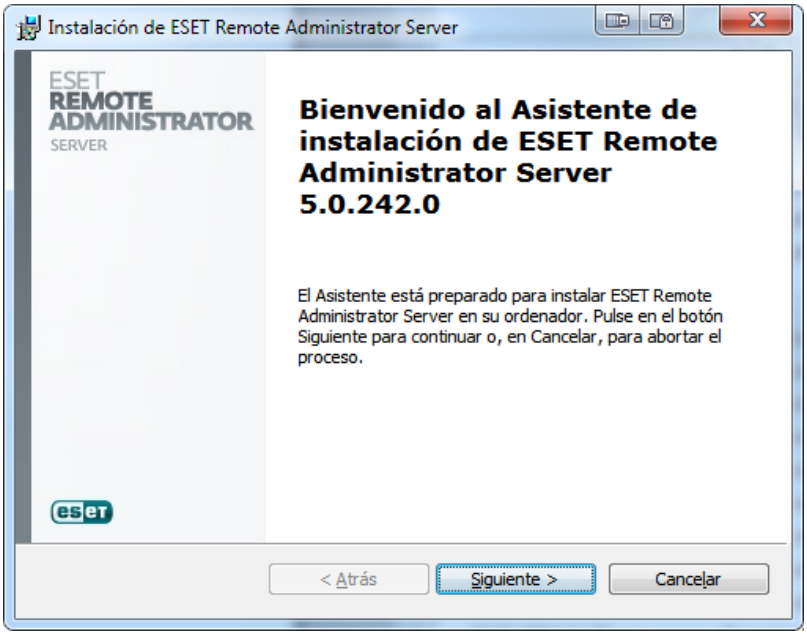

Fig. 1-4

3. En la ventana Acuerdo de licencia para el usuario final, seleccionar la opción ***Acepto las condiciones del Acuerdo de licencia***. Luego presionar el botón Siguiente.

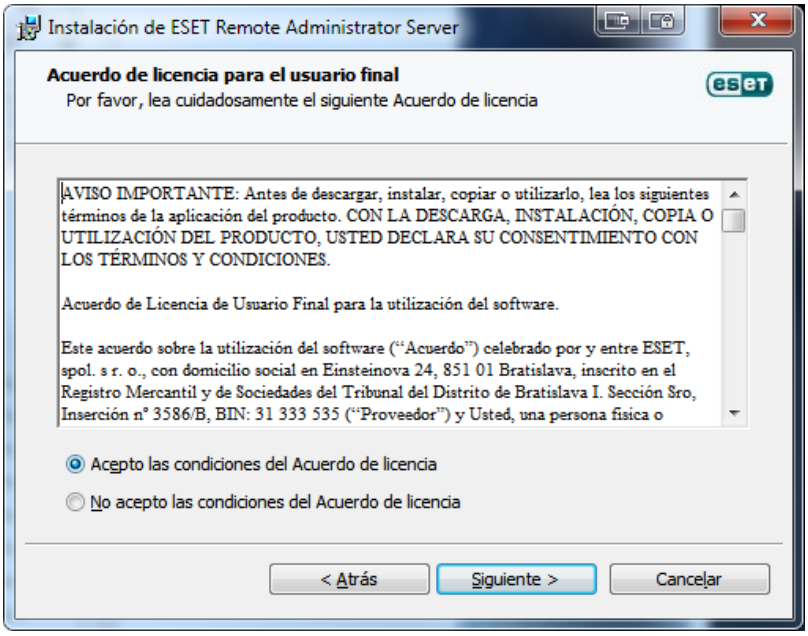

Fig. 1-5

4. En la ventana Seleccionar el tipo de instalación, tildar las opciones ***ESET Remote Administrator Server*** y ***Servidor de la consola HTTP de ESET***, luego seleccionar la opción ***Avanzada (instalación completa personalizada).*** Presionar el botón Siguiente.

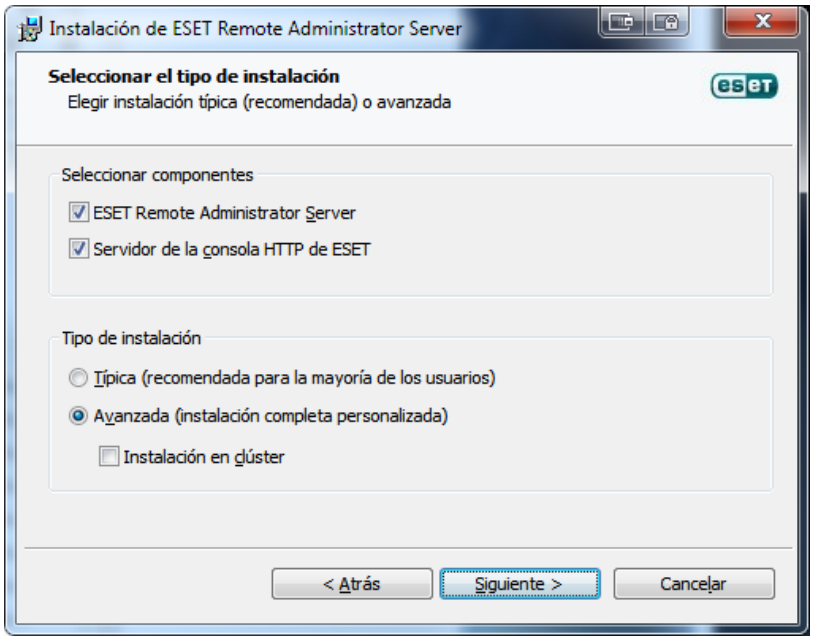

Fig. 1-6

5. En la ventana Clave de licencia, presionar el botón ***Examinar…*** y ubicar la carpeta donde se encuentra almacenado el archivo de licenciamiento (.lic)…

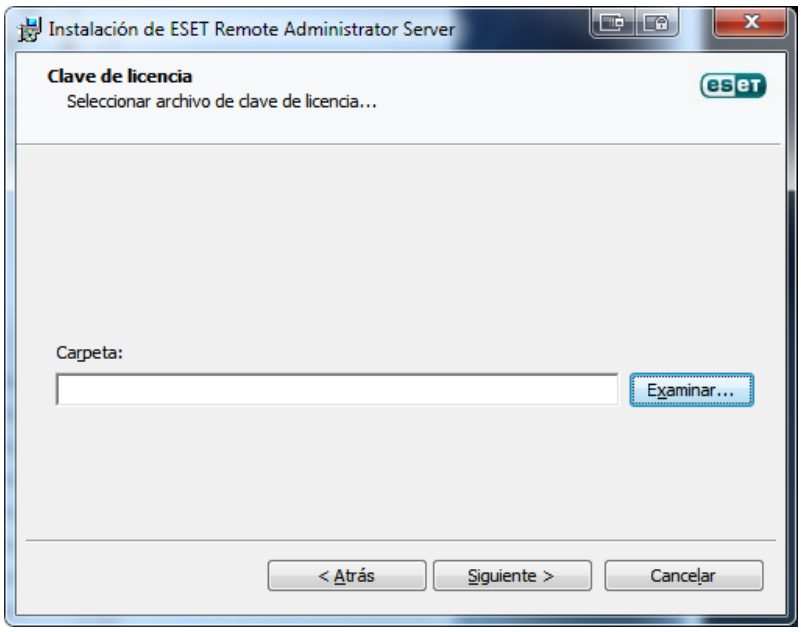

Fig. 1-7

6. En la siguiente ventana, ubicar la carpeta donde se encuentra almacenado el ***Archivo .lic (EAV-XXXXXXXX)***, seleccionar y presionar el botón Abrir.

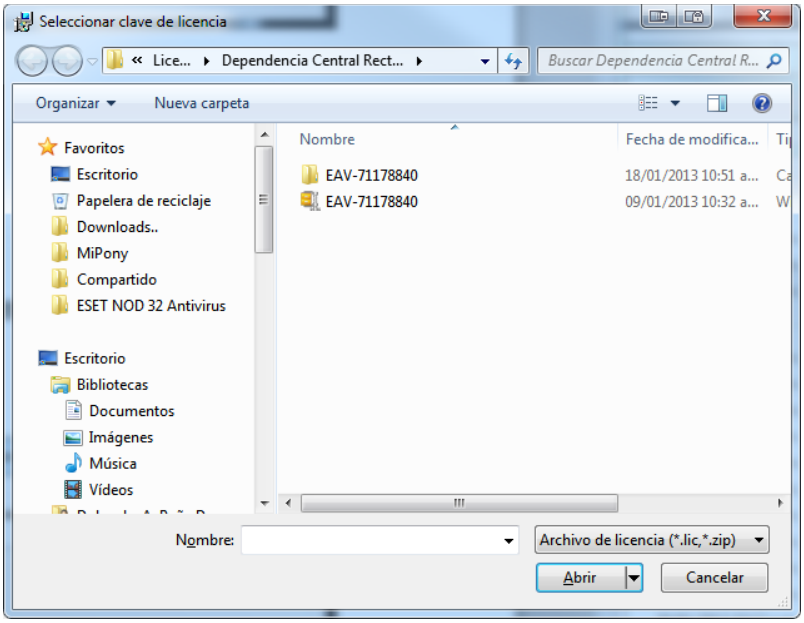

Fig. 1-8

7. Una vez ubicado y seleccionado el archivo, se debe volver a la ventana Clave de licencia, donde se mostrará información del archivo seleccionado como ***Producto, Cliente, Fecha de Expiración y la ruta de ubicación de la carpeta contenedora del Archivo .lic (EAV-XXXXXXXX).*** Luego presionar el botón Siguiente.

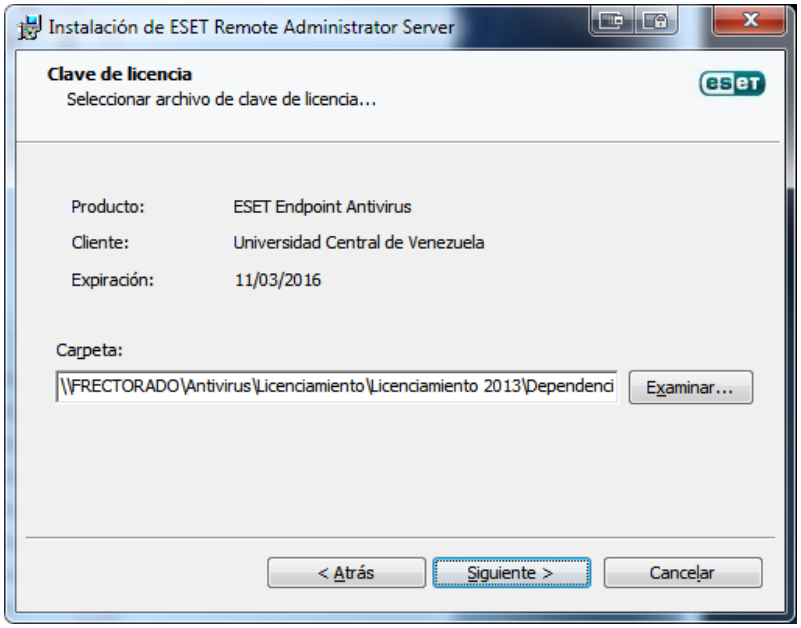

Fig. 1-9

8. En la ventana Carpeta de instalación, se mostrará ***la ruta de la carpeta donde será instalado el ESET Remote Administrator Server (ERAS)***. Luego presionar el botón Siguiente.

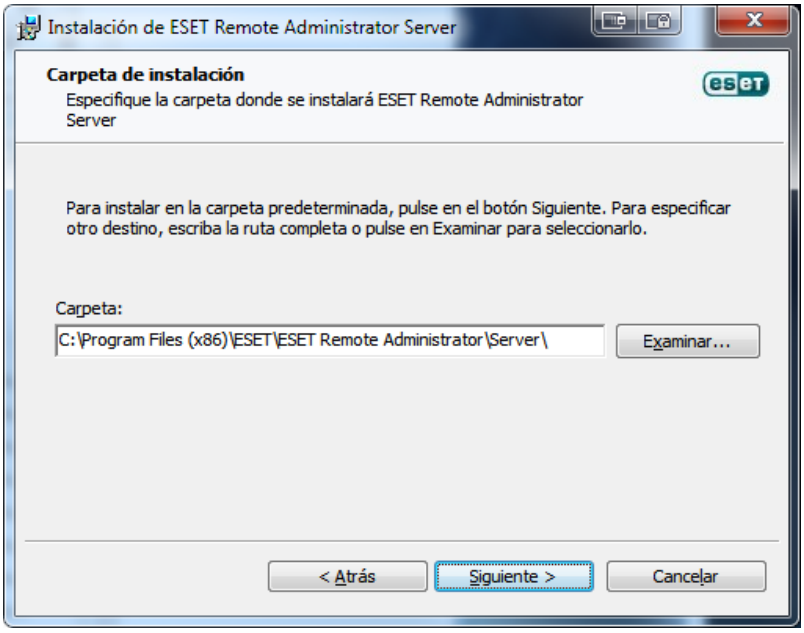

Fig. 1-10

9. En la ventana Cuenta de servicio, seleccionar la opción ***Cuenta del sistema local.*** Luego presionar el botón Siguiente.

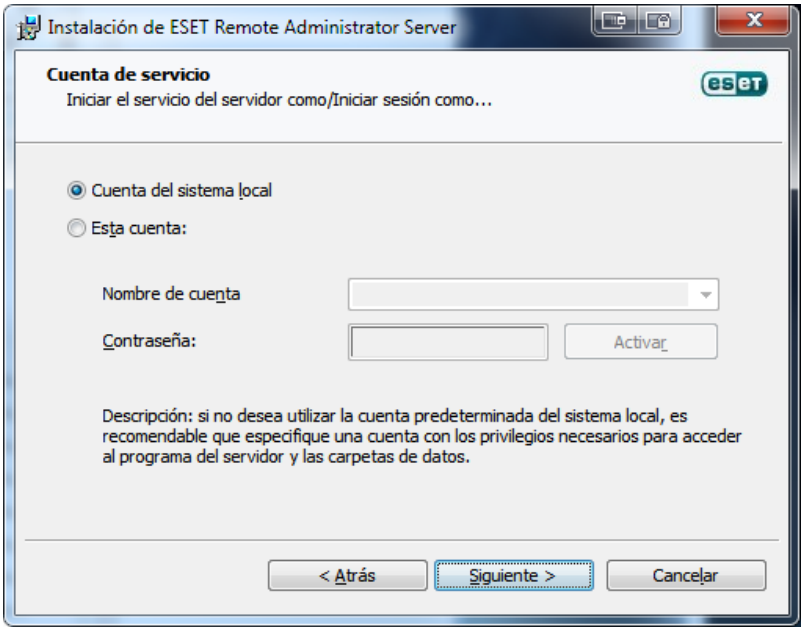

Fig. 1-11

10. En la ventana Base de datos, la selección de la opción dependerá del número de estaciones de trabajo que va a manejar el servidor, es decir, si el número es ***menor a Quinientos (500) clientes***, se debe seleccionar la opción ***MS Access (integrado).*** Luego presionar el botón Siguiente.

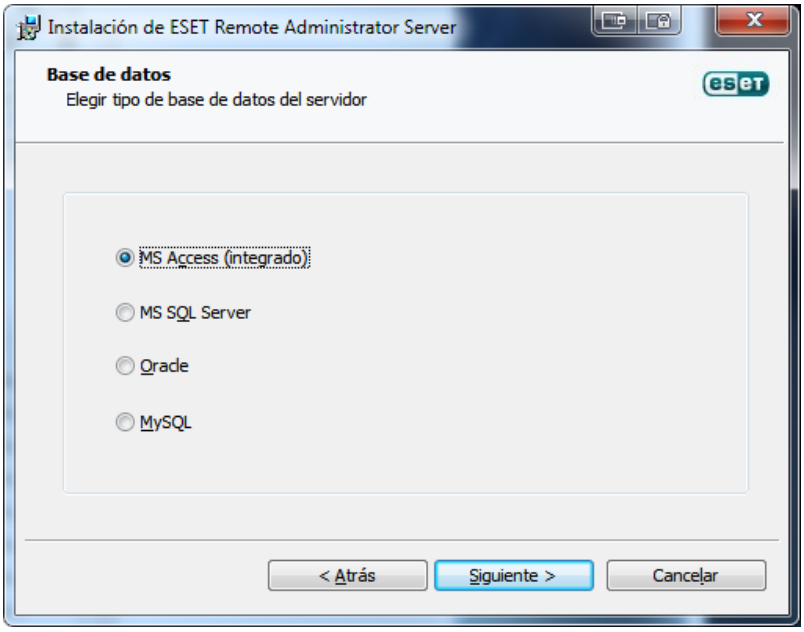

Fig. 1-12

<u>NOTA</u>: Si selecciona la opción MS Access (integrado), se debe ir directamente al paso número 13 del instructivo, de lo contrario continuar sin hacer ningún salto de pasos.

11. En la ventana Base de datos, la selección de la opción dependerá del número de clientes que va a manejar el servidor, es decir, si el número es ***mayor o igual a Quinientos (500) clientes***, se debe seleccionar la opción ***MySQL.*** Luego presionar el botón Siguiente.

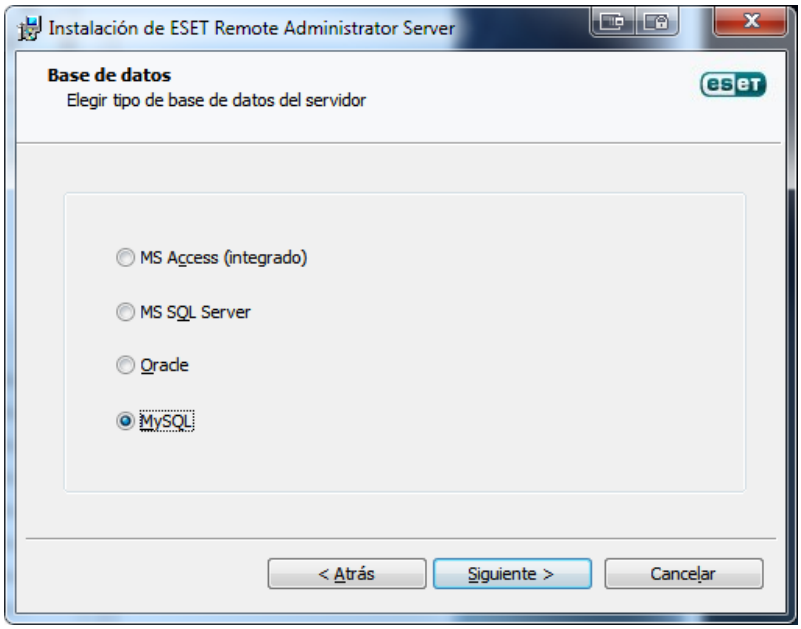

Fig. 1-13

12. En la ventana Servidor de base de datos My SQL, se debe ***modificar*** la ***Cadena de conexión:…***

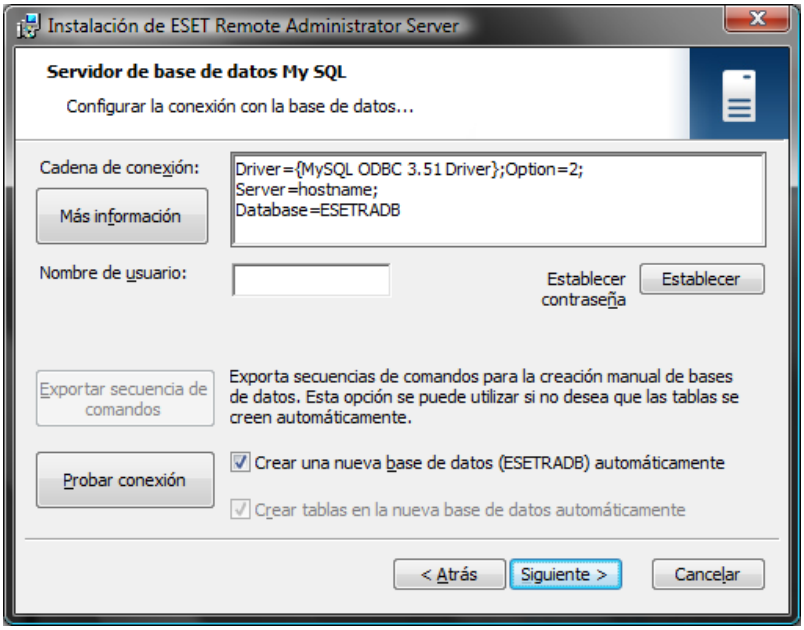

Fig. 1-14

Por defecto, los parámetros de la cadena de conexión son:

- ***Driver={MySQL ODBC 3.51 Driver};Option=2;***
- ***Server=hostname;***
- ***Database=ESETRAD***

Modificar los parámetros de la cadena de conexión por…

- ***Driver={MySQL ODBC 5.1 Driver};Option=2;***
- ***Server=localhost;***
- ***Database=ESETRADB***

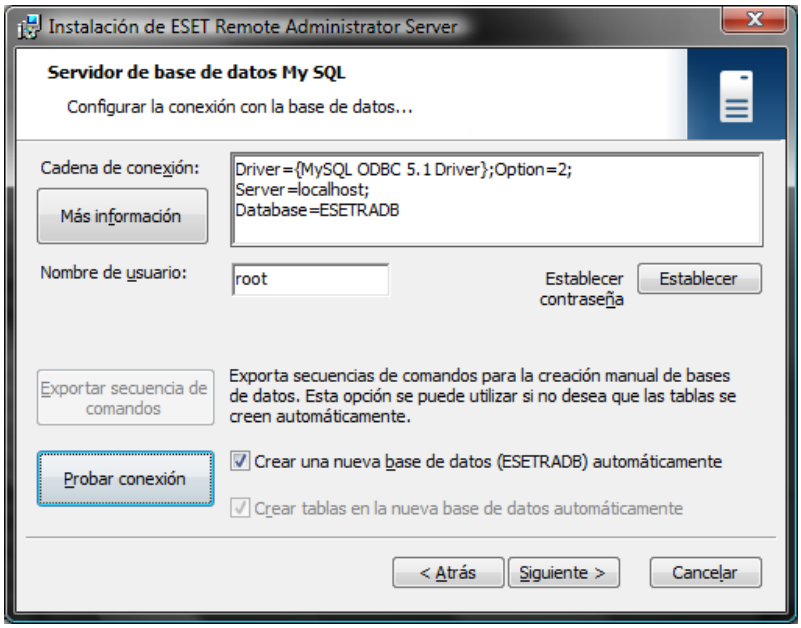

Fig. 1-15

NOTA: de ser necesario se deben colocar los parámetros de Nombre de usuario y contraseña para el usuario root de MySQL.

Luego presionar el botón ***Probar conexión.***

Se mostrará la ventana que indica que ***la prueba de conexión finalizó correctamente.*** Luego presionar el botón Aceptar.

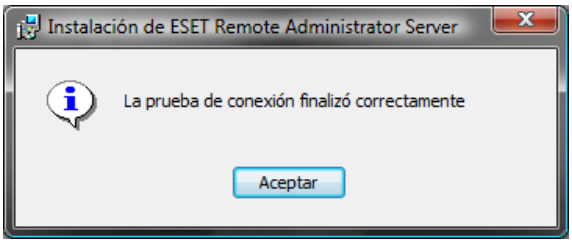

Fig. 1-16

13. En la ventana Carpeta de datos, se muestran las ***rutas de las carpetas para la base de datos y el almacenamiento***, no se realiza ninguna modificación. Luego presionar el botón Siguiente.

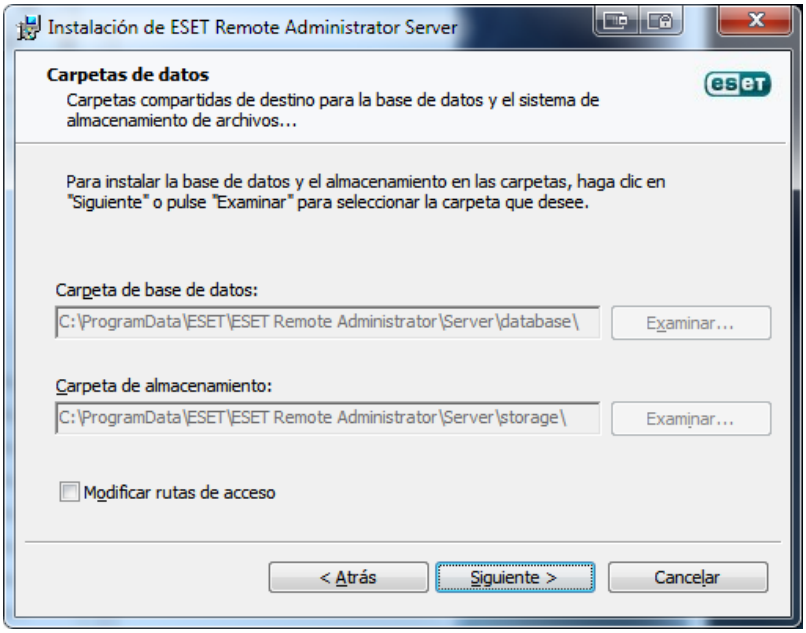

Fig. 1-17

14. En la ventana Nombre del servidor y puertos, ***se establecen por defecto los puertos y nombre del servidor***. Luego presionar el botón Siguiente.

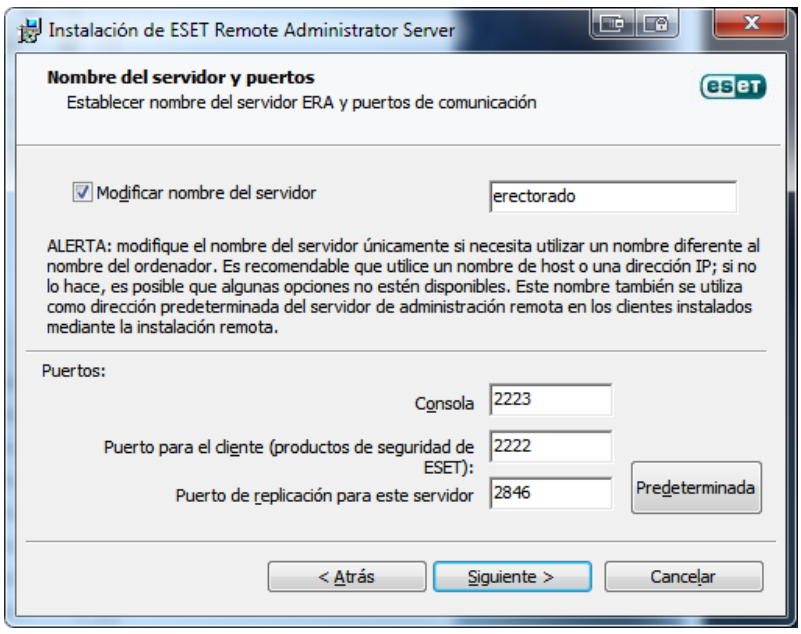

Fig. 1-18

15. En la ventana Configuración de seguridad, ***no se realizará ningún cambio, la definición de las contraseñas del servidor se realizará posteriormente***. Luego presionar el botón Siguiente.

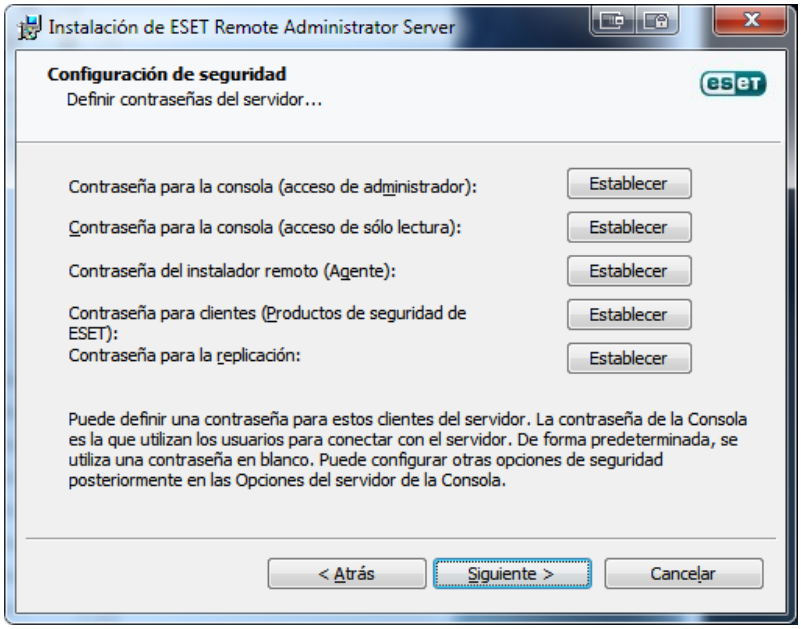

Fig. 1-19

16. En la ventana Actualizaciones, tildar la opción ***Establecer parámetros de actualización más tarde***. Luego presionar el botón Siguiente.

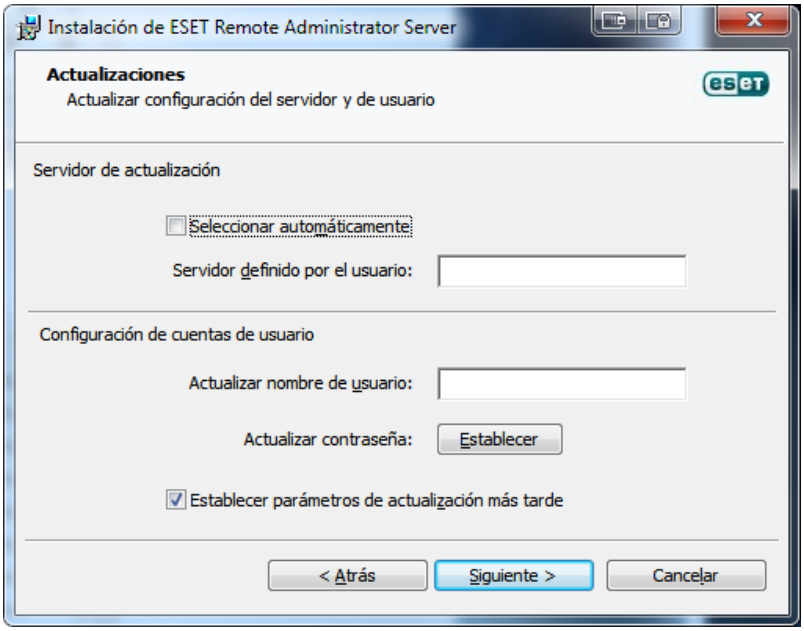

Fig. 1-20

17. En la ventana Configuración SMTP, ***no se realizará ninguna modificación***. Luego presionar el botón Siguiente.

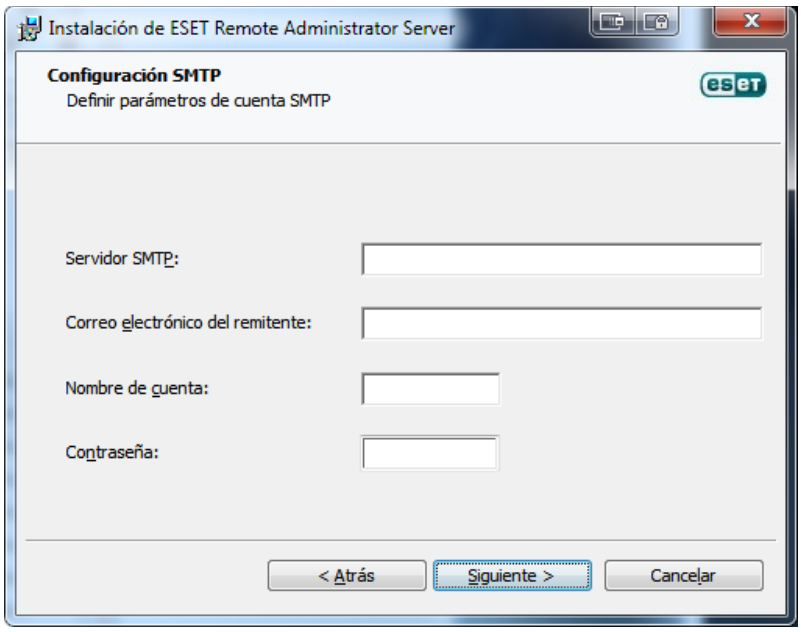

Fig. 1-21

18. En la ventana puertos y certificados del servidor HTTP, en ***Certificados de servidor HTTP***, se tilda la opción ***Utilizar certificados autofirmados generados automáticamente,*** en ***Protocolo de servidor HTTP,*** se selecciona ***HTTPS.*** Luego Presionar el botón ***Probar puertos de servidor***.

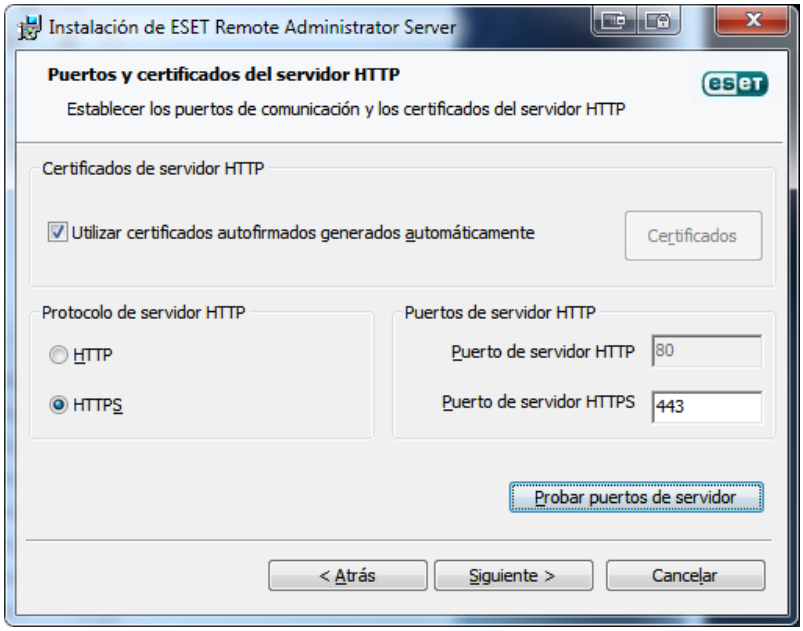

Fig. 1-22

Verificar que, ***El puerto de servidor seleccionado está disponible. De lo contrario se deberá seleccionar otro puerto y realizar la prueba nuevamente.*** Luego presionar el botón Aceptar.

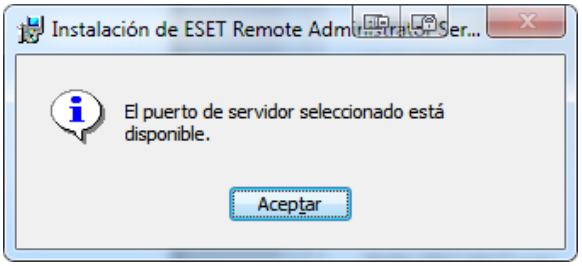

Fig. 1-23

19. En la ventana Configuración de registro, ***no se realiza ninguna modificación***. Luego presionar el botón Siguiente.

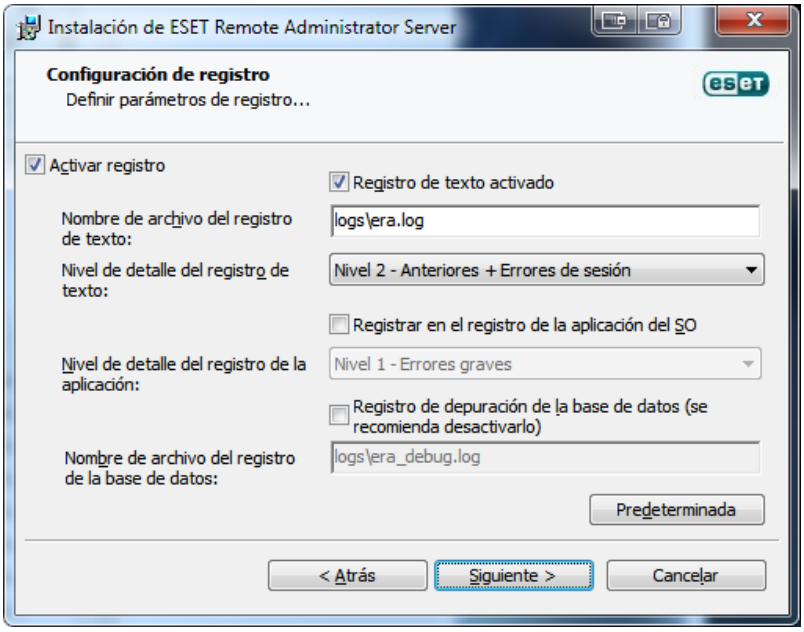

Fig. 1-24

20. En la ventana Preparado para instalar, presione el botón ***Instalar*** para comenzar la instalación de ESET Remote Administrator Server (ERAS).

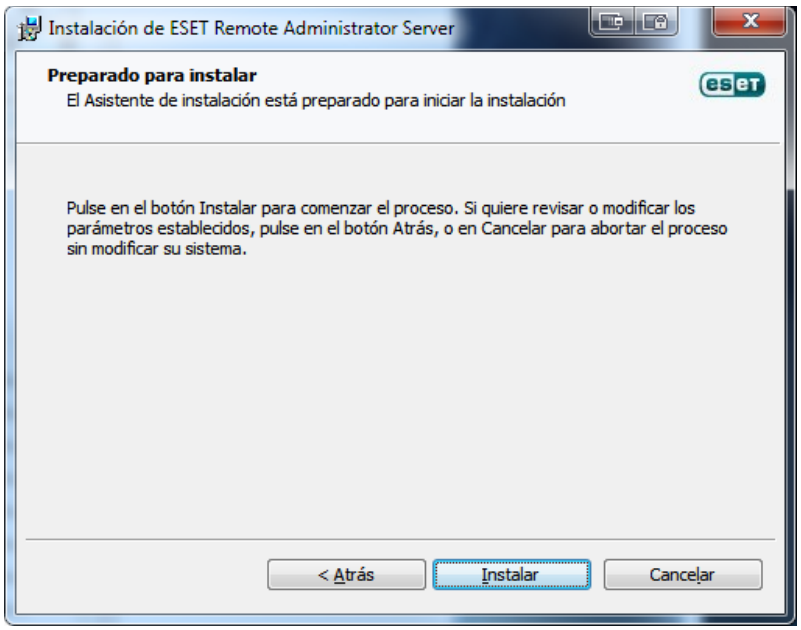

Fig. 1-25

21. Ventana Instalando ESET Remote Administrator Server (ERAS). Esperar que finalice el proceso de instalación.

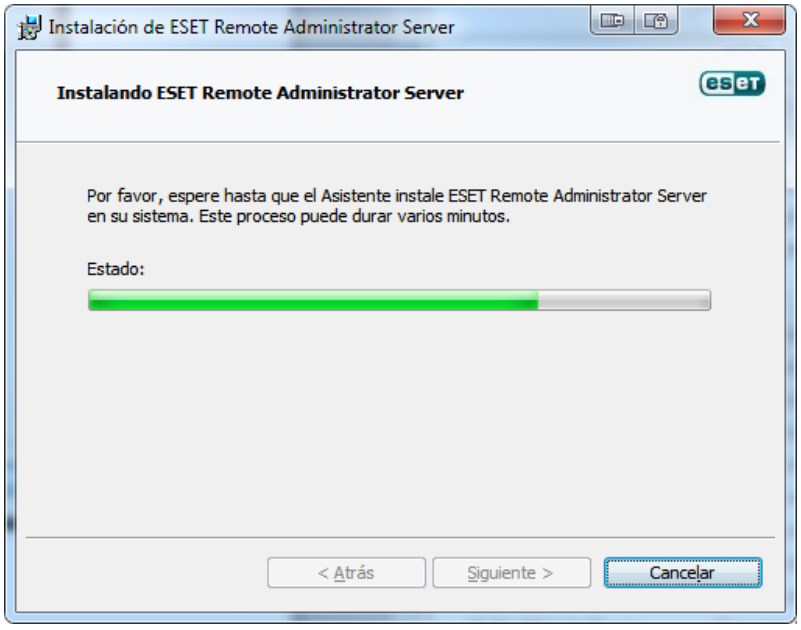

Fig. 1-26

22. Cuando se visualice la ventana Completando el Asistente de instalación de ESET Remote Administrator Server (ERAS), presionar el botón Finalizar.

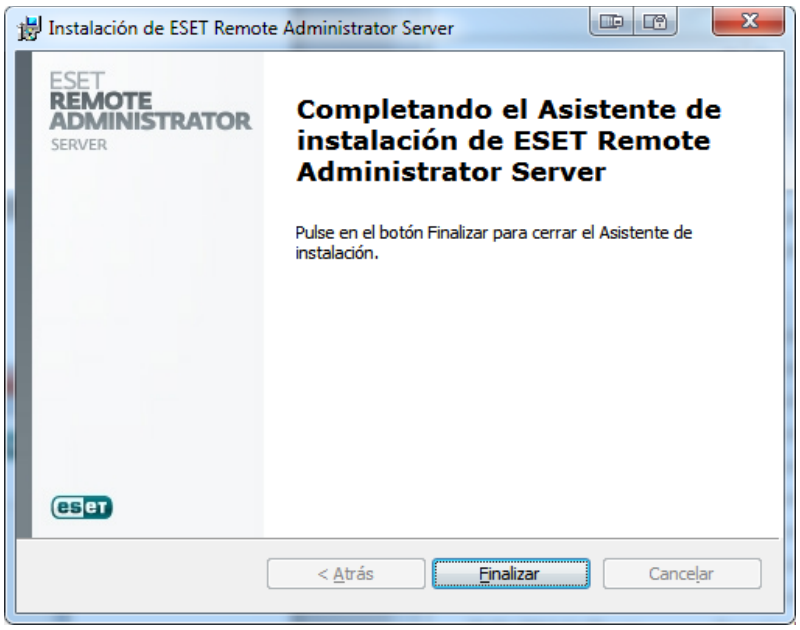

Fig. 1-27

INSTALANDO ESET REMOTE ADMINISTRATOR CONSOLE (ERAC)

1. Para comenzar la instalación, haga doble clic en el ícono del archivo instalador (***era_cosole_nt323_esn***) que guardó previamente en el equipo. Si Windows le solicita Abrir/Ejecutar el archivo, presione Abrir/Ejecutar.

Fig. 1-1

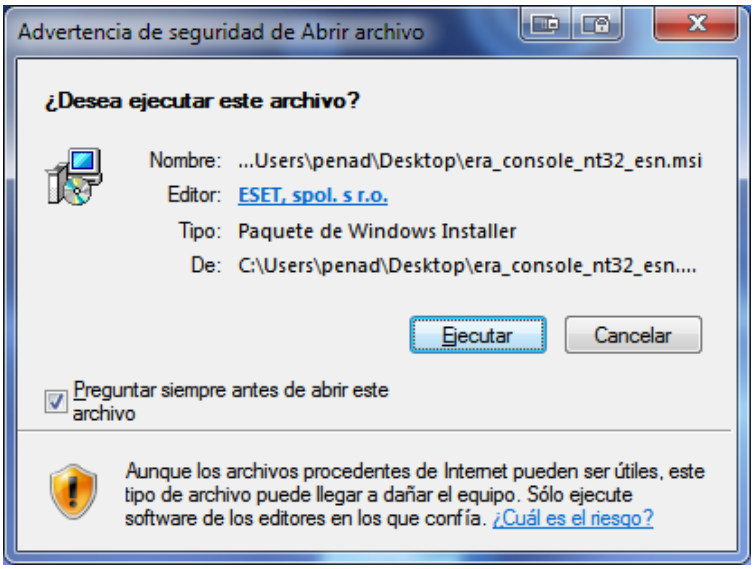

Fig. 1-2

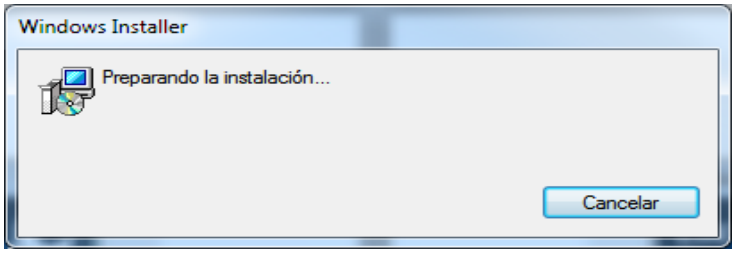

Fig. 1-3

2. En la siguiente ventana aparecerá ***el Asistente de instalación de ESET Remote Administrator Console 5.0.242.0***. Luego presione el botón Siguiente.

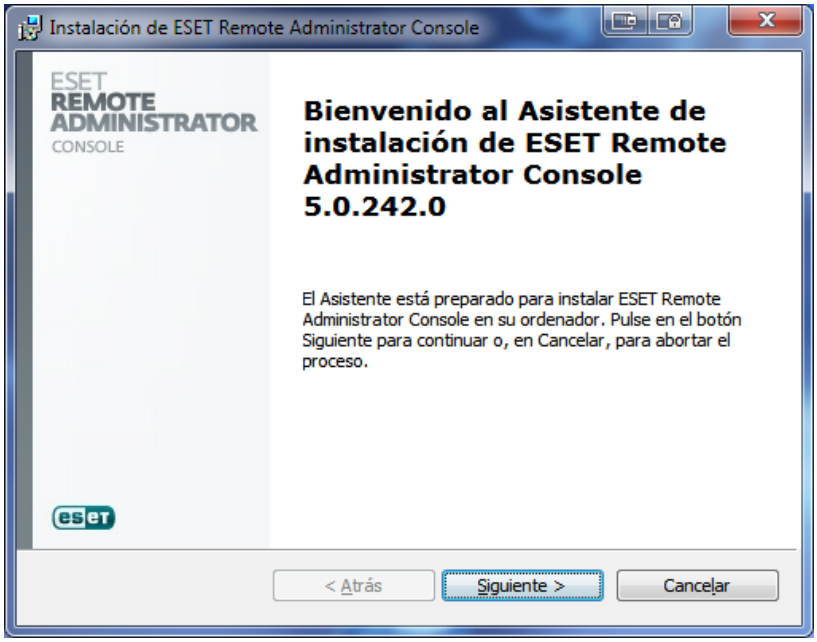

Fig. 1-4

3. En la ventana Acuerdo de licencia para el usuario final, seleccionar la opción ***Acepto las condiciones del Acuerdo de licencia***. Luego presione el botón Siguiente.

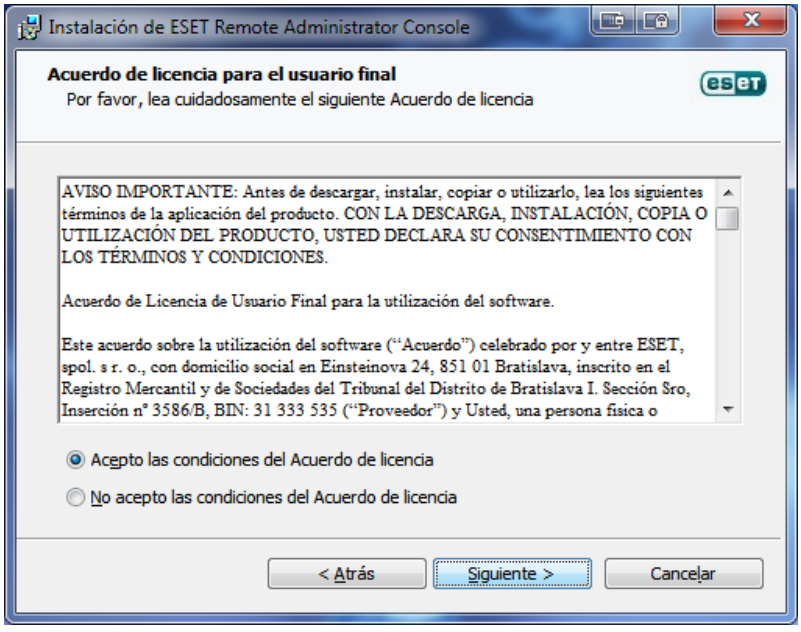

Fig. 1-5

4. En la ventana Seleccionar el tipo de instalación, seleccionar la opción ***Típica (recomendada para la mayoría de los usuarios)***. Luego presionar el botón Siguiente.

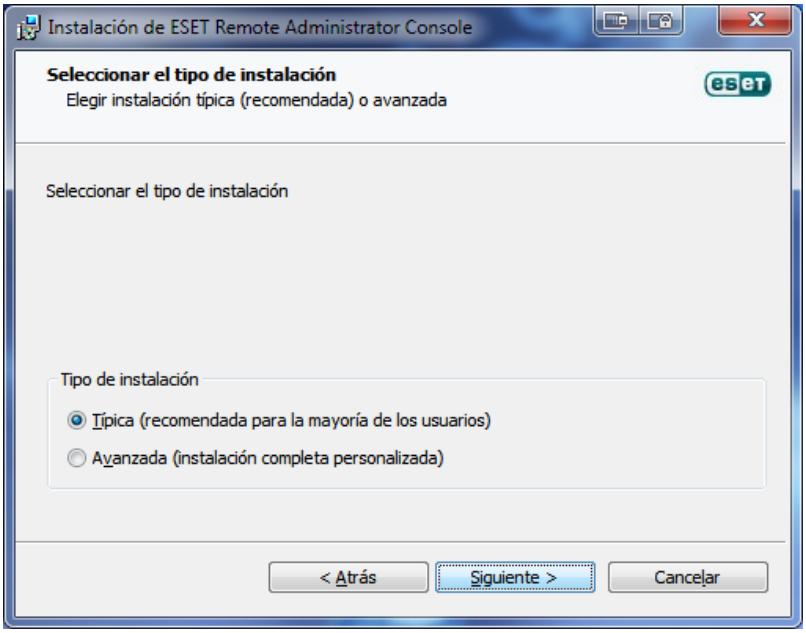

Fig. 1-6

5. En la ventana Preparado para instalar, presione el botón ***Instalar*** para comenzar la instalación de ***ESET Remote Administrator Console.***

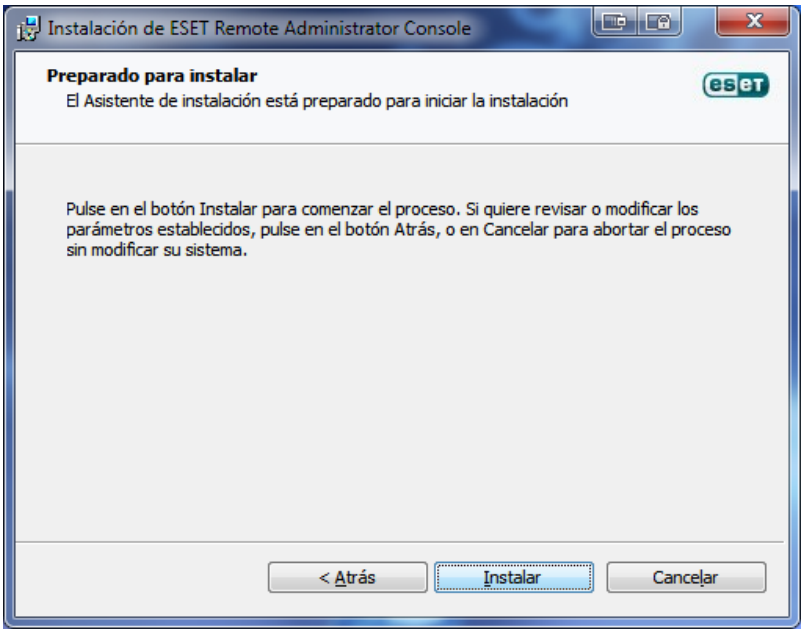

Fig. 1-7

6. Ventana Instalando ESET Remote Administrator Console. Esperar que finalice el proceso de instalación.

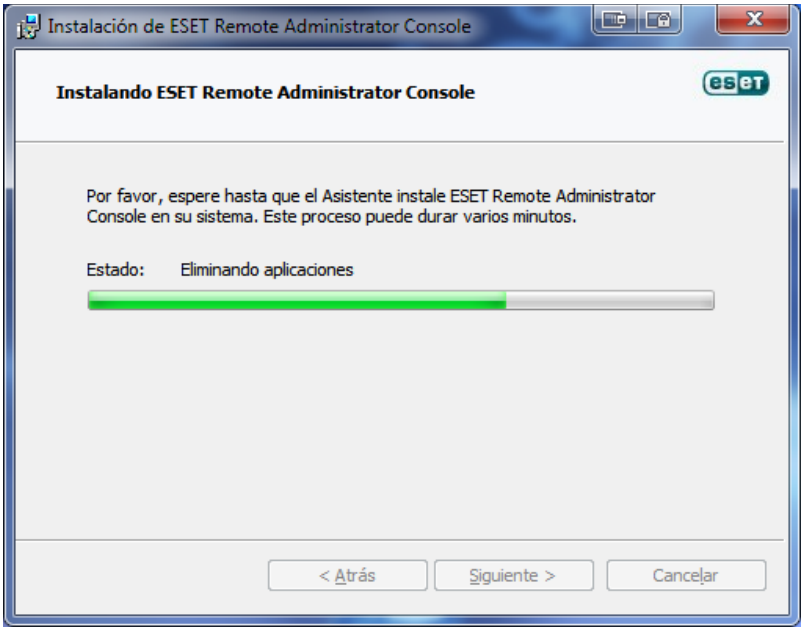

Fig. 1-8

7. Cuando se visualice la ventana ***Completando el Asistente instalación de ESET Remote Administrator Console,*** presione el botón Finalizar.

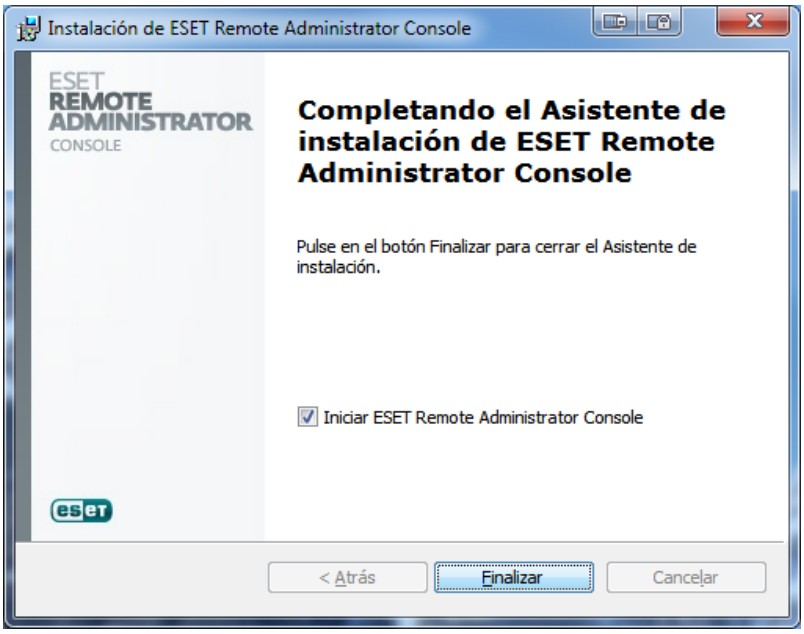

Fig. 1-9

CONFIGURANDO ESET REMOTE ADMINISTRATOR CONSOLE (ERAC)

1. Una vez que se ha finalizado correctamente el proceso de Instalación de ESET Remote Administrator Console, aparecerá el icono en el escritorio del equipo. Haga doble clic en el ícono para comenzar a hacer uso de la consola de administración.

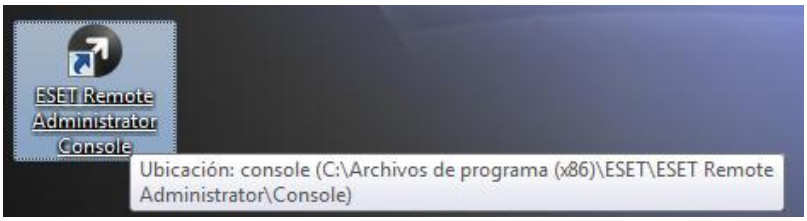

Fig. 1-1

2. En la ventana Escribir contraseña del servidor, se debe ***Ingresar los datos de acceso al servidor***, ***de no tener contraseña el espacio debe dejarse en blanco***. Luego presionar el botón Aceptar.

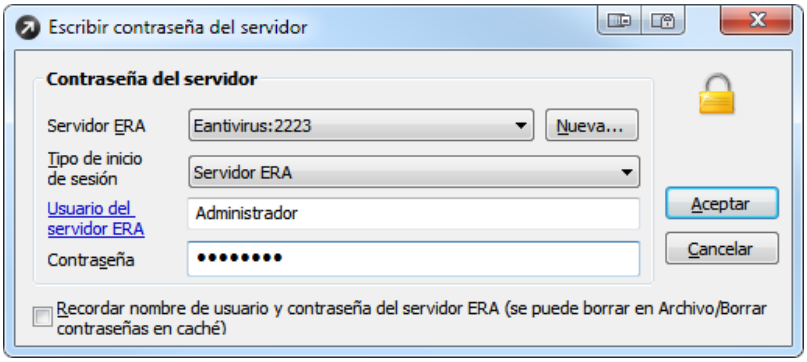

Fig. 1-2

Opciones:

1. ***Servidor ERA:*** *nombre del Servidor:2223*
2. ***Tipo de Inicio de sesión:*** *servidor ERA*
3. ***Usuario del servidor ERA:*** *administrador*
4. ***Contraseña:*** *Contraseña del Usuario Administrador*

3. Luego de haber ingresado a la consola de administración, se podrá visualizar la ventana principal.

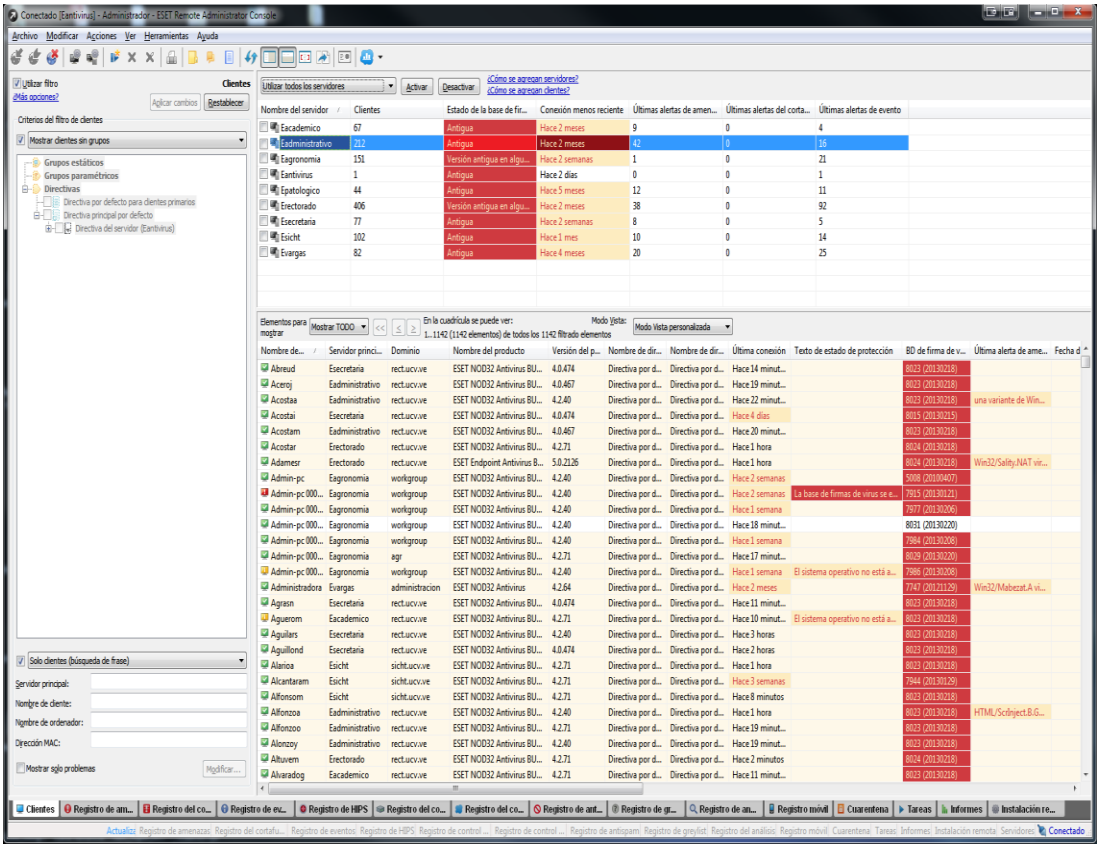

Fig. 1-3

4. En la ventana principal de la consola de administración, hacer click en el Menú ***Herramientas*** y luego ***Opciones del Servidor***.

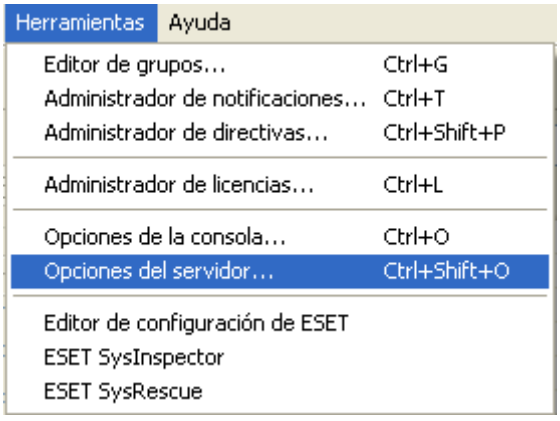

Fig. 1-4

5. En la ventana Opciones del Servidor, es donde se realizará la configuración de las opciones de Replicación, Actualización y Licenciamiento. En la Pestaña General se puede visualizar un resumen general del servidor. Hacer click en la pestaña ***Replicación.***

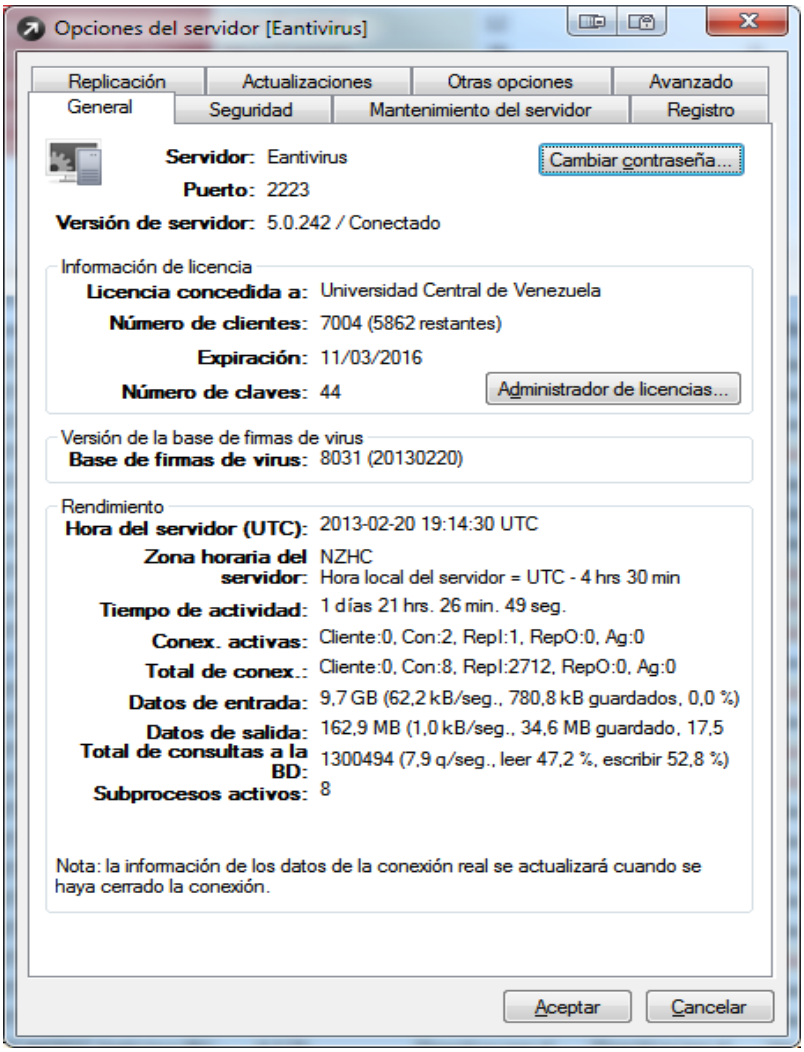

Fig. 1-5

6. Seleccionar la pestaña ***Replicación*** y modificar las siguientes opciones:
    - *Tildar la opción* ***Activar replicación "a"***
    - *Servidor superior:* ***eantivirus.rect.ucv.ve***
    - *Puerto:* ***2846 (puerto por defecto)***

Luego presionar el botón ***Replicar ahora***. Si se realizó correctamente el proceso de replicación, en la opción ***Estado de la replicación "a",*** debe mostrar ***Completado indicando la fecha y hora de la replicación.***

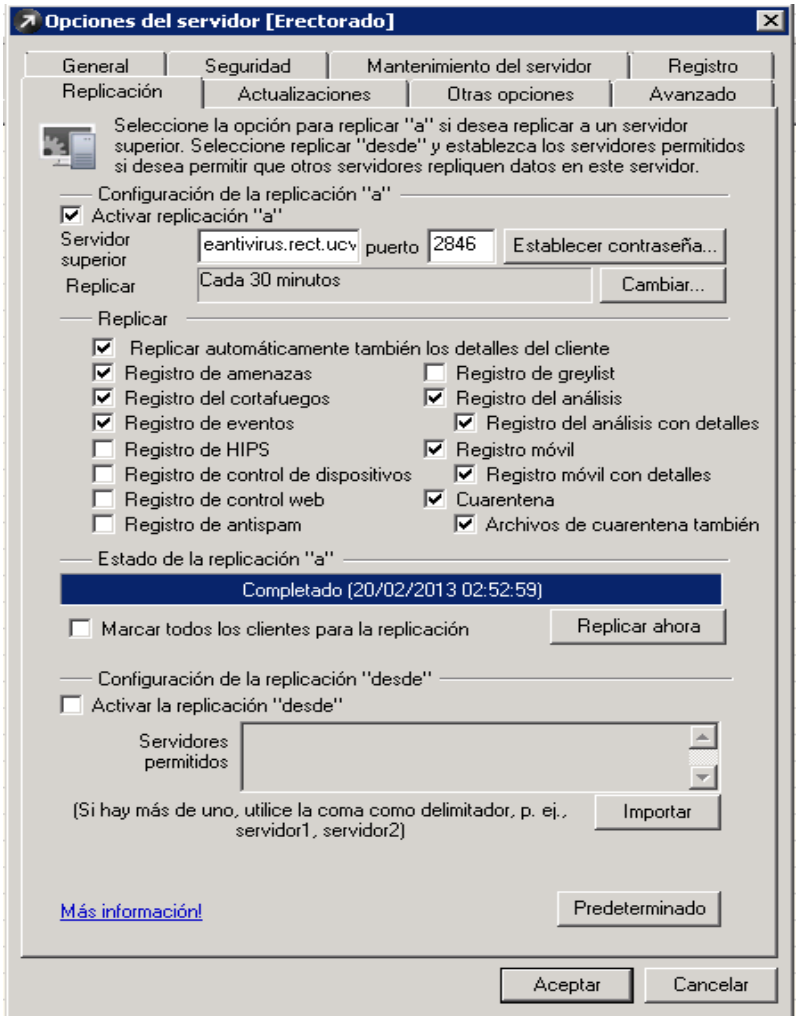

Fig. 1-6

<u>Nota</u>: es importante no dejar ninguno de estos campos en blanco o se puede correr el riesgo de que el servidor no realice el proceso de replicación de forma satisfactoria.

7. Luego seleccionar la pestaña ***Actualizaciones*** y modificar las siguientes opciones:
    - Actualizaciones del servidor: ***http://eantivirus.rect.ucv.ve:2221 si al realizar la actualización, se produce un error, cambiar el valor anterior por http://190.169.31.8:2221.***
    - Intervalo de actualización: ***cada 60 minutos.***
    - Actualizar nombre: ***este valor se encuentra en la carpeta de Licenciamiento en un archivo (.txt). Ubicar el archivo en el equipo e ingresar el valor asignado al nombre de usuario.***
    - Actualizar contraseña: ***este valor se encuentra en la carpeta de Licenciamiento en un archivo (.txt). Ubicar el archivo en el equipo e ingresar el valor asignado a la contraseña.***

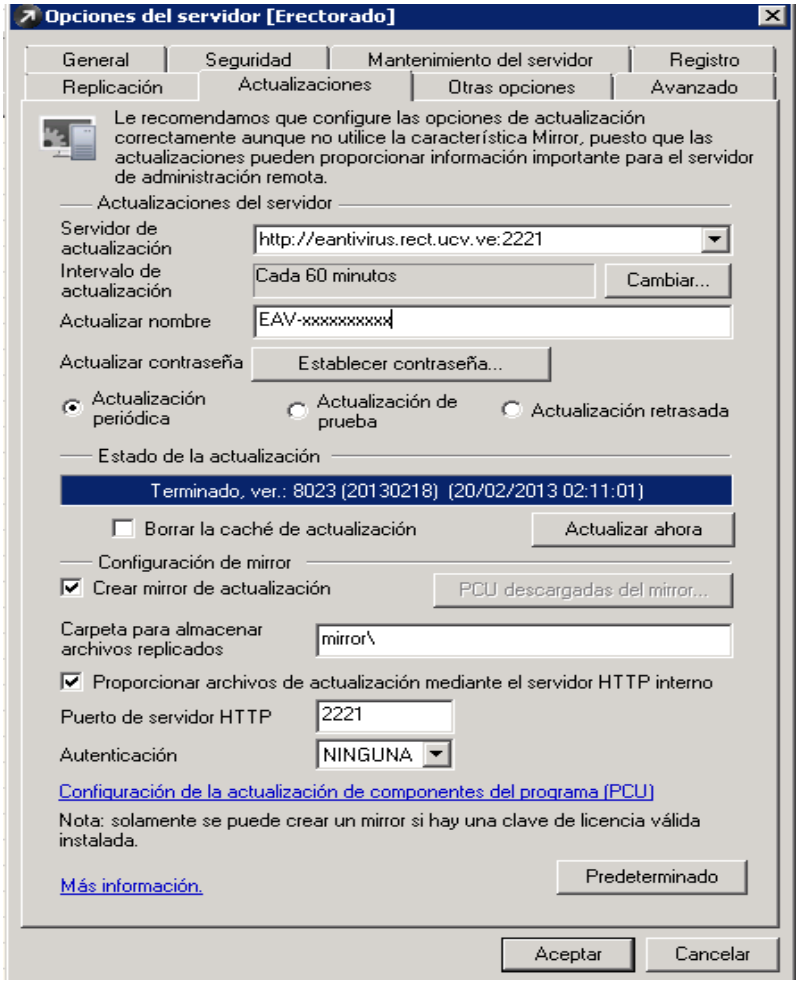

Fig. 1-7

Luego presionar el botón **Actualizar ahora**.

Si se realizó correctamente, en la opción ***Estado de la actualización*** debe decir ***Terminado*** indicando la ***versión de la base de firmas de virus, la fecha de esa base de firmas, la fecha y hora en que se realizó la actualización***. Luego presionar el botón **Aceptar**.

Nota: es importante no dejar ninguno de estos campos en blanco o se puede correr el riesgo de que el servidor no realice el proceso de actualización de forma satisfactoria.
Verificar que el estatus de la actualización alcance el 100%. En caso contrario, comunicarse con la DTIC para solventar el problema.

CARGANDO EL ARCHIVO DE LICENCIAMIENTO (.LIC) EN EL SERVIDOR (ERAS)

El archivo de licenciamiento (.lic) contiene datos como la fecha de expiración de la licencia y el número de equipos cliente para los cuales ésta es válida y es necesario para que su producto funcione correctamente.

1. Debe abrir la consola de ***administración ESET Remote Administrator Console***, haciendo click en **Inicio** → **Todos los programas** → **ESET** → **ESET Remote Administrator Console**.

En la barra de Menú, Haga clic en ***Herramientas*** → ***Administrador de licencias...***[2] o presione las teclas ***CTRL + L*** en su teclado.

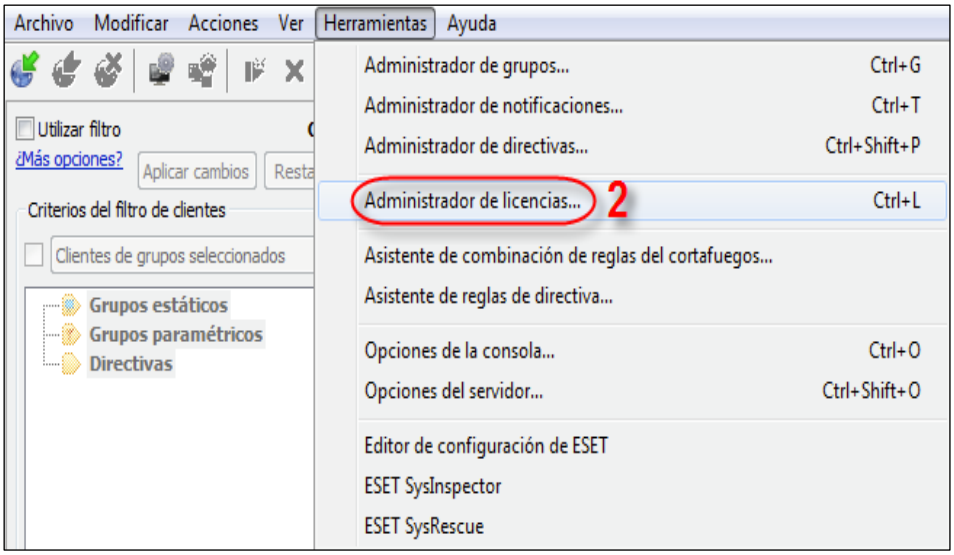

Fig. 1-1

2. En la ventana **Administrador de licencias**, Presione el botón ***Examinar...***[3] y luego localice el archivo .lic y Haga doble clic sobre él, seguidamente El **Administrador de licencias** mostrará la información de la nueva licencia. Luego Presione el botón ***Cargar en el servidor***[4].

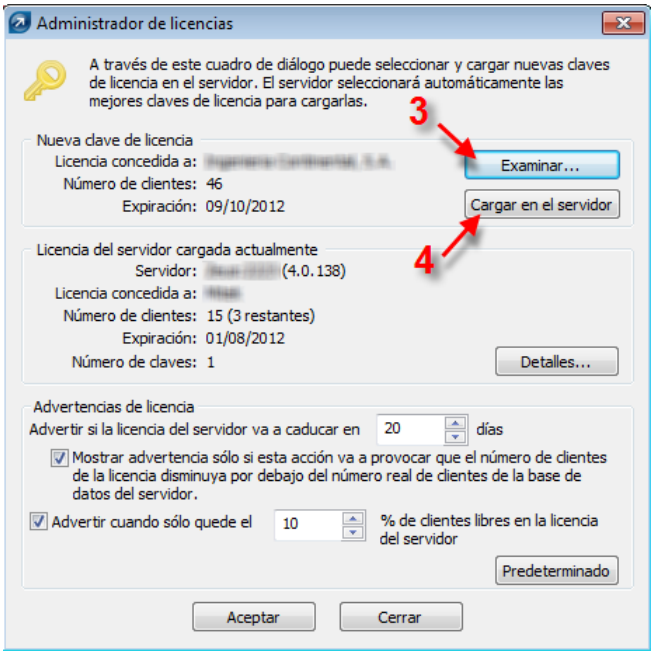

Fig. 1-2

Luego se Visualizará la siguiente ventana, al cargar exitosamente el archivo de licencia.

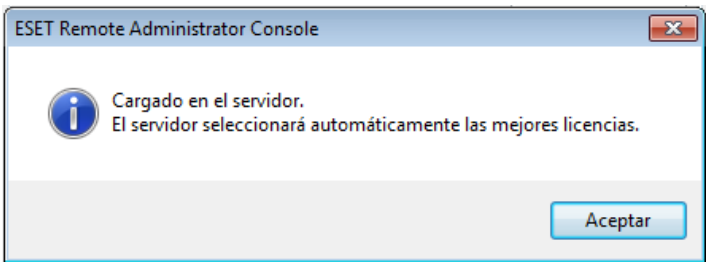

Fig. 1-3

Presione ***Aceptar dos veces*** a fines de cerrar la ventana del ***Administrador de licencias*** y ***guardar los cambios***. Su ERA Server ha sido actualizado con la nueva información de licencia.

NOTA: si usted quitó de modo completo su anterior archivo de licencia antes de descargar el nuevo no aparecerá el siguiente cuadro de diálogo.

CONFIGURANDO LAS EXCEPCIONES EN EL FIREWALL DE WINDOWS DEL SERVIDOR DE ANTIVIRUS

1. La siguiente tabla enumera las posibles comunicaciones de red con un ERAS instalado.

Protocolo	Puerto	Descripción
TCP	2221 (escucha del ERAS)	Puerto predeterminado que la función del servidor local de actualización integrada en ERAS utiliza (versión HTTP)
TCP	2222 (escucha del ERAS)	Comunicación entre clientes y el ERAS
TCP	2223 (escucha del ERAS)	Comunicación entre la ERAC y el ERAS
TCP	2224 (escucha del ERAS)	Comunicación entre el agente einstaller.exe y el ERAS durante la instalación remota
TCP	2846 (escucha del ERAS)	Replicación del ERAS

Fig. 1-1

2. Excepción de ESET para la actualización por el puerto 2221.

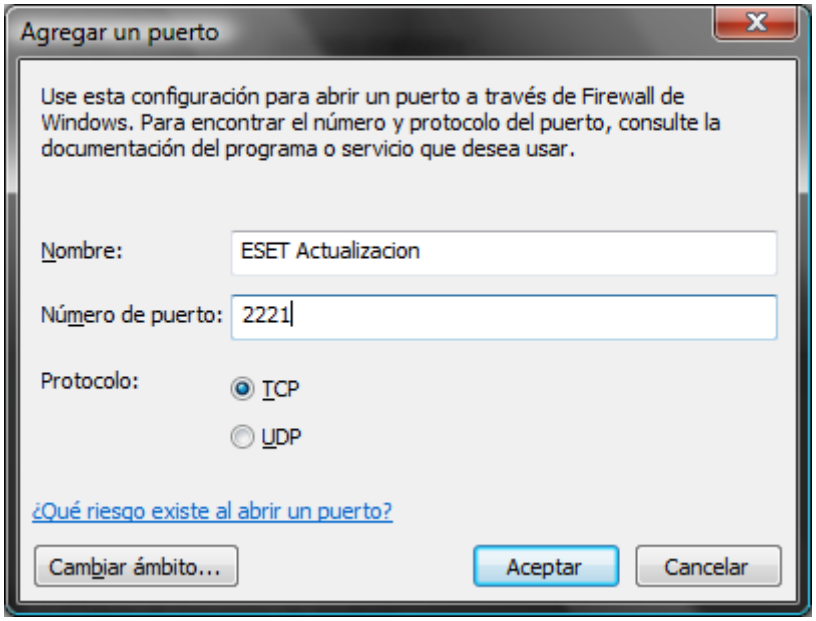

Fig. 1-2

3. Excepción de ESET para la administración por el puerto 2222.

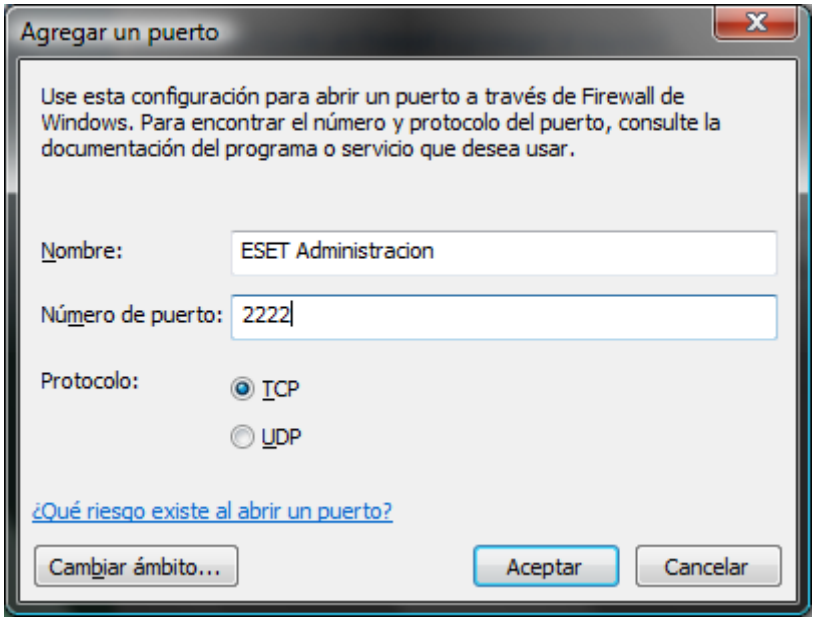

Fig. 1-3

4. Excepción de ESET para la administración remota por el puerto 2223.

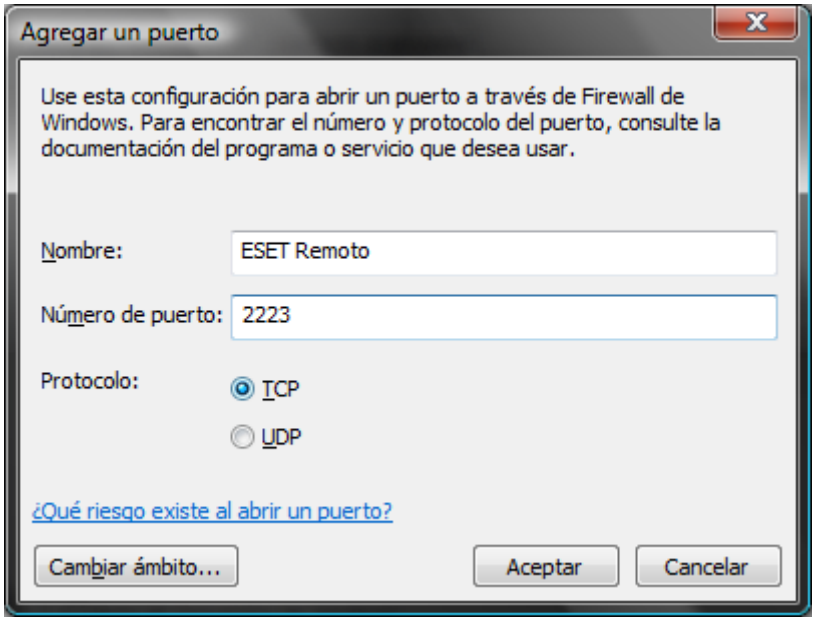

Fig. 1-4

5. Excepción de ESET para la administración remota por el puerto 2224.

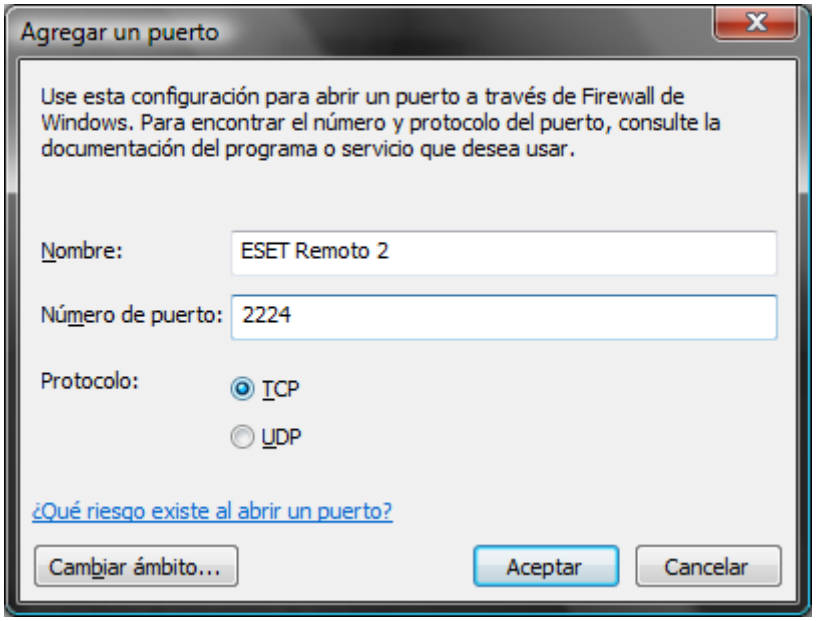

Fig. 1-5

6. Excepción de ESET para la replicación por el puerto 2846.

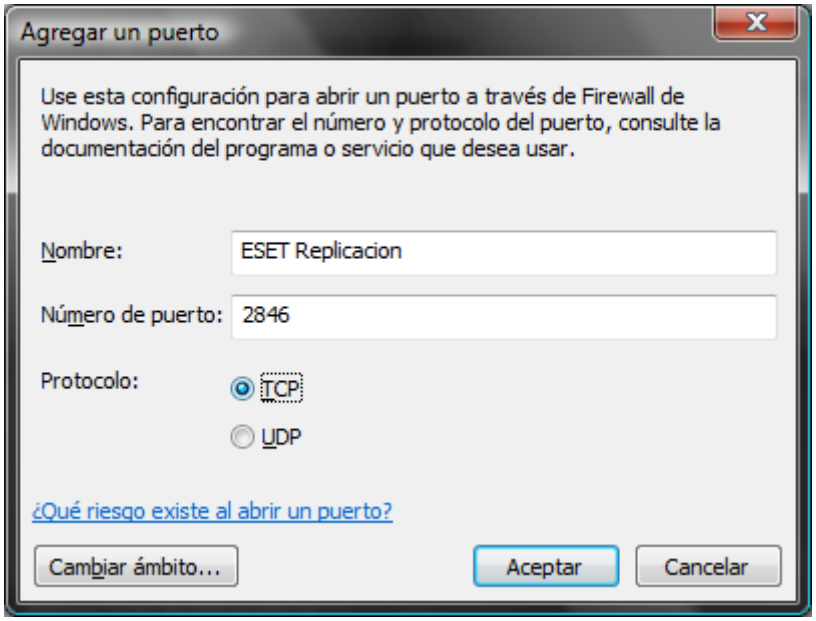

Fig. 1-6

CREANDO EL ARCHIVO DE CONFIGURACIÓN (.XML) PARA LOS CLIENTES INSTALADOS EN SERVIDORES

1. Abrir el Editor de configuraciones de ESET, presionar ***INICIO, TODOS LOS PROGRAMAS, ESET Y FINALMENTE EDITOR DE CONFIGURACIÓN DE ESET.***

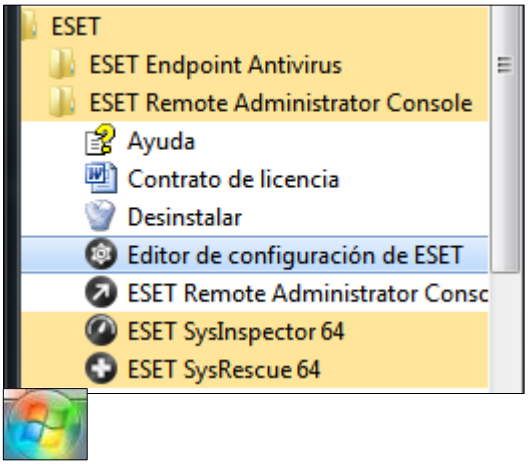

Fig. 1-1

2. En la siguiente ventana aparecerá el ***Editor de configuraciones de ESET***. Luego presione el botón Nuevo.

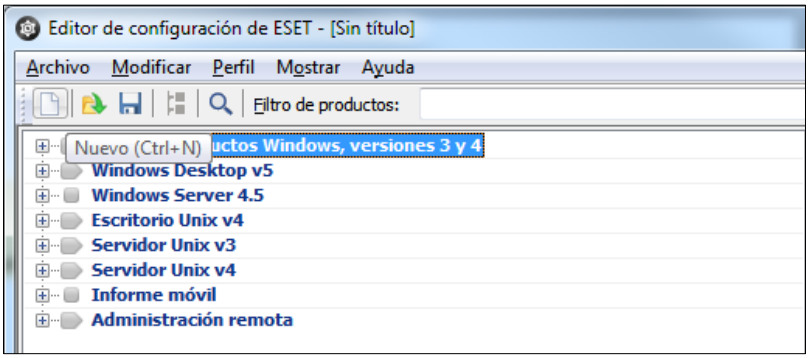

Fig. 1-2

3. Configuración de los Parámetros de ***Modulo de Actualización.***

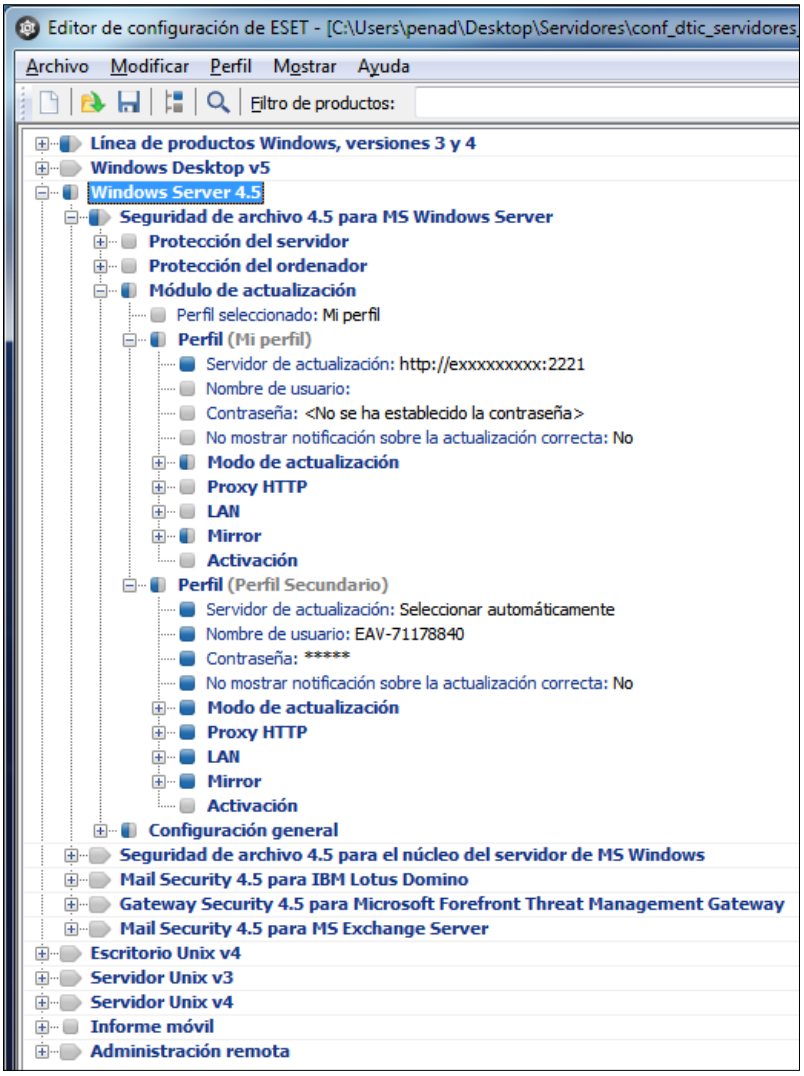

Fig. 1-3

Se deben desplegar las siguientes opciones:

- ***Windows Server 4.5***
  - ***Módulo de Actualización***
    - ***Perfil (Mi Perfil)***
      - ***Servidor de Actualización:*** ***http://nombredelservidor:2221***

En la opción **Servidor de actualización**, seleccionar el Valor <Servidor de actualización personalizada> y agregar el nombre del servidor (http://nombredelservidor:2221).

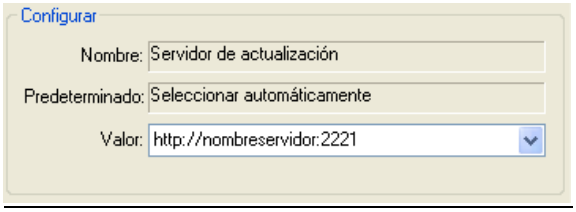

Fig. 1-4

Se debe ***agregar un segundo perfil de actualización***, para ello hacemos click (DERECHO) sobre la opción perfil y agregamos uno nuevo con el nombre ***PERFIL SECUNDARIO***. Luego desplegar las opciones del nuevo perfil:

- ***Perfil (Perfil Secundario)***
  - ***Servidor de Actualización: seleccionar Automáticamente***
  - ***Nombre de Usuario: EAV-00000000***
  - ***Contraseña:*** **********

4. Configuración del Parámetro ***Programador de tareas***

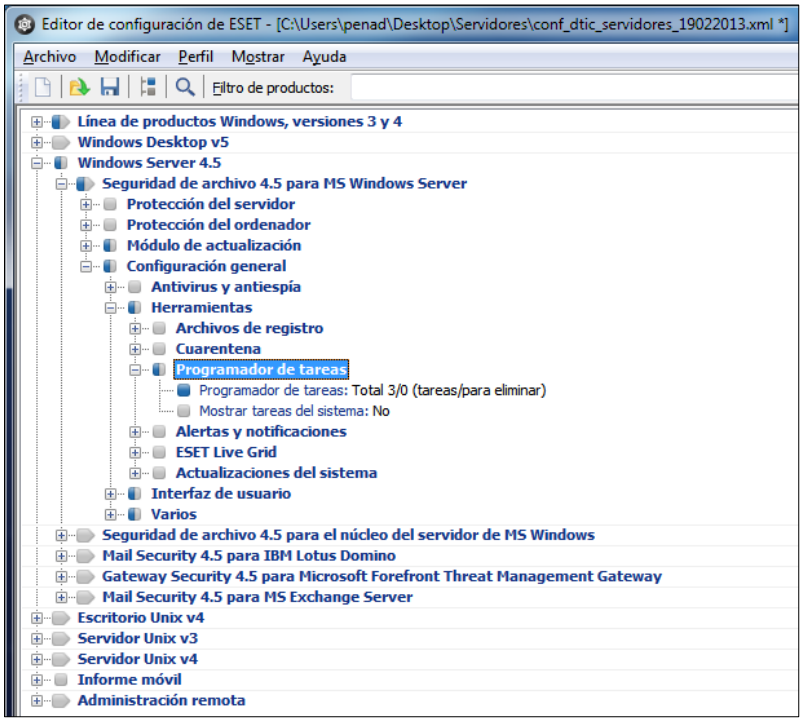

Fig. 1-5

Se debe desplegar las siguientes opciones:

- ***Windows Server 4.5***
  - ***Seguridad de archivo 4.5 para MS Windows Server***
    - ***Configuración general***
      - ***Herramientas***
        - ***Programador de Tareas***

En la ventana ***Programador de Tareas***, presionar el botón Agregar.

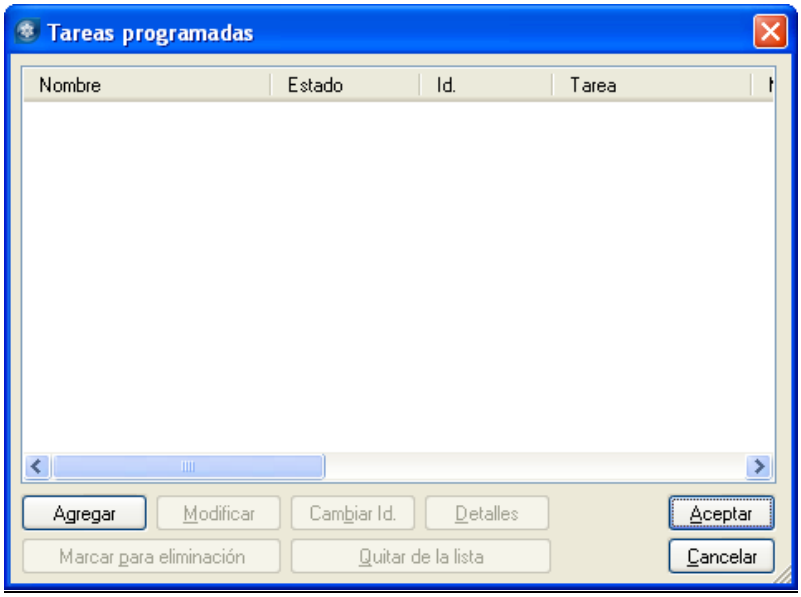

Fig. 1-6

En la ventana Agregar tarea, en la opción Tarea programada, seleccionar ***Análisis del equipo***, Luego presionar el botón Siguiente.

Fig. 1-7

En la siguiente ventana, en la opción Nombre de la tarea escribir ***Limpieza_Rutina***, y en la opción Ejecutar la tarea, seleccionar ***Semanalmente***, Luego presionar el botón Siguiente.

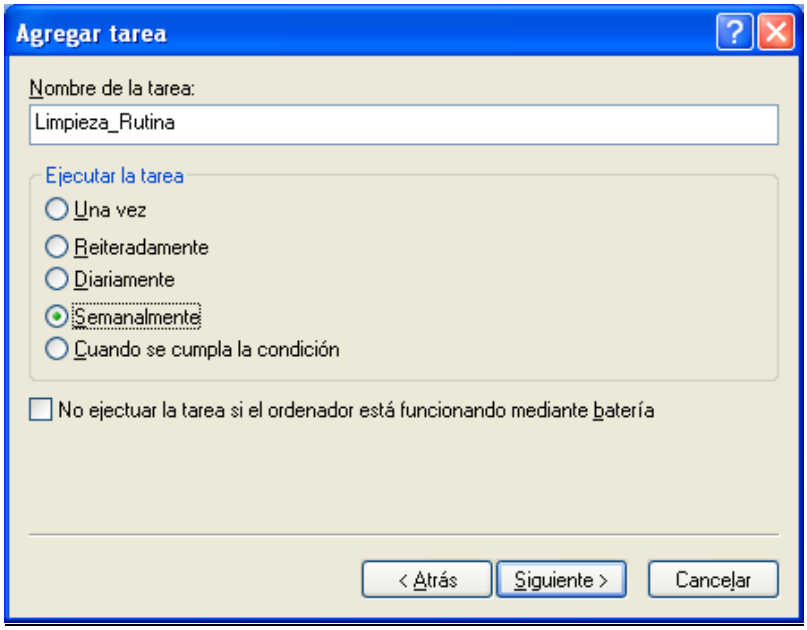

Fig. 1-8

Luego en la siguiente ventana, la opción Horario de ejecución de la tarea, el horario será ***12:05:00 p.m.,*** en la opción Ejecutar la tarea en los siguientes días, tildar ***Miércoles***, Luego presionar el botón Siguiente.

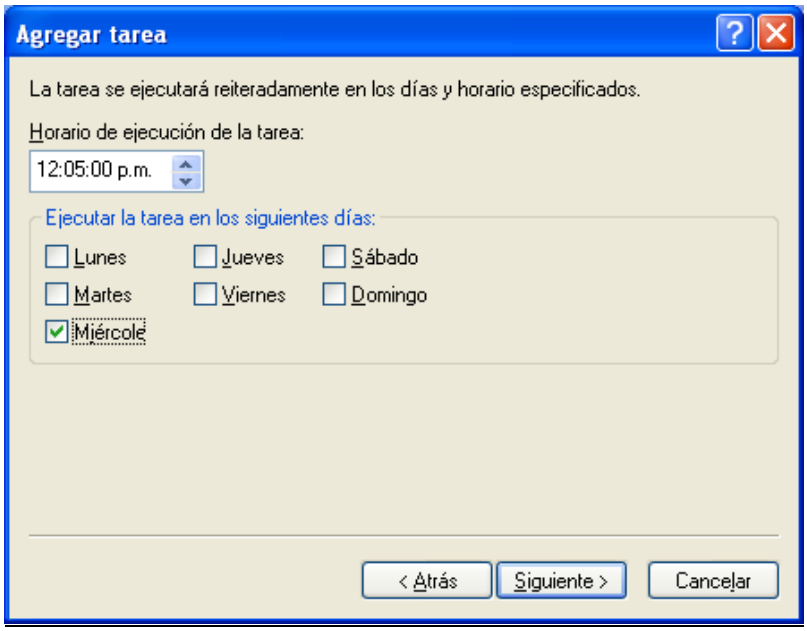

Fig. 1-9

***NOTA*: estas opciones pueden ser modificadas de acuerdo a los requerimientos y necesidades de cada Facultad, Dependencia Central o Extramuro.**

La próxima ventana, en la opción Si la tarea no se hubiera ejecutado, seleccionar ***Esperar hasta la próxima activación programada***, Luego presionar el botón Siguiente.

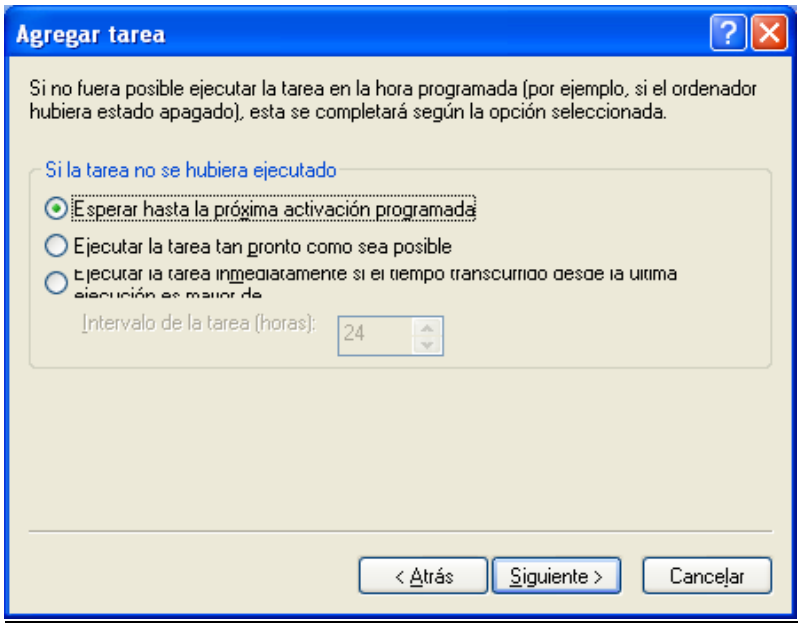

Fig. 1-10

Finalmente, se desplegará una ventana con la configuración suministrada anteriormente. Luego presionar el botón ***Finalizar***, para culminar con el proceso de configuración.

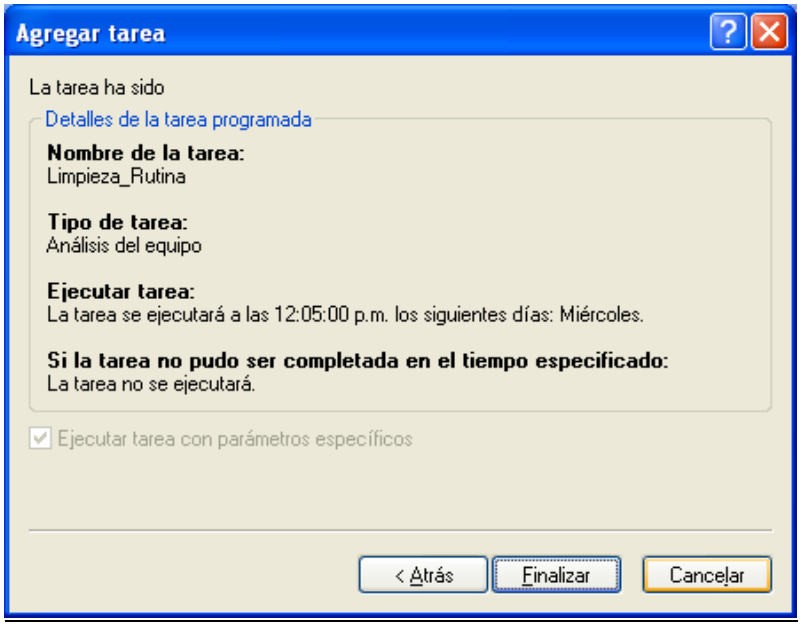

Fig. 1-11

En la ventana Configuración especial, en la opción Descripción escribir ***Limpieza_Rutina.***

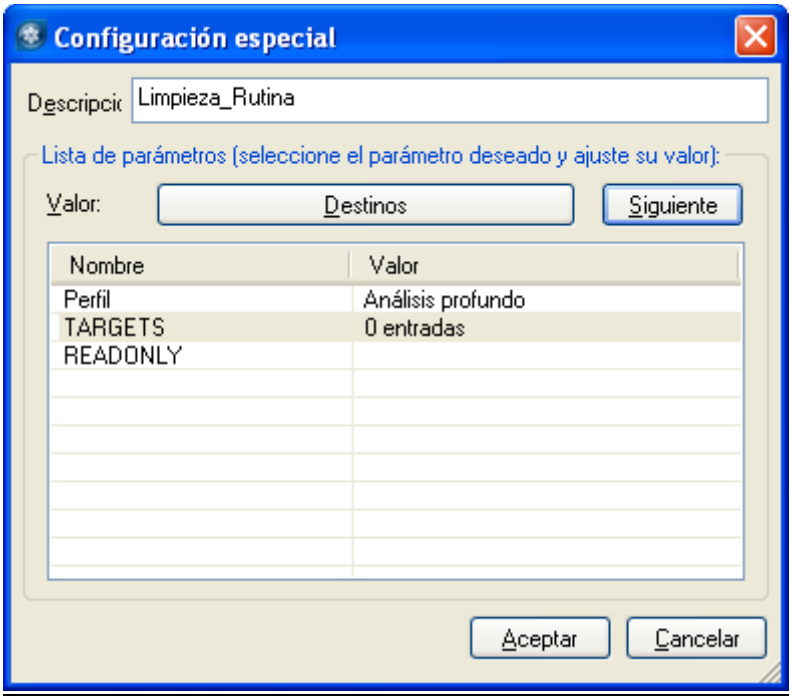

Fig. 1-12

En la misma ventana, seleccionar la opción ***TARGETS*** y luego presionar el botón ***Destinos***.

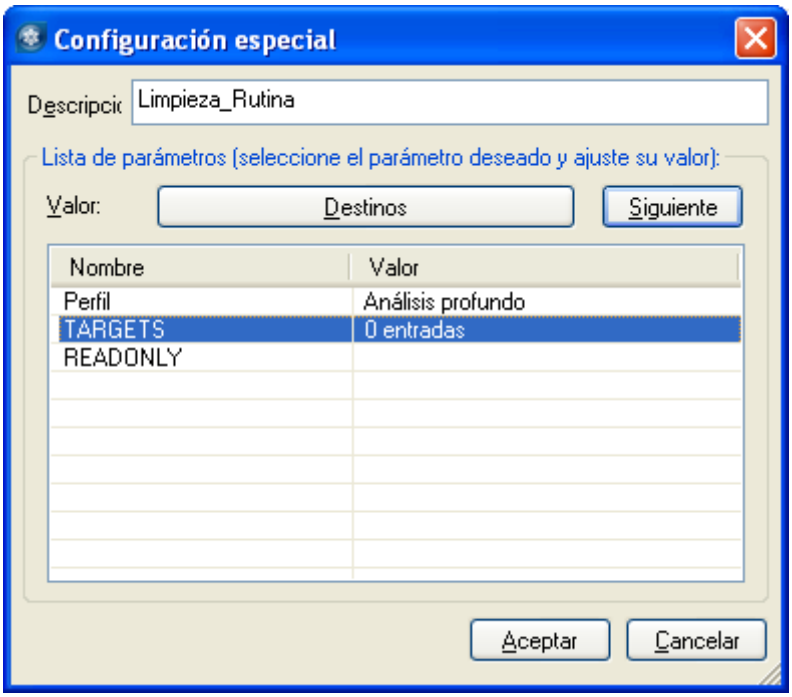

Fig. 1-13

En la ventana carpetas y archivos, presionar el botón ***+Unidades…***

Fig. 1-14

En la ventana Selección de destinos de análisis…, tildar ***Sectores de inicio de la unidad de disco duro*** y ***Unidades de disco duro***. Luego presionar el botón Aceptar.

Fig. 1-15

En la ventana carpetas y archivos, presionar el botón ***+Memoria...***, Luego presionar el botón Aceptar.

Fig. 1-16

Una vez que han sido configuradas las opciones de destino de análisis, se volverá a la ventana Configuración Especial, luego presionar el botón Aceptar.

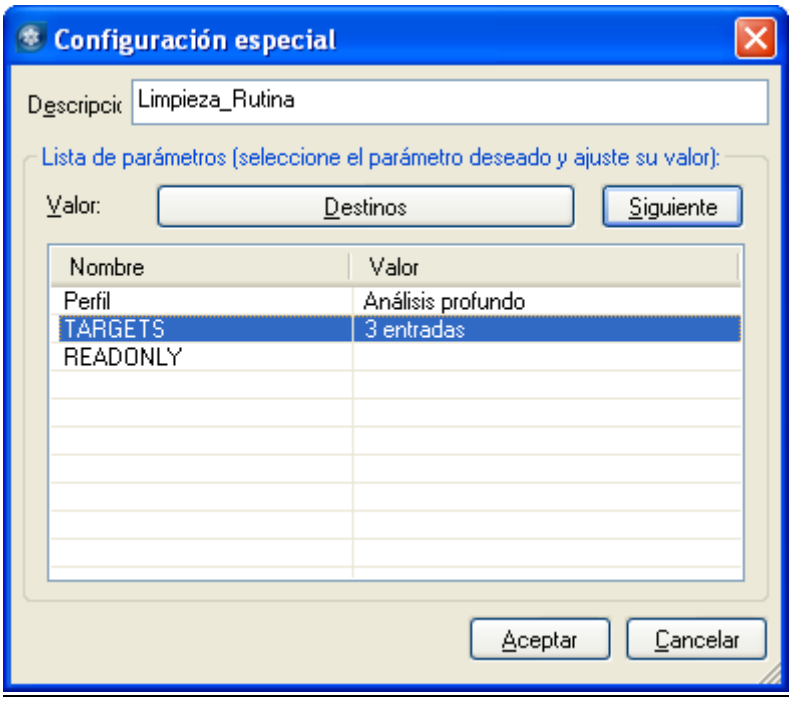

Fig. 1-17

Finalmente se mostrará en la ventana la tarea programada que se acaba de configurar, luego presionar el botón Aceptar.

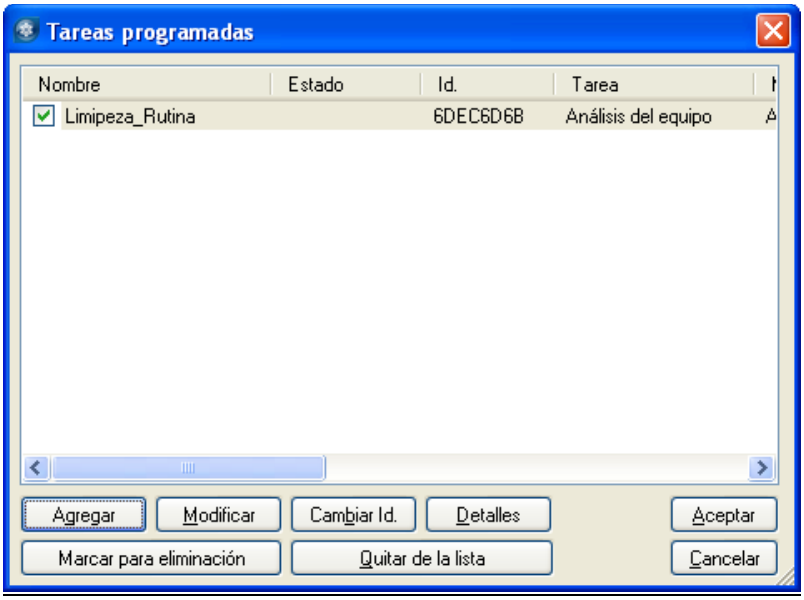

Fig. 1-18

5. Configuración del Parámetro ***Configuración de acceso,*** esta opción permite proteger los parámetros de configuración mediante una contraseña de acceso.

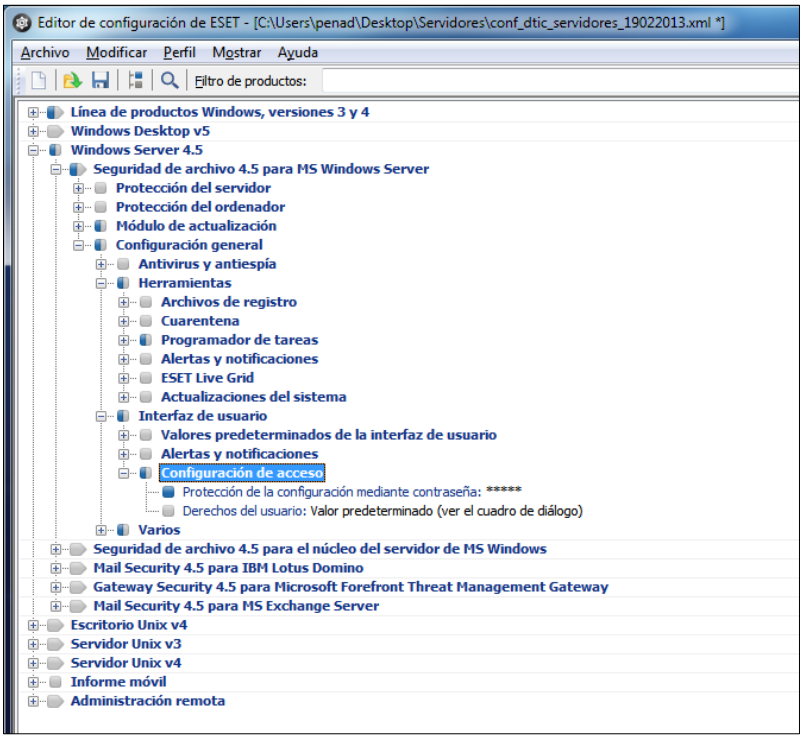

Fig. 1-19

Se deben desplegar las siguientes opciones:

- ***Windows Server 4.5***
  - ***Seguridad de archivo 4.5 para MS Windows Server***
    - ***Configuración general***
      - ***Herramientas***
        - ***Interfaz de Usuario***
          - ***Configuración de acceso***
            - ***Protección de la configuración mediante contraseña***

Se debe escribir una contraseña y confirmarla, como se muestra a continuación.

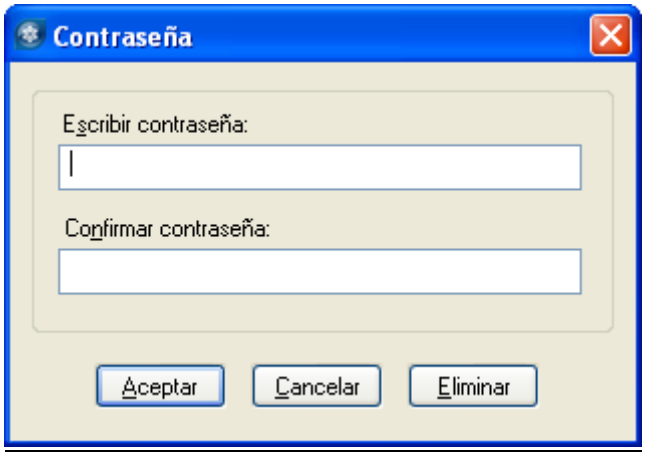

Fig. 1-20

Luego presionar el botón Aceptar.

Al seleccionar esta opción se debe colocar una contraseña que permita proteger el acceso a los parámetros de configuración del archivo que se está creando y que será importado más adelante en el cliente instalado en el servidor (ESET File Security).

Esta contraseña deberá tener un ***mínimo de 8 caracteres***, entre los cuales se deben colocar ***MAYUSCULAS, MINUSCULAS, CARACTERES ESPECIALES y NUMEROS***

6. Configuración del Parámetro ***Administración remota.***

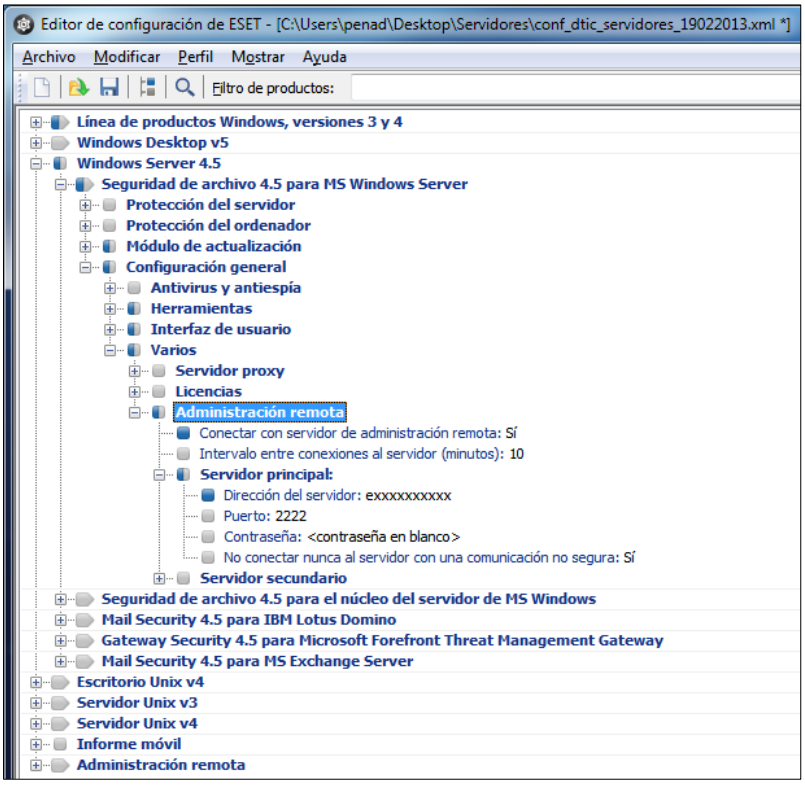

Fig. 1-21

Se deben desplegar las siguientes opciones:

- ***Windows Server 4.5***
  - ***Seguridad de archivo 4.5 para MS Windows Server***
    - ***Configuración general***
      - ***Varios***
        - ***Administración Remota***
          - ***Servidor Principal***

Opciones:

1. ***Conectar con el servidor de administración:*** seleccionar el Valor ***Sí/NO*** que se encuentra en la parte superior derecha, como se muestra a continuación.

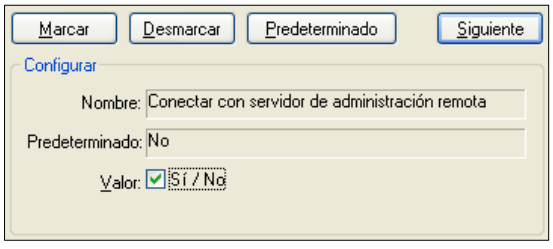

Fig. 1-22

2. ***Dirección del servidor: nombredelservidor*** donde se instaló la solución de antivirus.

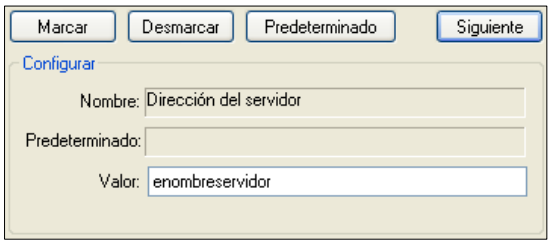

Fig. 1-23

3. ***Intervalo entre conexiones al servidor (en minutos)***, agregar el Valor de 5.

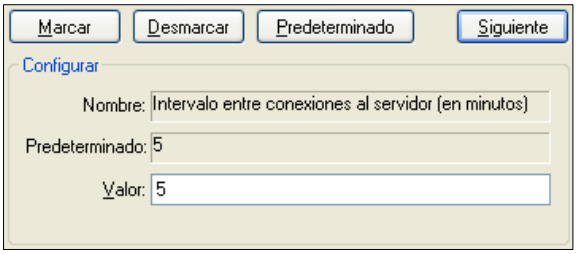

Fig. 1-24

Finalmente, se procede a guardar el archivo de configuración para su posterior uso.

El archivo de configuración debe de ser guardado con la siguiente estructura en el nombre: ***conf_nombredelservidor_servidor_díamesaño***.

INSTALANDO ESET FILE SECURITY CLIENTE PARA SERVIDORES

¡Importante!

Antes de realizar la instalación verifique la versión de su sistema operativo.

Cualquier solución de antivirus instalada previamente en su equipo debe ser desinstalada antes de comenzar con la instalación de su producto ESET.

1. Para comenzar la instalación, haga doble clic en el ícono del archivo instalador (***efsw_nt64_esn***) que guardó en el equipo. Si Windows le solicita Abrir/Ejecutar el archivo, presione Abrir/Ejecutar.

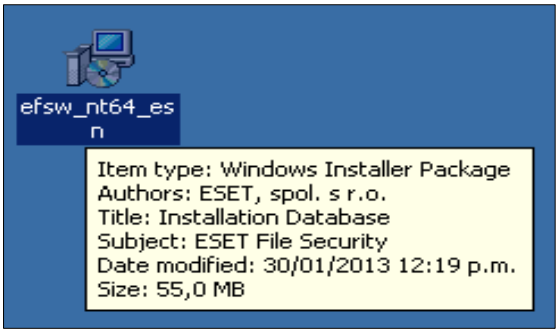

Fig. 1-1

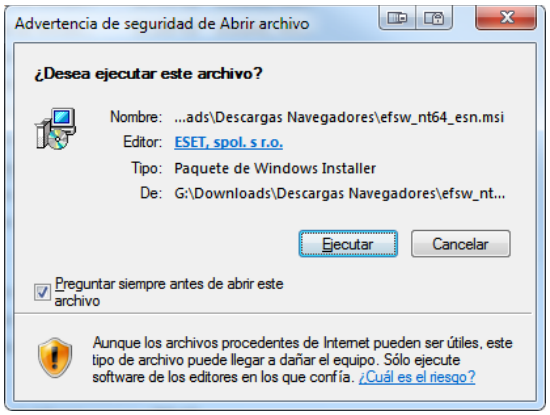

Fig. 1-2

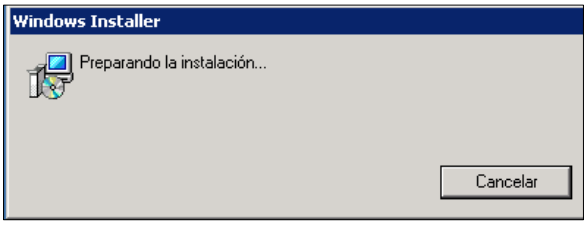

Fig. 1-3

2. En la siguiente ventana aparecerá el Asistente de instalación de ESET File Security. Luego presione Siguiente.

Fig. 1-4

3. En la ventana Acuerdo de licencia de usuario final, seleccione la opción ***Acepto las condiciones del acuerdo de licencia,*** para aceptar el acuerdo de licencia de ESET Endpoint Antivirus. Luego presione Siguiente.

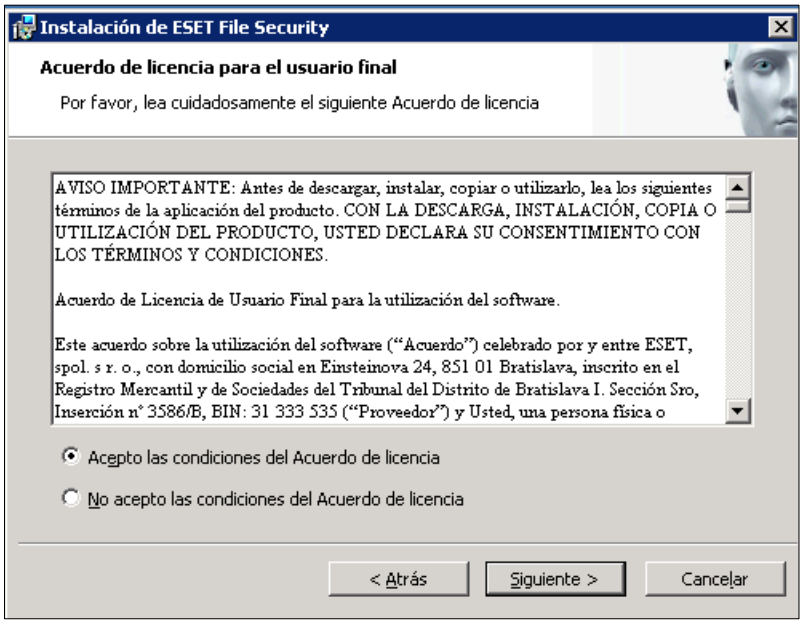

Fig. 1-5

4. En la ventana Modo de instalación, seleccione la opción ***Típica (Recomendada para la mayoría de los usuarios)*** y luego presione Siguiente.

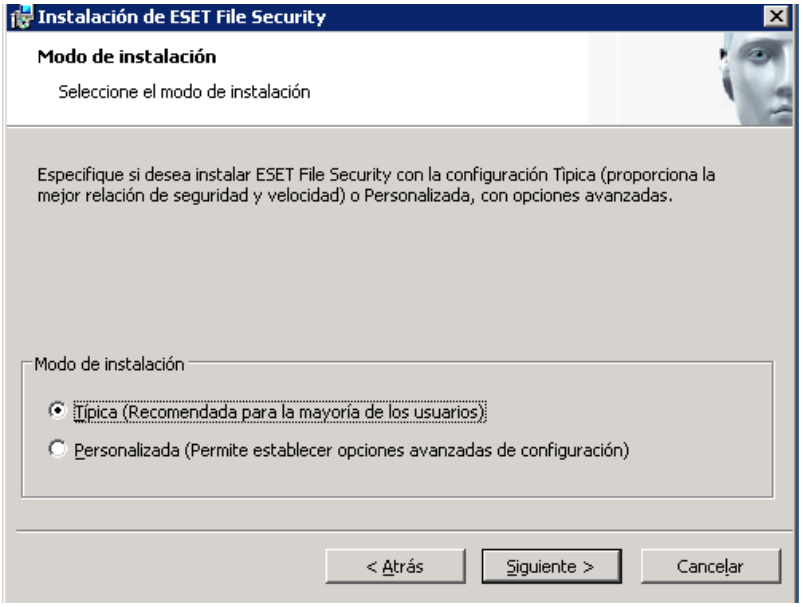

Fig. 1-6

5. En la ventana Actualización automática, tildar la opción ***Definir los parámetros de actualización más tarde*** y luego presione Siguiente.

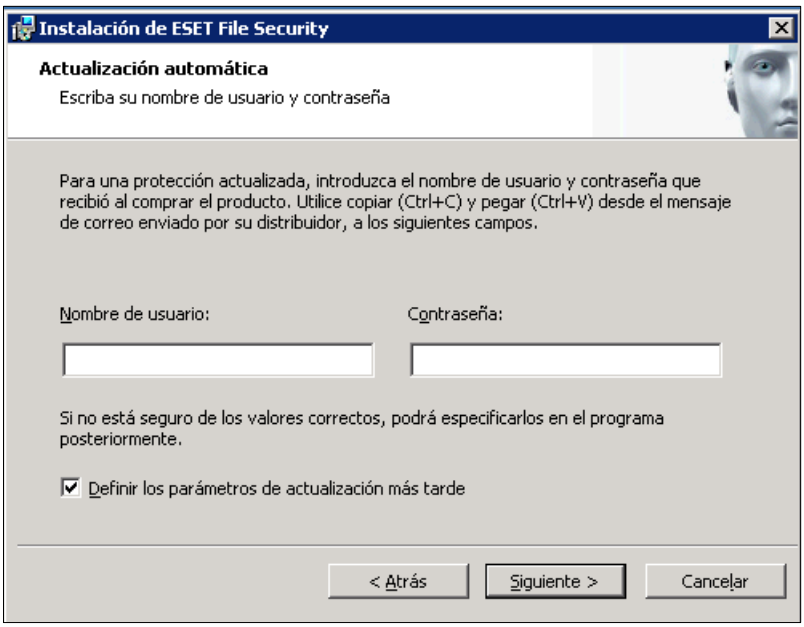

Fig. 1-7

6. En la ventana Sistema de alerta temprana ThreatSense.Net, tildar la opción ***Activar el sistema de alerta*** **temprana ThreatSense.Net** y luego presione Siguiente.

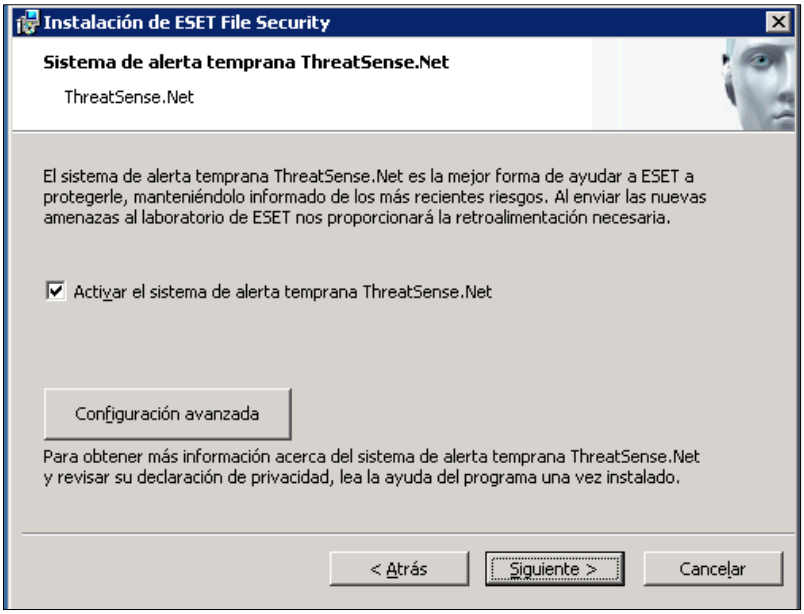

Fig. 1-8

7. En la ventana Detección de aplicaciones potencialmente indeseables, seleccione la opción ***Detección de aplicaciones potencialmente indeseables*** …

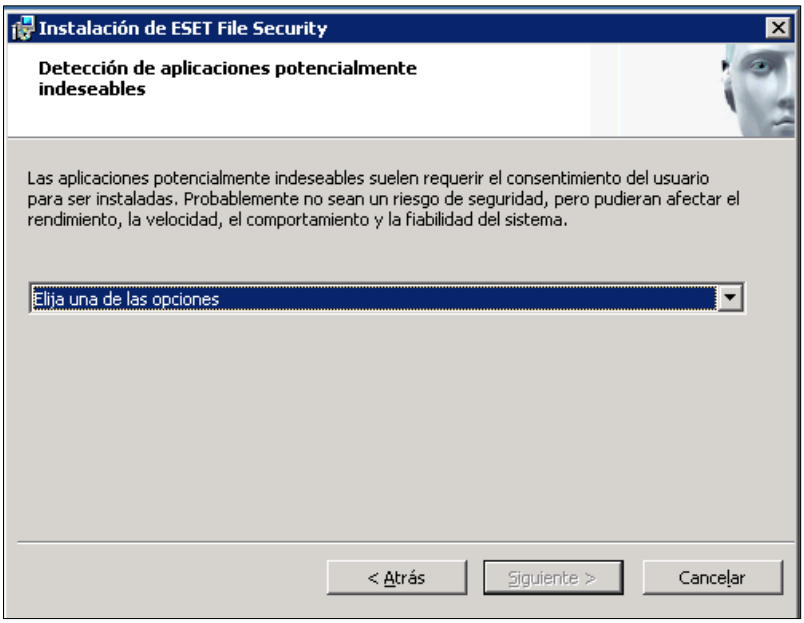

Fig. 1-9

8. Ventana con la opción ***Activar la detección de aplicaciones potencialmente indeseables*** *seleccionada.* Luego debe presionar Siguiente.

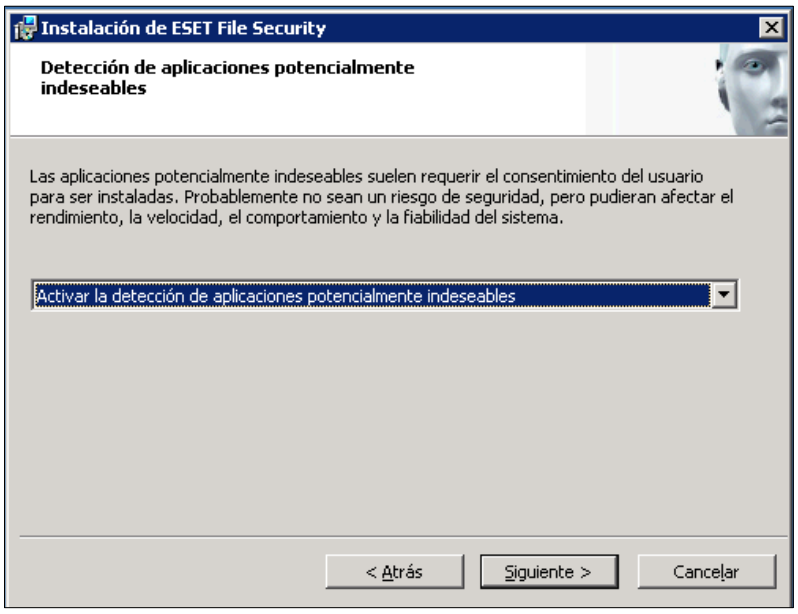

Fig. 1-10

9. En la ventana Preparado para instalar, debe presionar ***Instalar*** para comenzar la instalación de ***ESET File Security.***

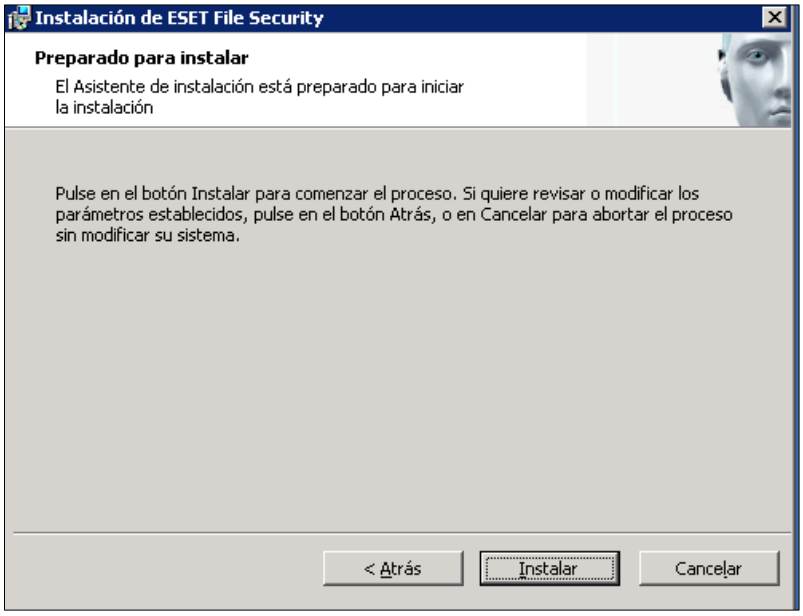

Fig. 1-11

10. Ventana Instalando ESET Endpoint Antivirus. Esperar que finalice el proceso de instalación.

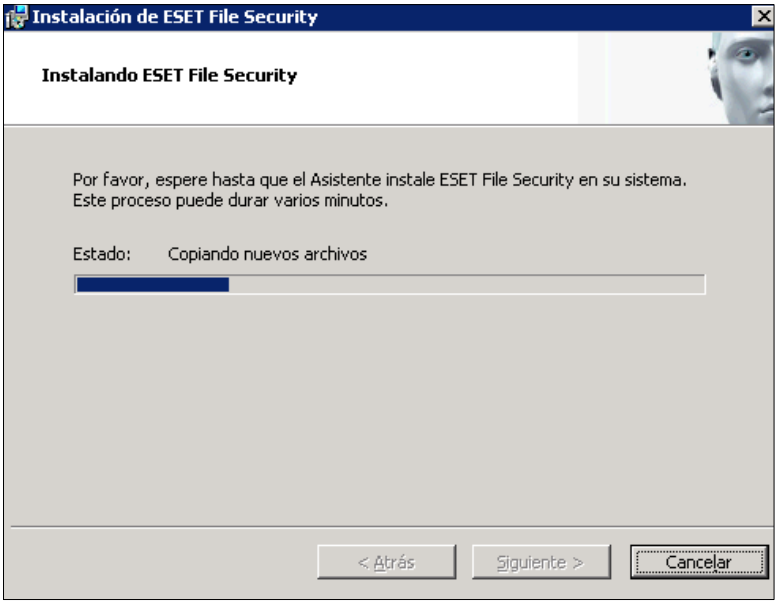

Fig. 1-12

11. Cuando se visualice la ventana Completando el Asistente de instalación de ESET File Security haga clic en ***Finalizar***.

Fig. 1-13

CARGANDO EL ARCHIVO DE CONFIGURACIÓN (.XML) EN EL CLIENTE DEL SERVIDOR

La opción de importar y exportar configuraciones de ESET File Security está disponible en **Configuración** y se activa haciendo clic en **Importar y exportar configuración.**

Tanto en la importación como en la exportación se utiliza el tipo de archivo .xml. La importación y la exportación son útiles para realizar copias de seguridad de la configuración actual de ESET File Security y, así, poder utilizarla más adelante.

La opción de exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida de ESET File Security en varios sistemas, ya que les permite importar fácilmente el archivo .xml para transferir los ajustes deseados.

1. Abrir ESET File Security.

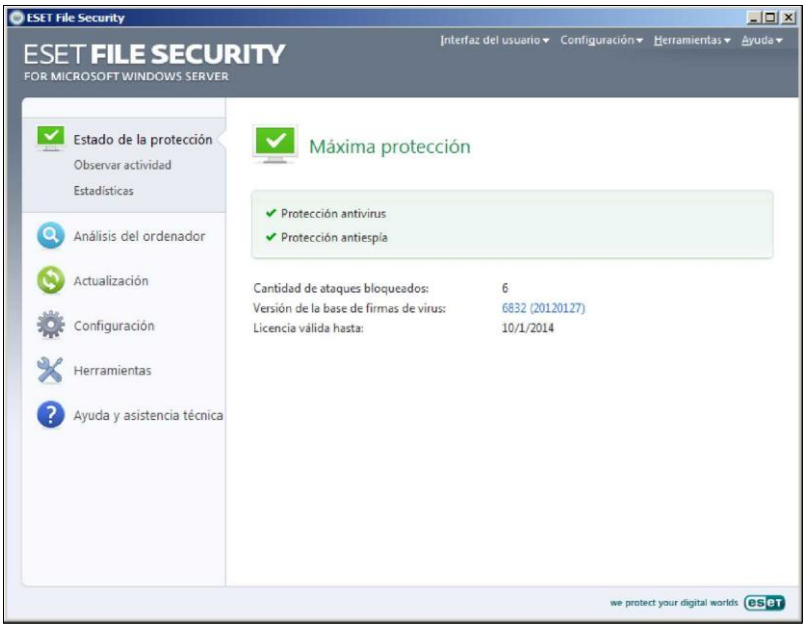

Fig. 1-1

2. En la ventana principal del ESET File Security, en el panel de opciones ubicado en el lado izquierdo, presionar ***Configuración*** → ***Importar o exportar la configuración…***

Fig. 1-2

3. En la ventana Importar y Exporta una configuración, presionar el botón ***…*** para ubicar la ruta donde se almaceno el archivo de configuración (.xml) previamente elaborado con el ***Editor de configuración de ESET.***

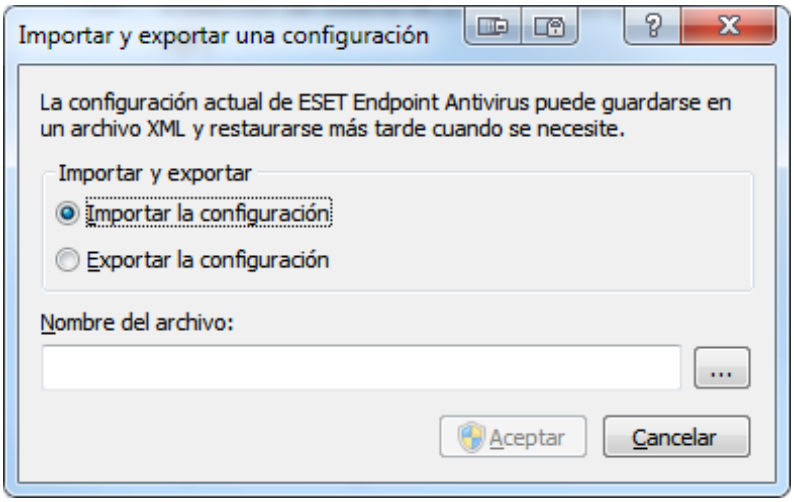

Fig. 1-3

4. En la ventana Abrir, seleccionar el archivo de configuración (.xml) que será cargado en el cliente de ESET Endpoint Antivirus. Luego presionar Abrir.

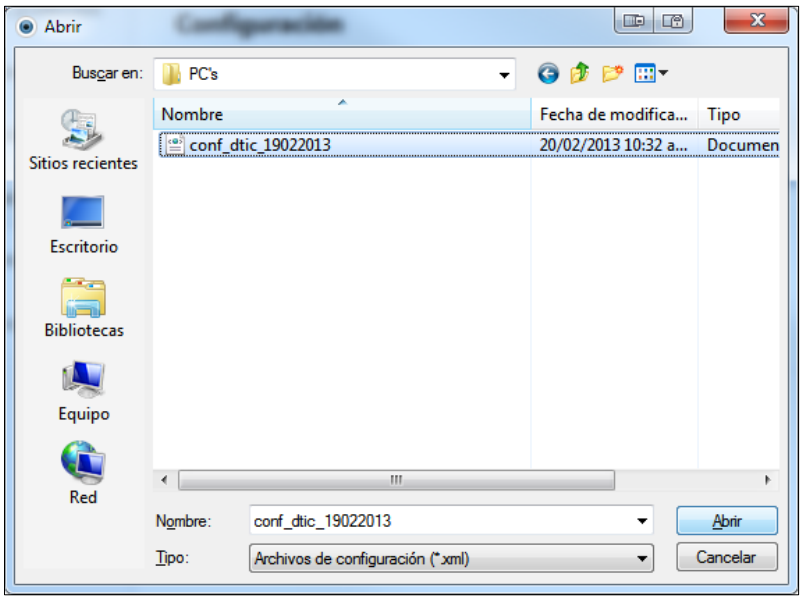

Fig. 1-4

5. En la siguiente ventana se mostrará la ruta de donde se seleccionó el archivo de configuración (.xml). Luego presionar Aceptar.

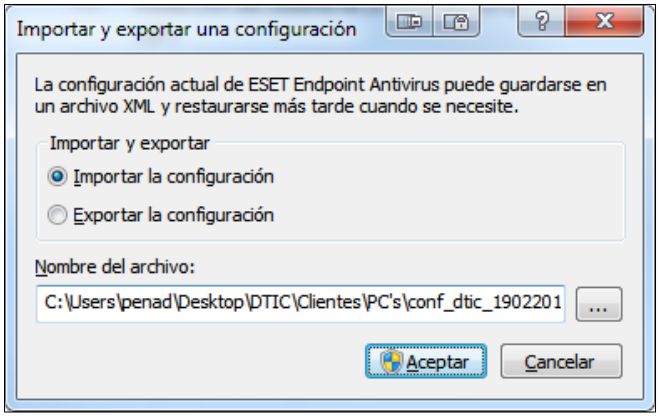

Fig. 1-5

6. Una vez que se ha cargado el Archivo de configuración (.xml), se procede a realizar la ***Actualización*** de la base de firmas de virus del ESET Endpoint Antivirus.

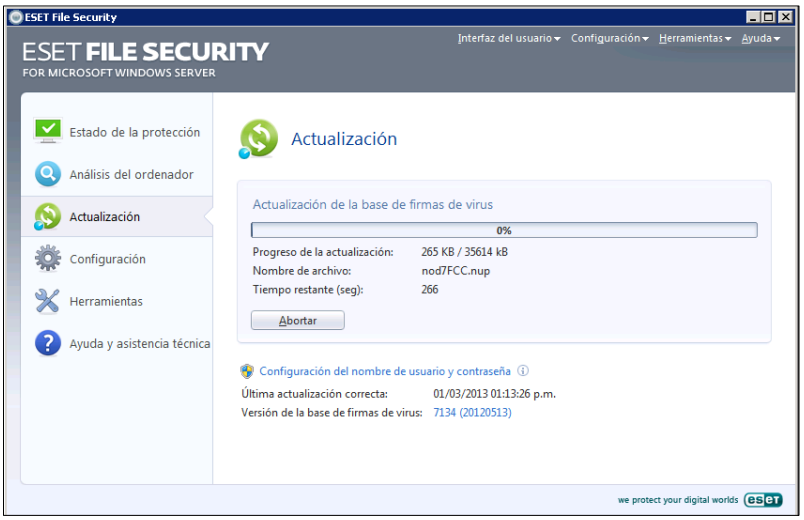

Fig. 1-6

7. En la siguiente ventana, se mostrará que el proceso de actualización se realizó satisfactoriamente.

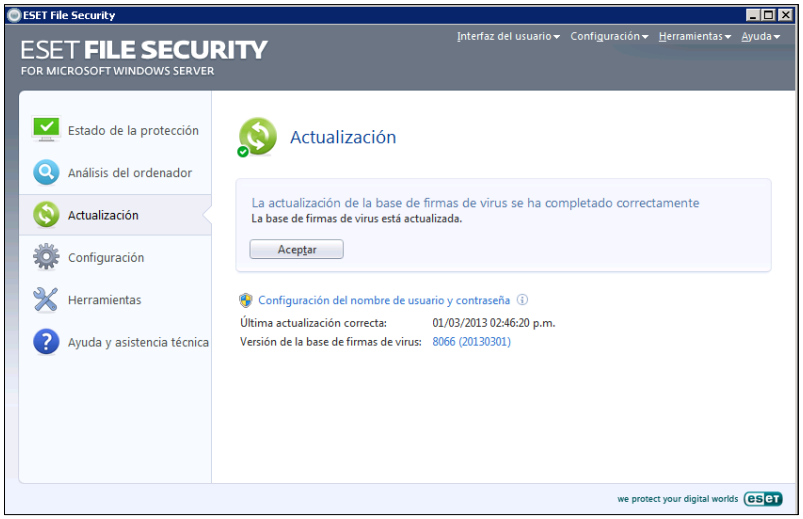

Fig. 1-7

CARGANDO EL ARCHIVO DE LICENCIA (.LIC) EN EL CLIENTE DEL SERVIDOR

Las claves de licencia se proporcionan junto con el nombre de usuario y la contraseña. Para **agregar/quitar** una clave de licencia, haga clic en el botón correspondiente de la ventana del administrador de licencias.

La clave de licencia es un archivo de texto que contiene información acerca del producto adquirido: su propietario, número de licencias y fecha de expiración.

1. Abrir ESET File Security.

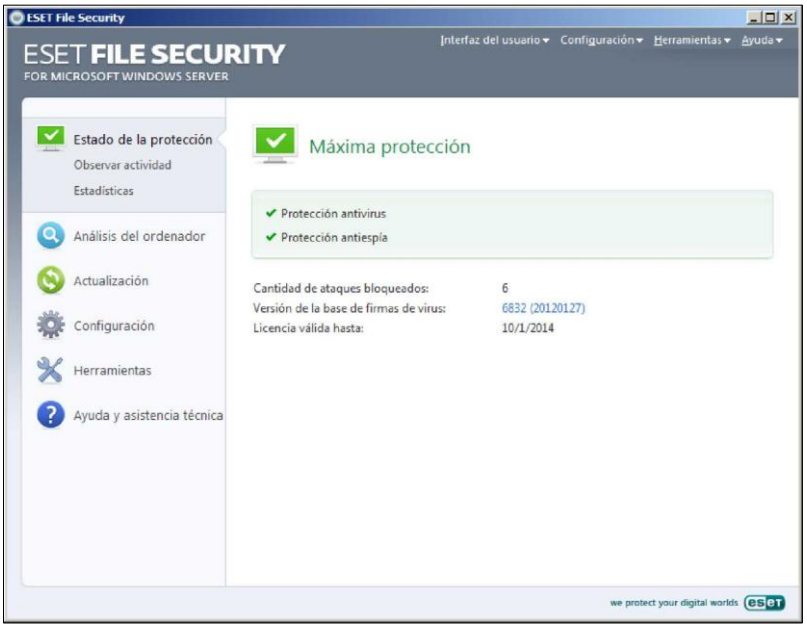

Fig. 1-1

2. En la Barra de menú, ubicada en la parte superior derecha, hacer click en ***CONFIGUARCIÓN*** o presionar en su teclado ***F5,*** para acceder a la configuración avanzada.

3. Puede acceder al administrador de licencias desde el árbol de configuración avanzada disponible debajo de **Varios** > **Licencias.**

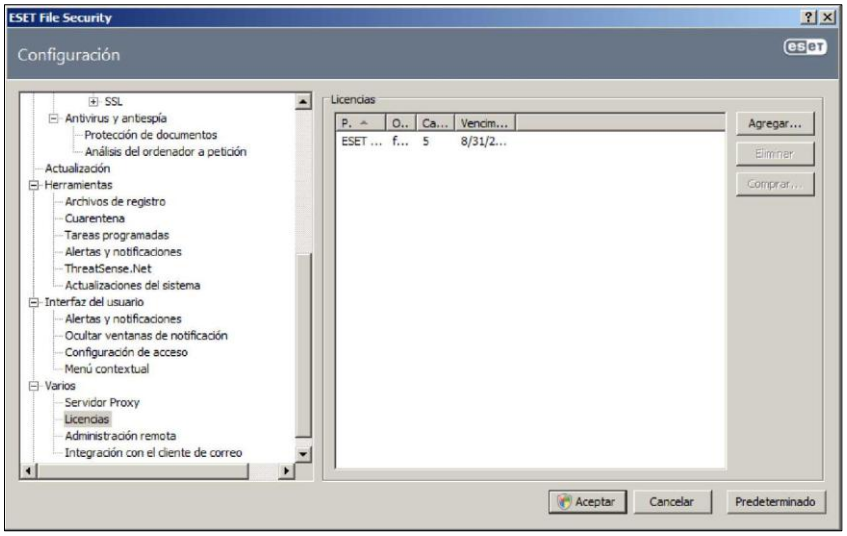

Fig. 1-2

La ventana del administrador de licencias le permite cargar y ver el contenido de una clave de licencia mediante el botón **Agregar,** de modo que puede ver su información en el administrador.

Al presionar el botón agregar… se debe buscar y seleccionar el archivo de licencia que se desea agregar. Una vez agregado el archivo de licencia se presiona el botón aceptar.

Para eliminar los archivos de licencia de la lista, seleccionar **Quitar.**

CREANDO EL ARCHIVO DE CONFIGURACIÓN (.XML) PARA LOS CLIENTES INSTALADOS EN LAS ESTACIONES DE TRABAJO Y/O LAPTOPS

¡IMPORTANTE!

Hay que tener en cuenta que, en la creación de este archivo de configuración que será utilizado únicamente en estaciones de trabajo y/o laptops, se deben hacer dos (2) veces las mismas configuraciones. La primera configuración se hace en la opción ***LÍNEA DE PRODUCTOS WINDOWS, VERSIONES 3 Y 4,*** luego se repiten las mismas configuraciones en la opción ***WINDOWS DESKTOP V5.***

A continuación se describen las configuraciones para la opción ***LÍNEA DE PRODUCTOS WINDOWS, VERSIONES 3 Y 4***

1. Abrir el Editor de configuraciones de ESET, presionar ***INICIO, TODOS LOS PROGRAMAS, ESET Y FINALMENTE EDITOR DE CONFIGURACIÓN DE ESET.***

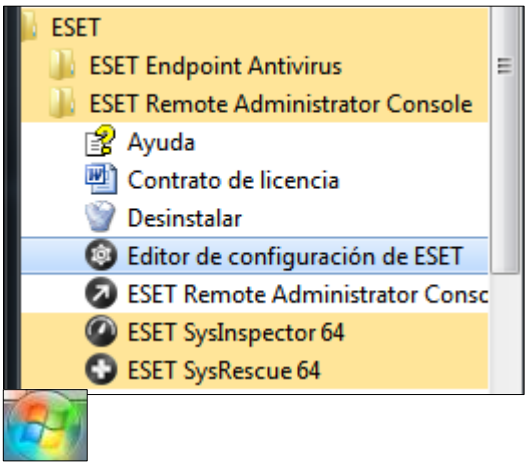

Fig. 1-1

2. En la siguiente ventana aparecerá el ***Editor de configuraciones de ESET***. Luego presionar el botón Nuevo.

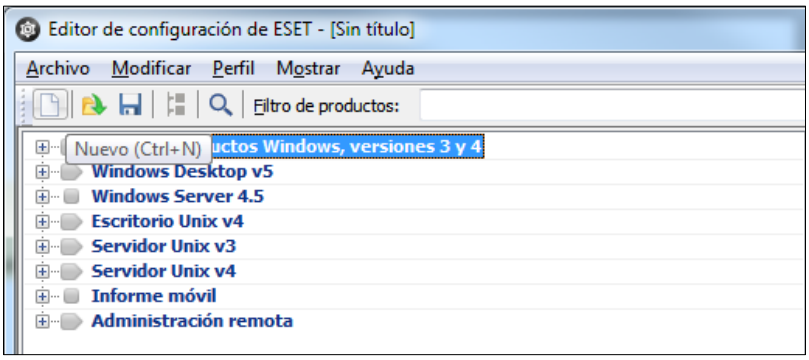

Fig. 1-2

3. Configuración de los Parámetros de ***Administración Remota***.

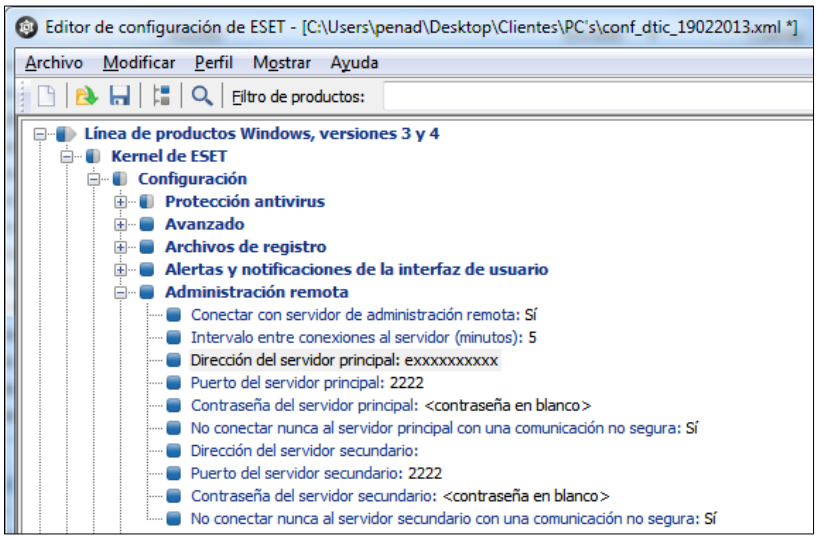

Fig. 1-3

Se deben desplegar las siguientes opciones:

- ***Línea de productos Windows, versiones 3 y 4***
  - ***Kernel***
    - ***Configuración***
      - ***Administración remota***

Opciones:

1. ***Conectar con el servidor de administración:*** seleccionar el Valor ***Sí/NO*** que se encuentra en la parte superior derecha, como se muestra a continuación.

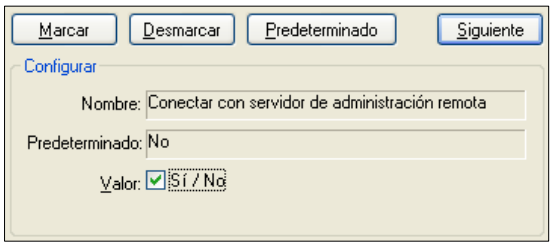

Fig. 1-4

1. ***Intervalo entre conexiones al servidor (en minutos)***, agregar el Valor de 5.

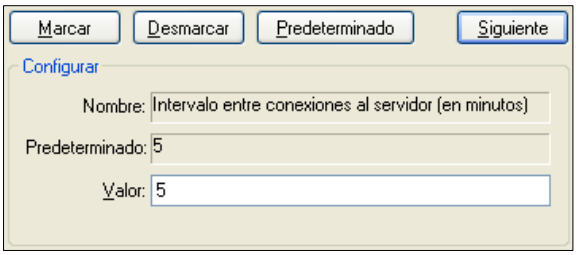

Fig. 1-5

2. ***Dirección del servidor principal: nombredelservidor*** donde se instaló la solución de antivirus.

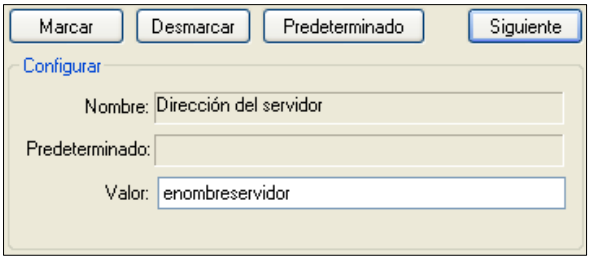

Fig. 1-6

3. ***Puerto del servidor principal: 2222***

4. ***Puerto del servidor secundario: 2222***

4. Configuración del Parámetro ***Proteger parámetros de configuración,*** esta opción permite proteger todas las configuraciones establecidas mediante una contraseña de acceso.

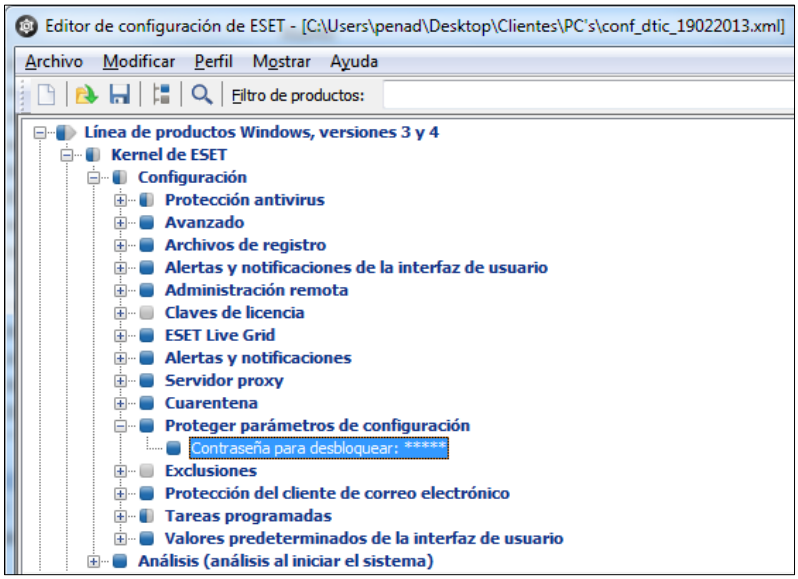

Fig. 1-7

Se deben desplegar las siguientes opciones:

- ***Línea de productos Windows, versiones 3 y 4***
  - ***Kernel***
    - ***Configuración***
      - ***proteger parámetros de configuración***

Se debe escribir una contraseña y confirmarla, como se muestra a continuación.

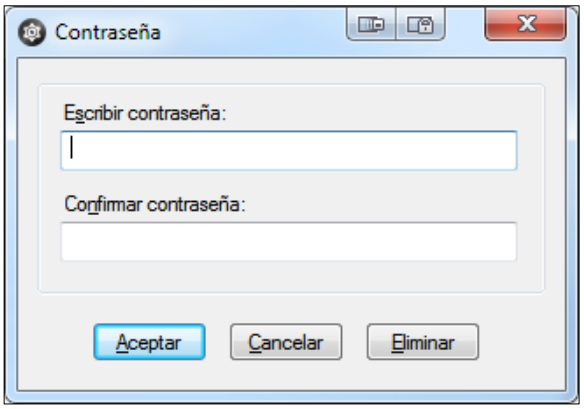

Fig. 1-8

Luego presionar el botón Aceptar.

Al seleccionar esta opción se debe colocar una contraseña que permita proteger el acceso a los parámetros de configuración del archivo que se está creando y que será importado más adelante en el cliente instalado en las estaciones de trabajo y/o laptops (ESET Endpoint Antivirus).

Esta contraseña deberá tener un ***mínimo de 8 caracteres***, entre los cuales se deben colocar ***MAYUSCULAS, MINUSCULAS, CARACTERES ESPECIALES y NUMEROS***

5. Configuración del Parámetro ***Tareas Programadas***

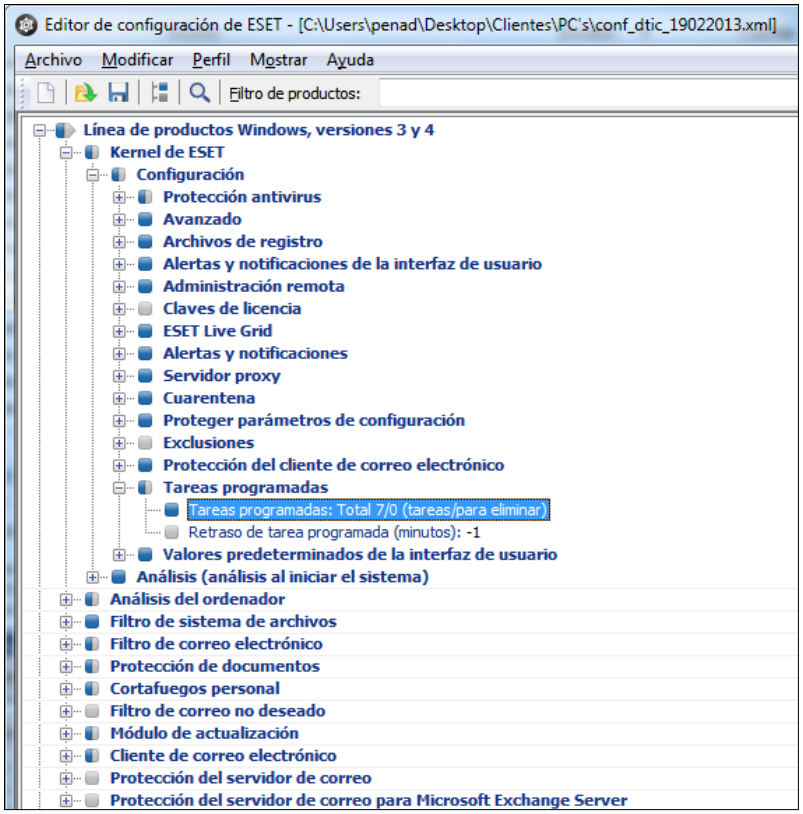

Fig. 1-9

Se debe desplegar las siguientes opciones:

- ***Línea de productos Windows, versiones 3 y 4***
  - ***Kernel***
    - ***Configuración***
      - ***Tareas Programadas***

En la ventana ***Programador de Tareas***, presionar el botón Agregar.

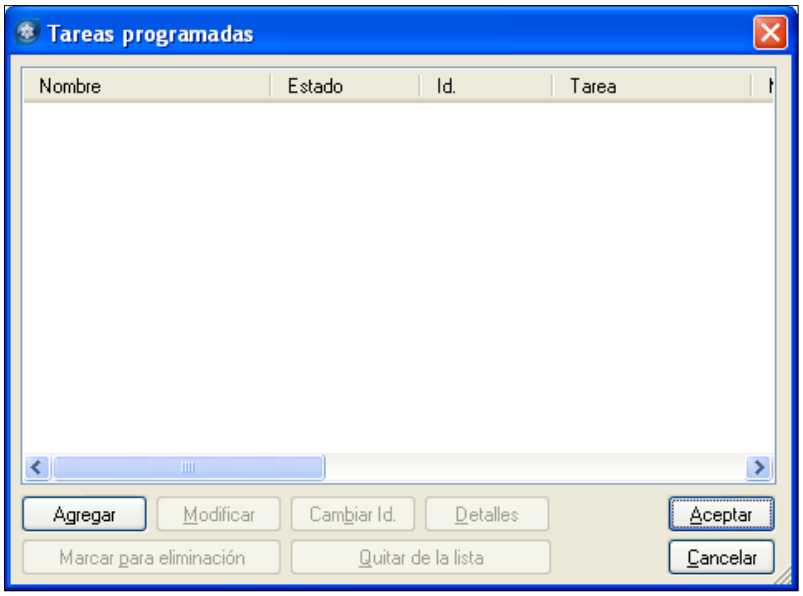

Fig. 1-10

En la ventana Agregar tarea, en la opción Tarea programada, seleccionar ***Análisis del equipo***, Luego presionar el botón Siguiente.

Fig. 1-11

En la siguiente ventana, en la opción Nombre de la tarea escribir ***Limpieza_Rutina***, y en la opción Ejecutar la tarea, seleccionar ***Semanalmente***, Luego presionar el botón Siguiente.

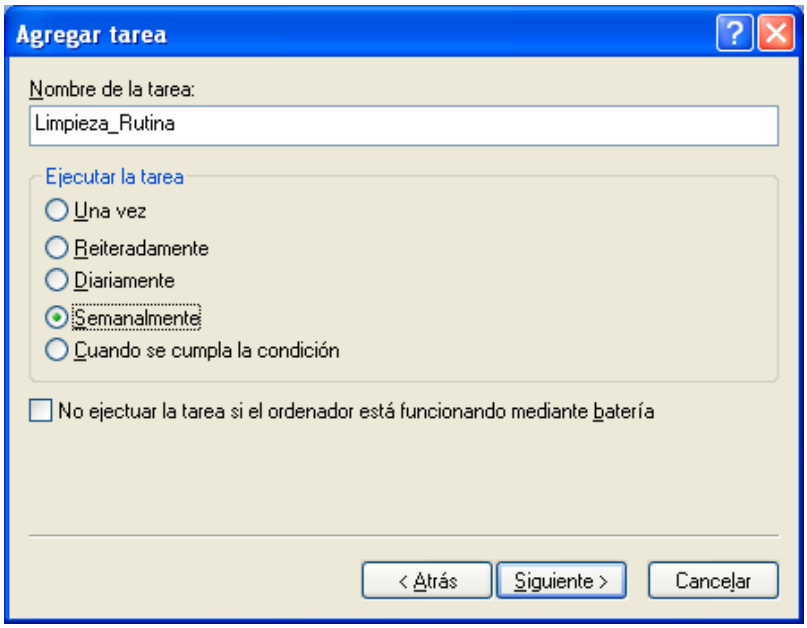

Fig. 1-12

Luego en la siguiente ventana, la opción Horario de ejecución de la tarea, el horario será ***12:05:00 p.m.,*** en la opción Ejecutar la tarea en los siguientes días, tildar ***Miércoles***, Luego presionar el botón Siguiente.

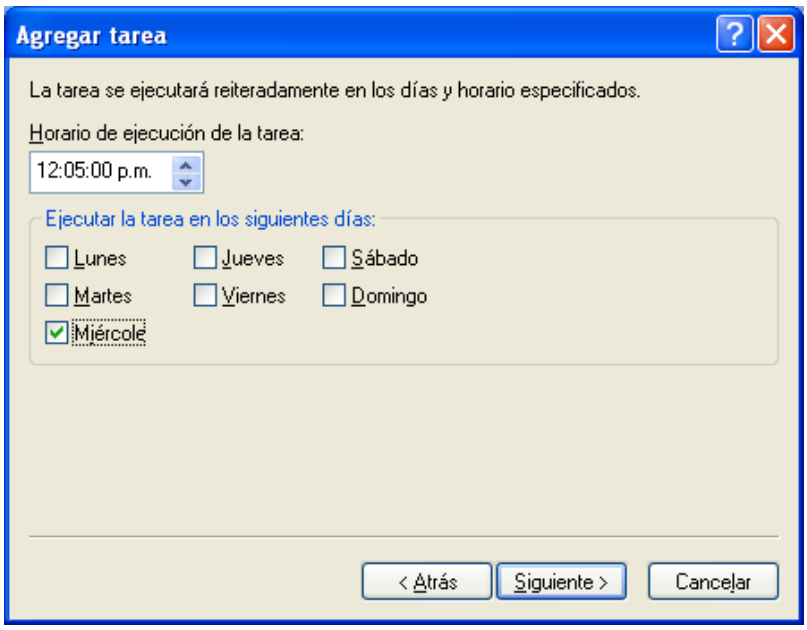

Fig. 1-13

***NOTA*: estas opciones pueden ser modificadas de acuerdo a los requerimientos y necesidades de cada Facultad, Dependencia Central o Extramuro.**

La próxima ventana, en la opción Si la tarea no se hubiera ejecutado, seleccionar ***Esperar hasta la próxima activación programada***, Luego presionar el botón Siguiente.

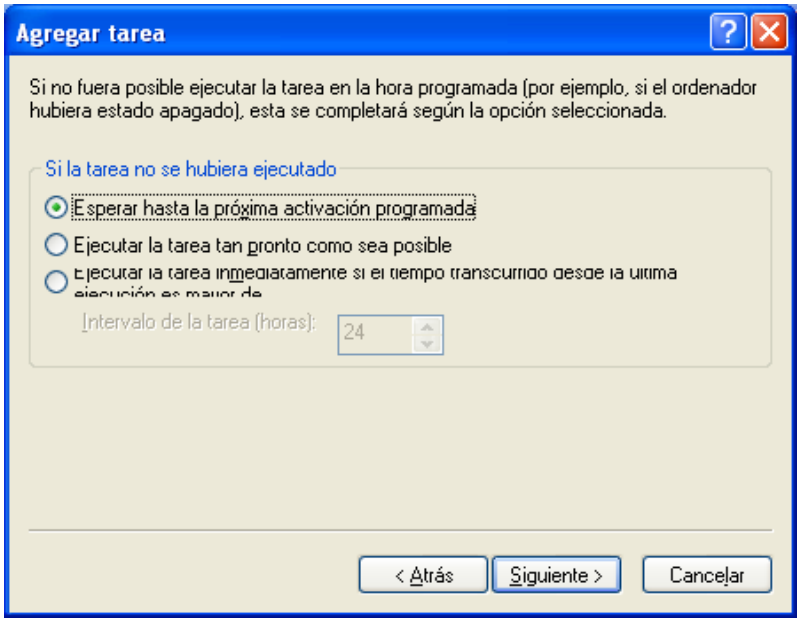

Fig. 1-14

Finalmente, se desplegará una ventana con la configuración suministrada anteriormente. Luego presionar el botón ***Finalizar***, para culminar con el proceso de configuración.

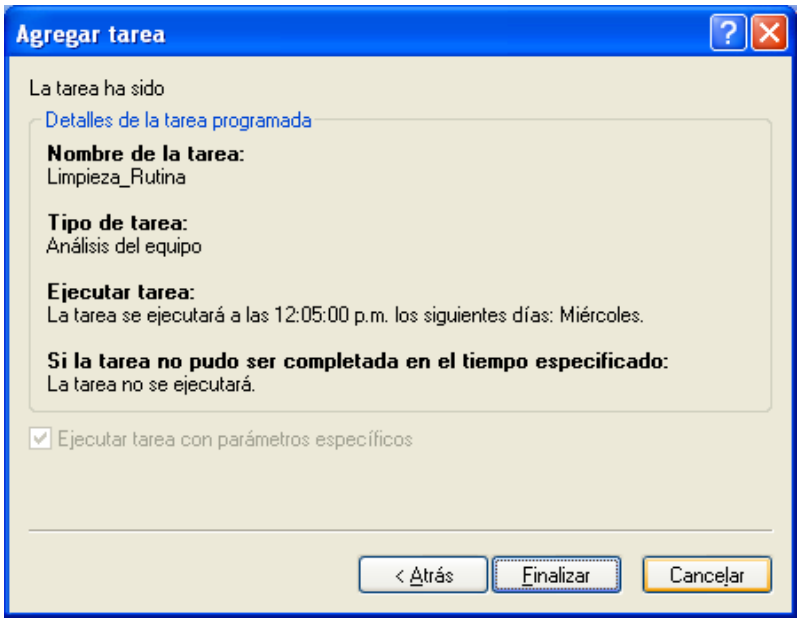

Fig. 1-15

En la ventana Configuración especial, en la opción Descripción escribir ***Limpieza_Rutina.***

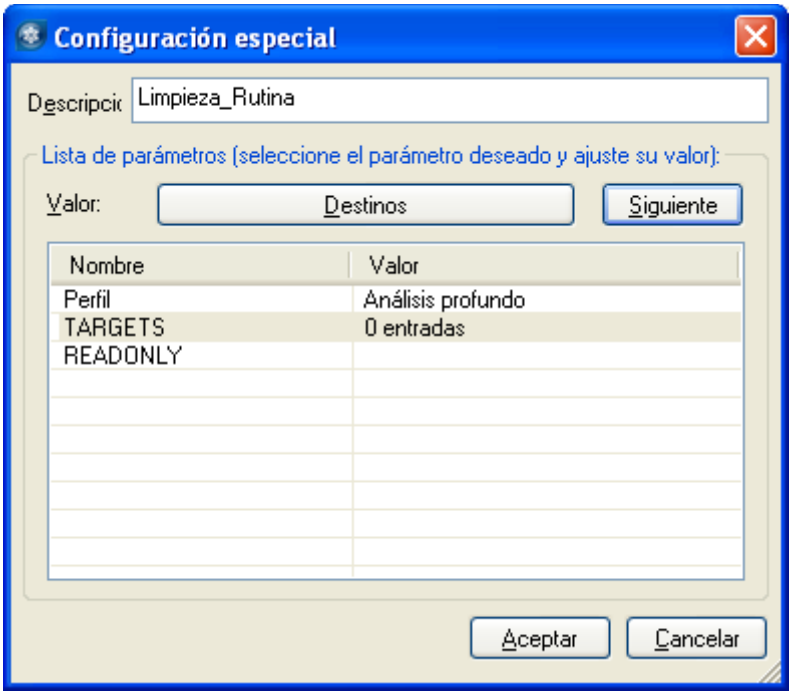

Fig. 1-16

En la misma ventana, seleccionar la opción ***TARGETS*** y luego presionar el botón ***Destinos***.

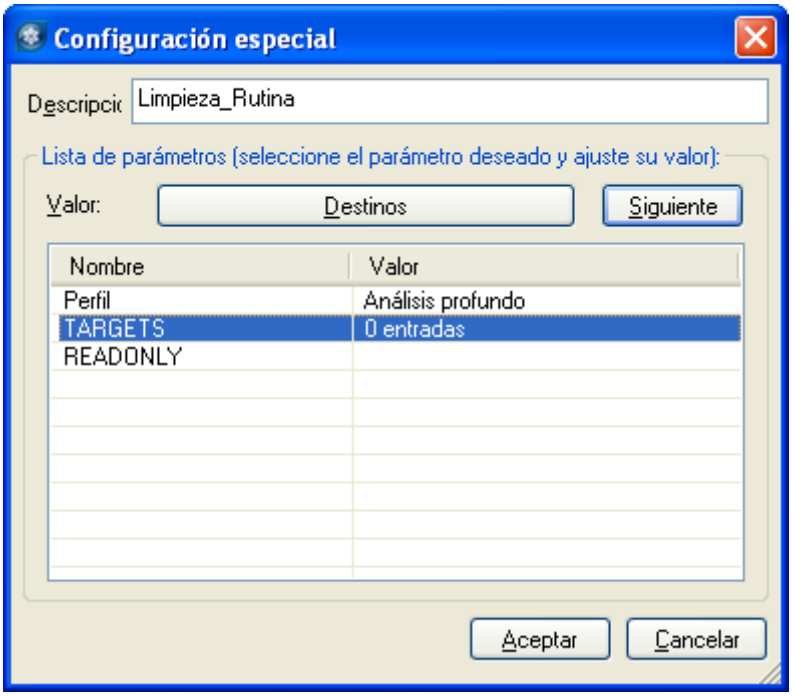

Fig. 1-17

En la ventana carpetas y archivos, presionar el botón ***+Unidades…***

Fig. 1-18

En la ventana Selección de destinos de análisis…, tildar ***Sectores de inicio de la unidad de disco duro*** y ***Unidades de disco duro***. Luego presionar el botón Aceptar.

Fig. 1-19

En la ventana carpetas y archivos, presionar el botón ***+Memoria...***, Luego presionar el botón Aceptar.

Fig. 1-20

Una vez que han sido configuradas las opciones de destino de análisis, se volverá a la ventana Configuración Especial, luego presionar el botón Aceptar.

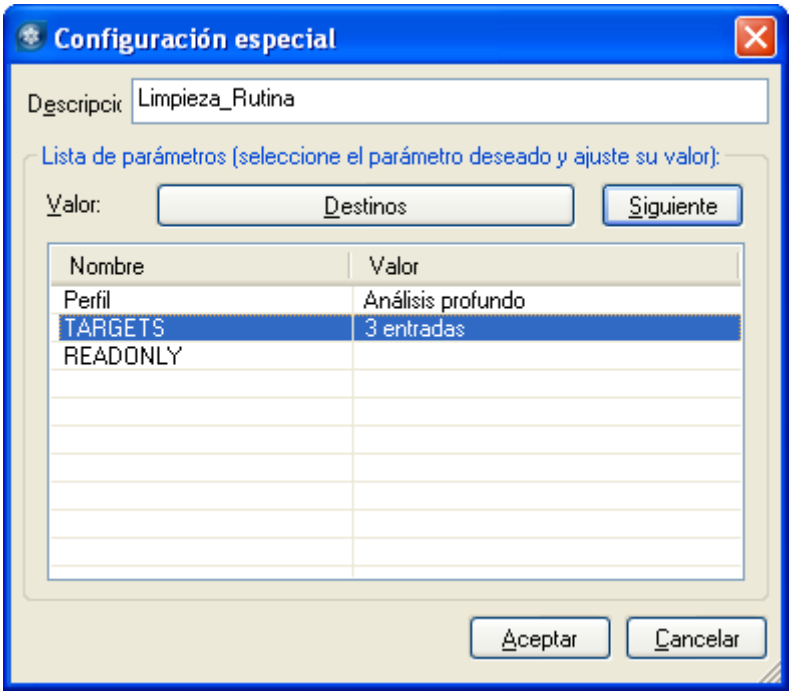

Fig. 1-21

Finalmente se mostrará en la ventana la tarea programada que se acaba de configurar, luego presionar el botón Aceptar.

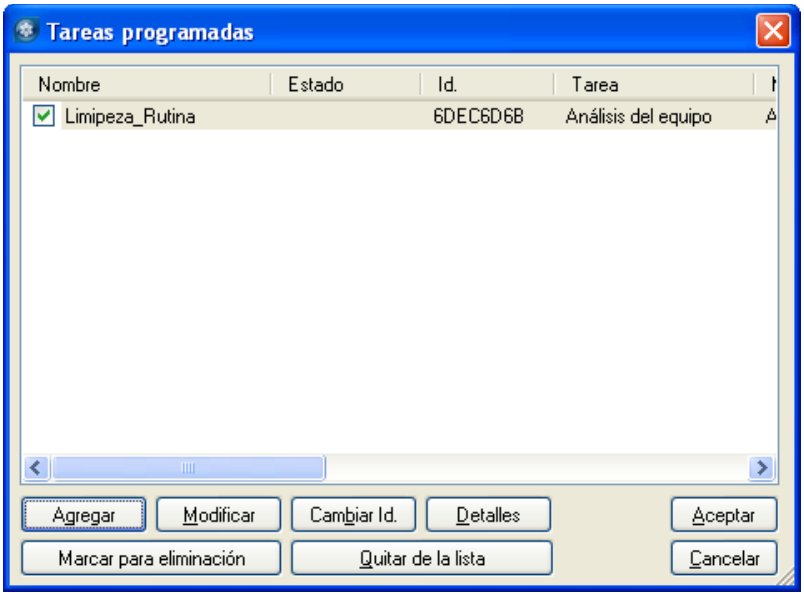

Fig. 1-22

6. Configuración de los Parámetros de ***Modulo de Actualización***

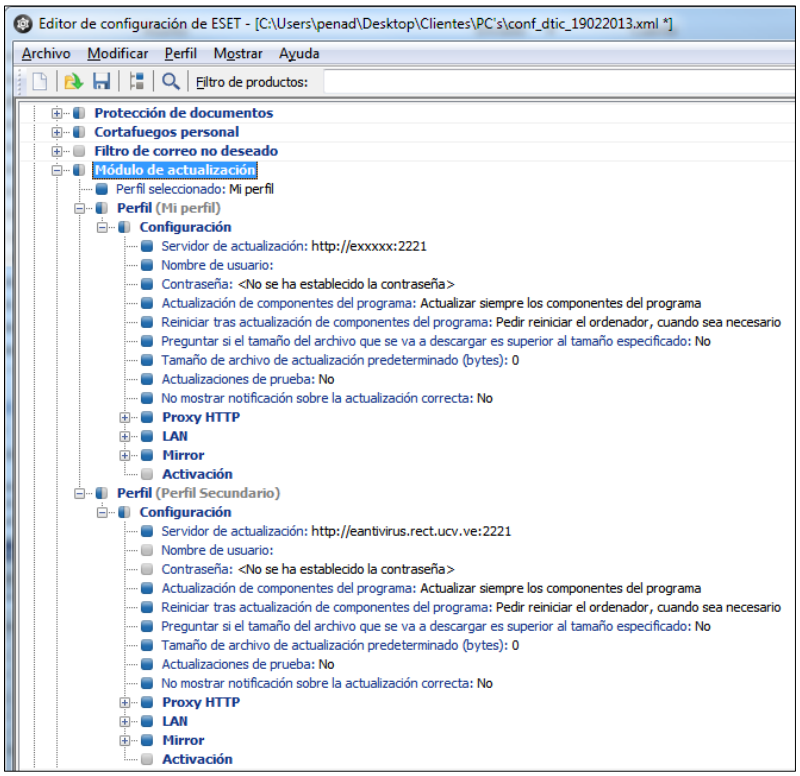

Fig. 1-23

Se deben desplegar las siguientes opciones:

- ***Línea de productos Windows, versiones 3 y 4***
  - ***Kernel***
    - ***Configuración***
      - ***Módulo de actualización***
        - ***Perfil***

En la opción **Servidor de actualización**, seleccionar el Valor <Servidor de actualización personalizada> y agregar el nombre del servidor (http://nombredelservidor:2221).

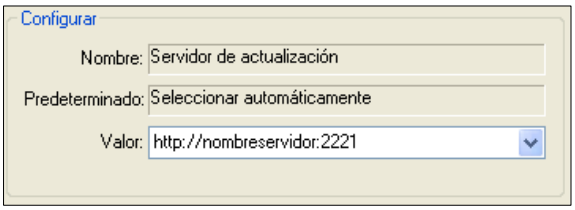

Fig. 1-24

Se debe ***agregar un segundo perfil de actualización***, para ello se hace click (DERECHO) sobre la opción perfil y se agrega uno nuevo con el nombre ***PERFIL SECUNDARIO***. Luego desplegar las opciones del nuevo perfil:

En el caso de que el archivo de configuración sea para estaciones de trabajo, las configuraciones del segundo perfil deben ser:

En la opción **Servidor de actualización**, seleccionar el Valor <Servidor de actualización personalizada> y agregar el nombre del servidor ***http://eantivirus.rect.ucv.ve:2221***.

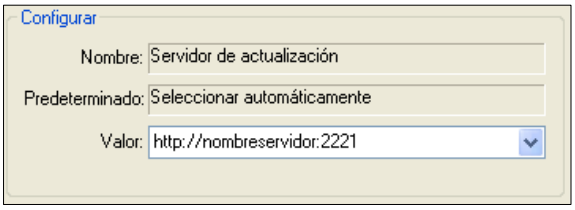

Fig. 1-25

En el caso de que el archivo de configuración sea para laptops, las configuraciones del segundo perfil deben ser:

- ***Perfil (Perfil Secundario)***
  - ***Servidor de Actualización: seleccionar Automáticamente***
  - ***Nombre de Usuario: EAV-00000000***
  - ***Contraseña:*** **********

<u>NOTA:</u> el nombre de usuario y contraseña se encuentran en la carpeta del archivo de licenciamiento en un archivo de texto (.txt)

A continuación se describen las configuraciones para la opción ***WINDOWS DESKTOP V5.***

1. Configuración de los Parámetros de ***Administración Remota***.

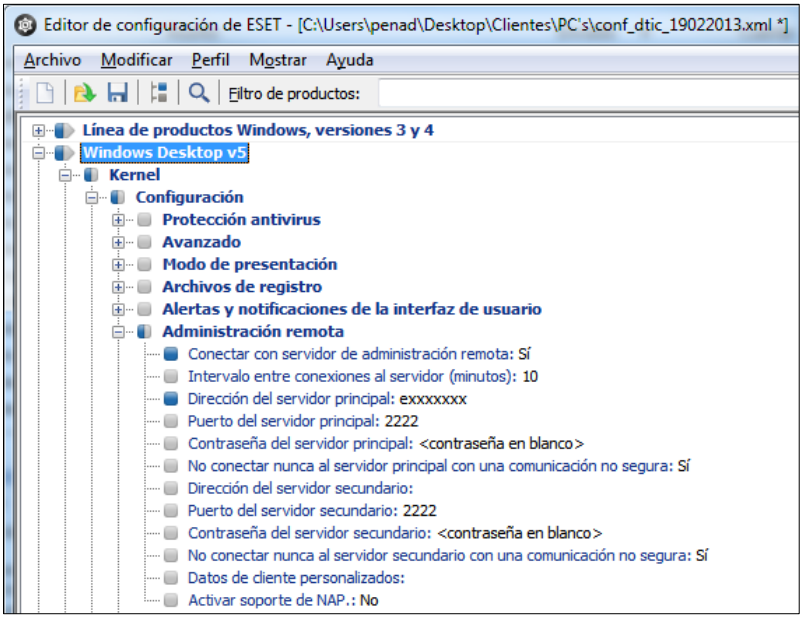

Fig. 1-26

Se deben desplegar las siguientes opciones:

- ***Windows Desktop v5***
  - ***Kernel***
    - ***Configuración***
      - ***Administración Remota***

Opciones:

1. ***Conectar con el servidor de administración:*** seleccionar el Valor ***Sí/NO*** que se encuentra en la parte superior derecha, como se muestra a continuación.

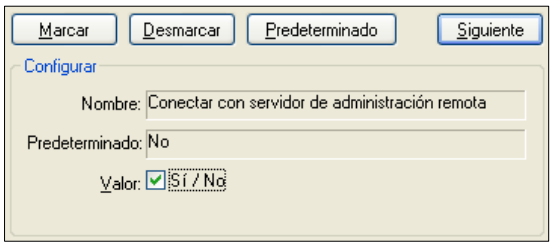

Fig. 1-27

2. ***Intervalo entre conexiones al servidor (en minutos)***, agregar el Valor de 5.

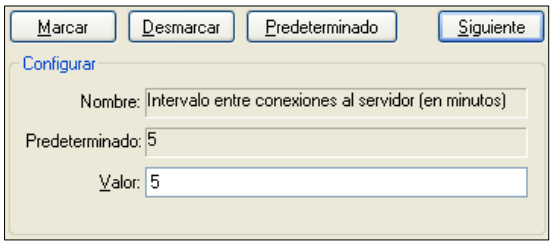

Fig. 1-28

3. ***Dirección del servidor principal: nombredelservidor*** donde se instaló la solución de antivirus.

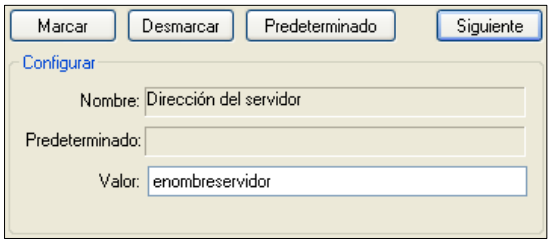

Fig. 1-29

4. ***Puerto del servidor principal: 2222***

5. ***Puerto del servidor secundario: 2222***

2. Configuración del Parámetro ***Proteger parámetros de configuración,*** esta opción permite proteger todas las configuraciones establecidas mediante una contraseña de acceso.

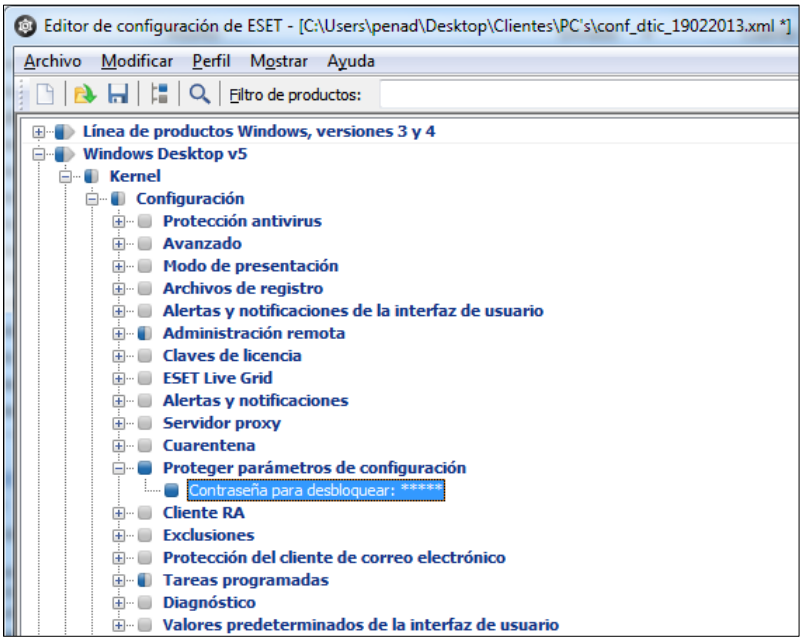

Fig. 1-30

Se deben desplegar las siguientes opciones:

- ***Windows Desktop v5***
  - ***Kernel***
    - ***Configuración***
      - ***Proteger parámetros de configuración***

Se debe escribir una contraseña y confirmarla, como se muestra a continuación.

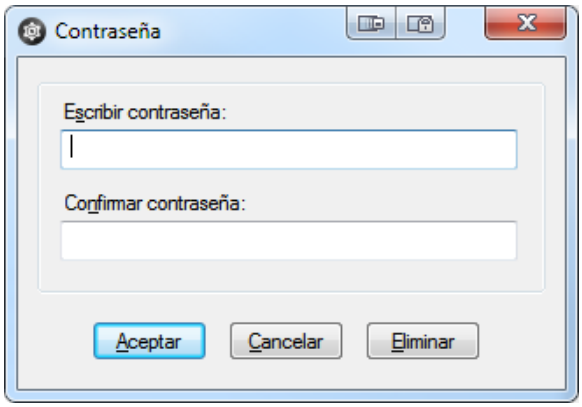

Fig. 1-31

Luego presionar el botón Aceptar.

Al seleccionar esta opción se debe colocar una contraseña que permita proteger el acceso a los parámetros de configuración del archivo que se está creando y que será importado más adelante en el cliente instalado en las estaciones de trabajo y/o laptops (ESET Endpoint Antivirus).

Esta contraseña deberá tener un ***mínimo de 8 caracteres***, entre los cuales se deben colocar ***MAYUSCULAS, MINUSCULAS, CARACTERES ESPECIALES y NUMEROS***

3. Configuración del Parámetro ***Tareas programadas***

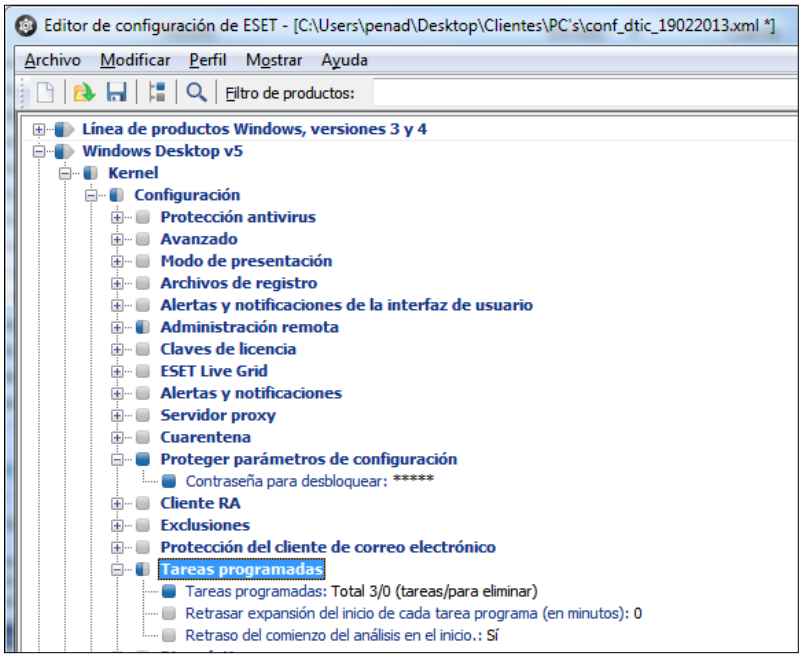

Fig. 1-32

Se debe desplegar las siguientes opciones:

- ***Windows Desktop v5***
  - ***Kernel***
    - ***Configuración***
      - ***Tareas Programadas***

En la ventana ***Tareas Programadas***, presionar el botón Agregar.

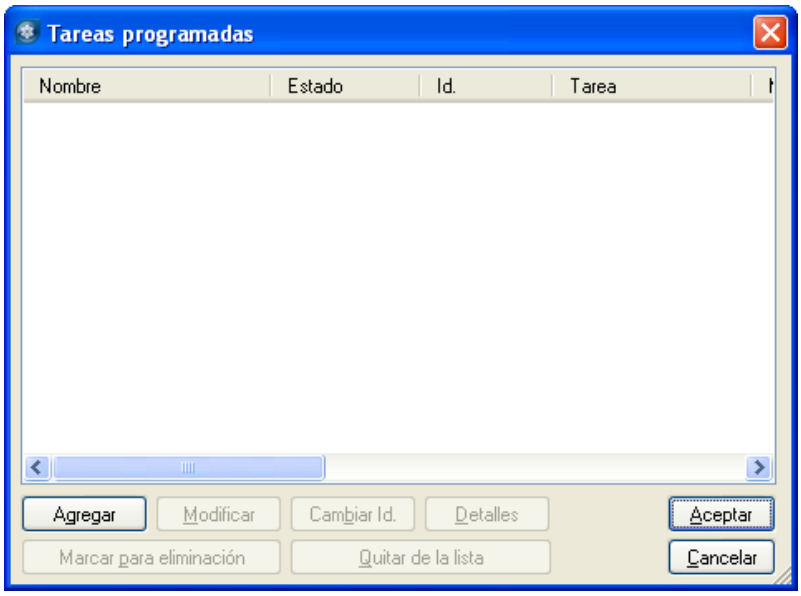

Fig. 1-33

En la ventana Agregar tarea, en la opción Tarea programada, seleccionar ***Análisis del equipo***, Luego presionar el botón Siguiente.

Fig. 1-34

En la siguiente ventana, en la opción Nombre de la tarea escribir ***Limpieza_Rutina***, y en la opción Ejecutar la tarea, seleccionar ***Semanalmente***, Luego presionar el botón Siguiente.

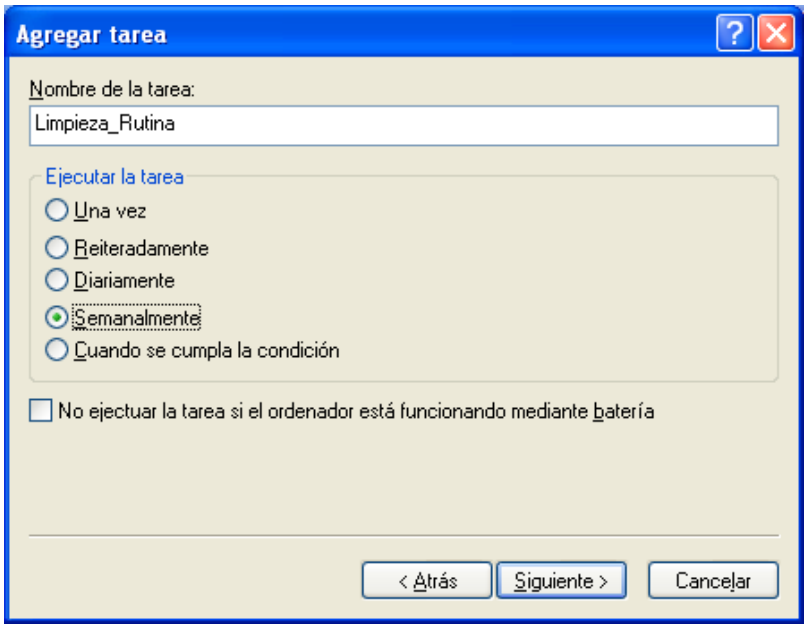

Fig. 1-35

Luego en la siguiente ventana, la opción Horario de ejecución de la tarea, el horario será ***12:05:00 p.m.,*** en la opción Ejecutar la tarea en los siguientes días, tildar ***Miércoles***, Luego presionar el botón Siguiente.

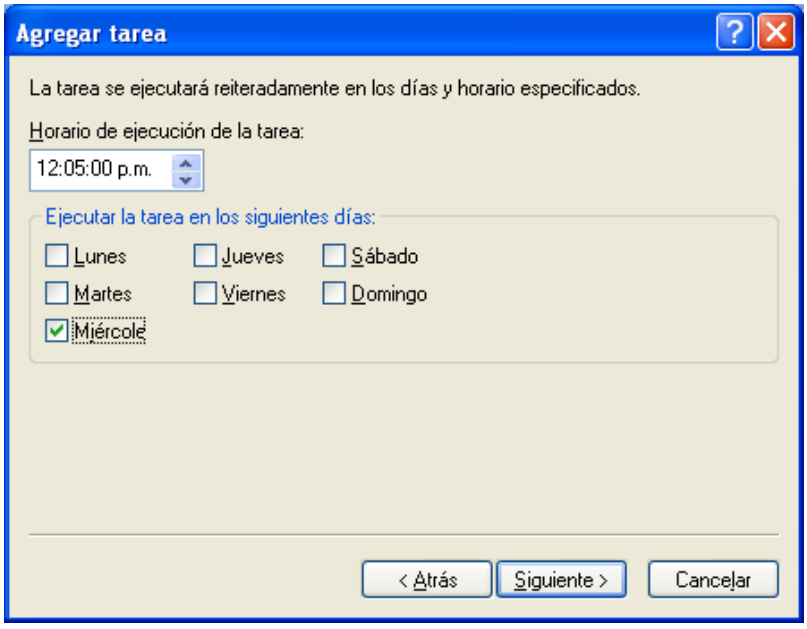

Fig. 1-36

***NOTA*: estas opciones pueden ser modificadas de acuerdo a los requerimientos y necesidades de cada Facultad, Dependencia Central o Extramuro.**

La próxima ventana, en la opción Si la tarea no se hubiera ejecutado, seleccionar ***Esperar hasta la próxima activación programada***, Luego presionar el botón Siguiente.

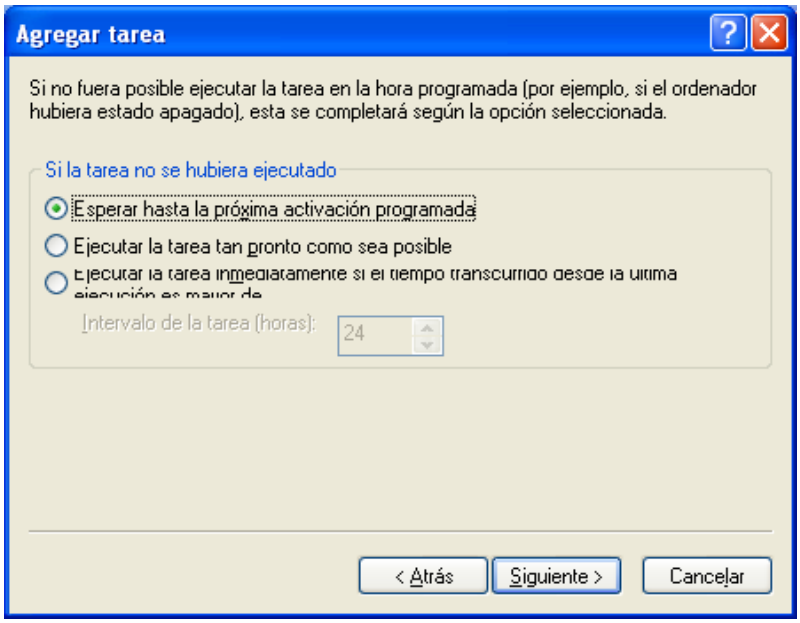

Fig. 1-37

Finalmente, se desplegará una ventana con la configuración suministrada anteriormente. Luego presionar el botón ***Finalizar***, para culminar con el proceso de configuración.

Fig. 1-38

En la ventana Configuración especial, en la opción Descripción escribir ***Limpieza_Rutina.***

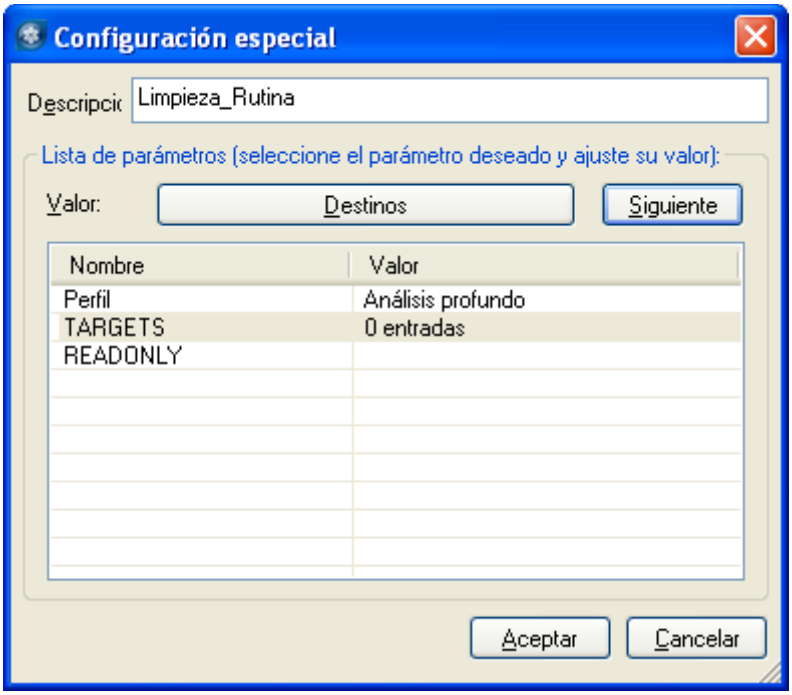

Fig. 1-39

En la misma ventana, seleccionar la opción ***TARGETS*** y luego presionar el botón ***Destinos***.

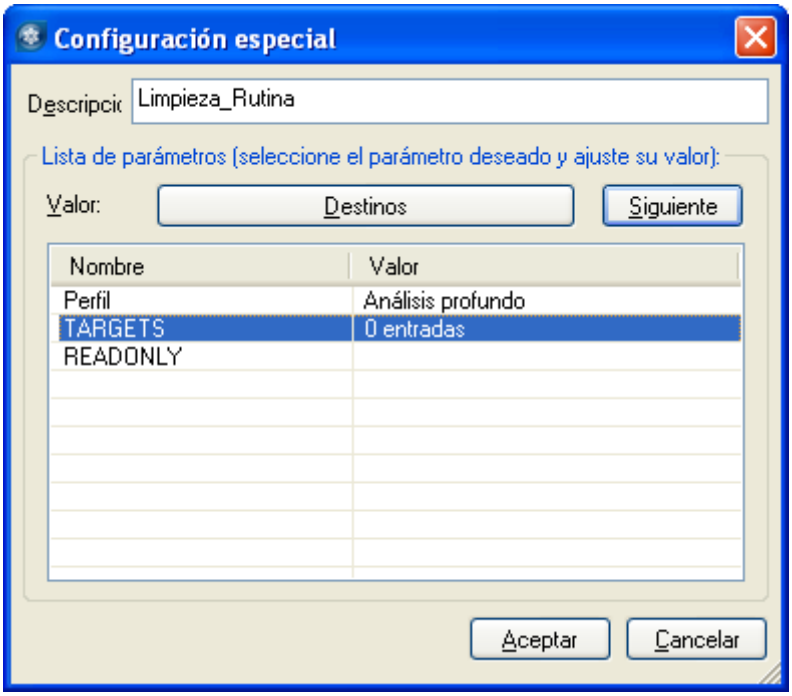

Fig. 1-40

En la ventana carpetas y archivos, presionar el botón ***+Unidades…***

Fig. 1-41

En la ventana Selección de destinos de análisis…, tildar ***Sectores de inicio de la unidad de disco duro*** y ***Unidades de disco duro***. Luego presionar el botón Aceptar.

Fig. 1-42

En la ventana carpetas y archivos, presionar el botón ***+Memoria...***, Luego presionar el botón Aceptar.

Fig. 1-43

Una vez que han sido configuradas las opciones de destino de análisis, se volverá a la ventana Configuración Especial, luego presionar el botón Aceptar.

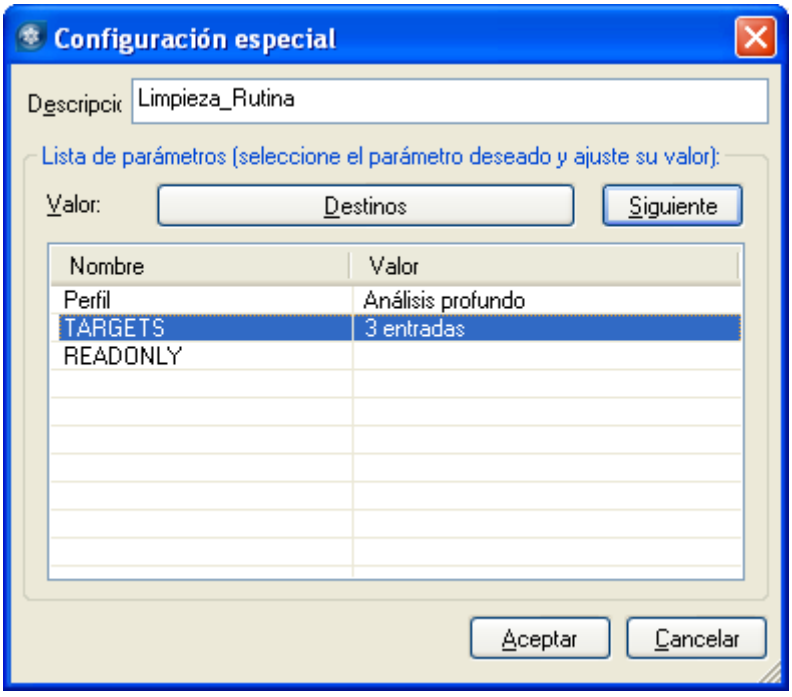

Fig. 1-44

Finalmente se mostrará en la ventana la tarea programada que se acaba de configurar, luego presionar el botón Aceptar.

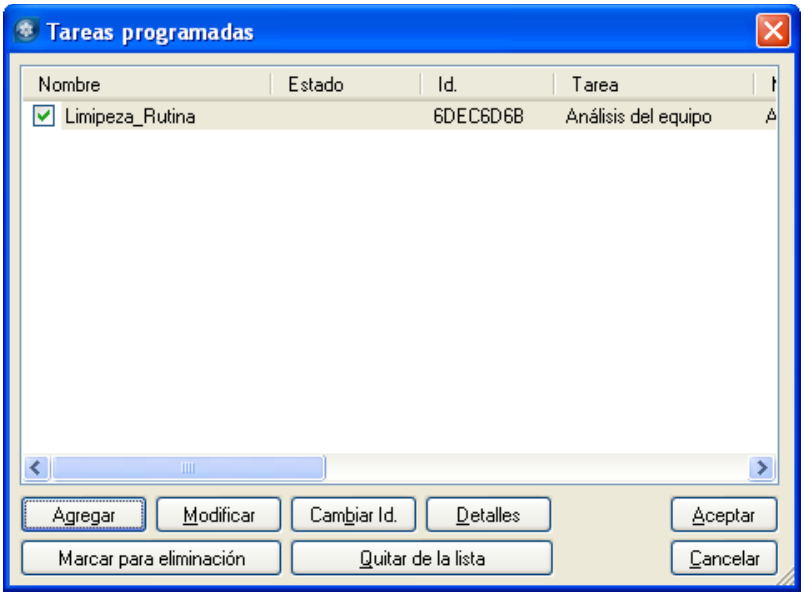

Fig. 1-45

4. Configuración de los Parámetros de ***Actualizar***

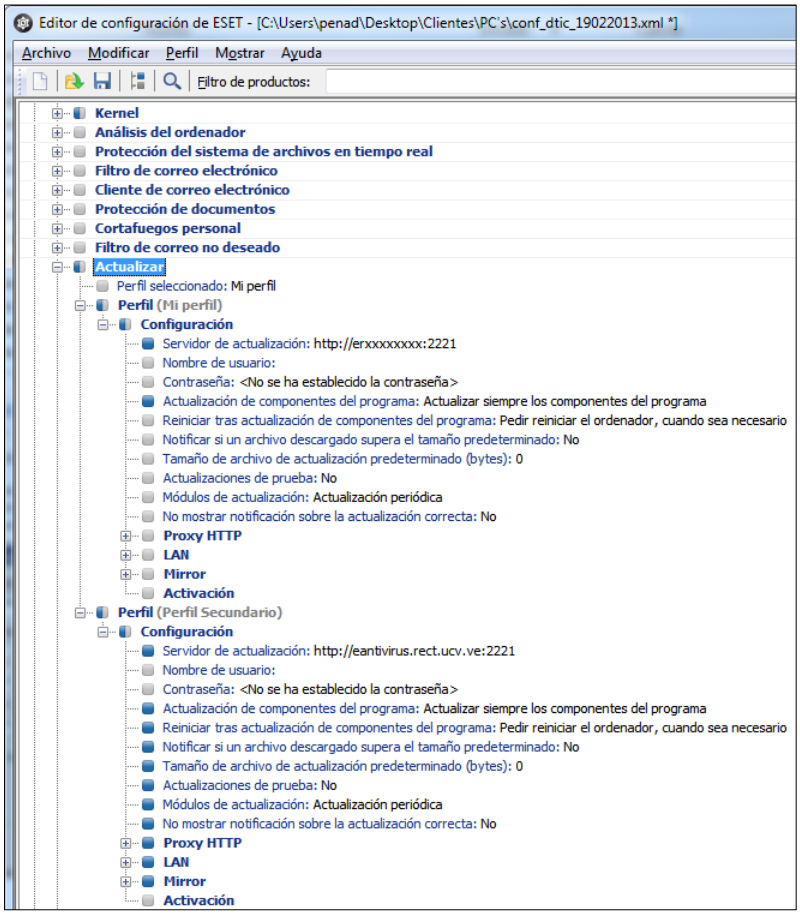

Fig. 1-46

Se deben desplegar las siguientes opciones:

- ***Windows Desktop v5***
  - ***Kernel***
    - ***Configuración***
      - ***Actualizar***
        - ***Perfil***

En la opción **Servidor de actualización**, seleccionar el Valor <Servidor de actualización personalizada> y agregar el nombre del servidor (http://nombredelservidor:2221).

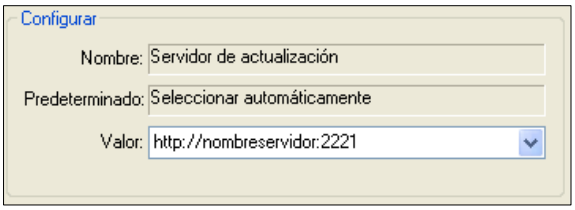

Fig. 1-47

Se debe ***agregar un segundo perfil de actualización***, para ello se hace click (DERECHO) sobre la opción perfil y se agrega uno nuevo con el nombre ***PERFIL SECUNDARIO***. Luego desplegar las opciones del nuevo perfil:

En el caso de que el archivo de configuración sea para estaciones de las trabajo, las configuraciones del segundo perfil deben ser:

En la opción **Servidor de actualización**, seleccionar el Valor <Servidor de actualización personalizada> y agregar el nombre del servidor ***http://eantivirus.rect.ucv.ve:2221***.

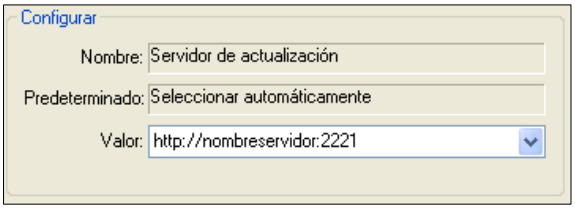

Fig. 1-48

En el caso de que el archivo de configuración sea para laptops, las configuraciones del segundo perfil deben ser:

- ***Perfil (Perfil Secundario)***
    - ***Servidor de Actualización: seleccionar Automáticamente***
    - ***Nombre de Usuario: EAV-00000000***
    - ***Contraseña:*************

NOTA: el nombre de usuario y contraseña se encuentran en la carpeta del archivo de licenciamiento en un archivo de texto (.txt)

Finalmente, se procede a guardar el archivo de configuración para su posterior uso.

En el caso que se haya creado el archivo de configuración para estaciones de trabajo debe de ser guardado con la siguiente estructura en el nombre:

- ***conf_nombredelservidor_desktop_díamesaño***.

En el caso que se haya creado el archivo de configuración para estaciones de trabajo debe de ser guardado con la siguiente estructura en el nombre:

- ***conf_nombredelservidor_laptops_díamesaño***.

INSTALANDO ESET ENDPOINT ANTIVIRUS PARA CLIENTES PC'S Y LAPTOPS

¡Importante!

Antes de realizar la instalación Verifique la versión de su sistema operativo.

Cualquier solución de antivirus instalada previamente en su equipo debe ser desinstalada antes de comenzar con la instalación de su producto ESET.

1. Para comenzar la instalación, haga doble clic en el ícono del instalador que guardó en el Escritorio. Si Windows le solicita Abrir/Ejecutar el archivo, presione Abrir/Ejecutar.

Fig. 1-1

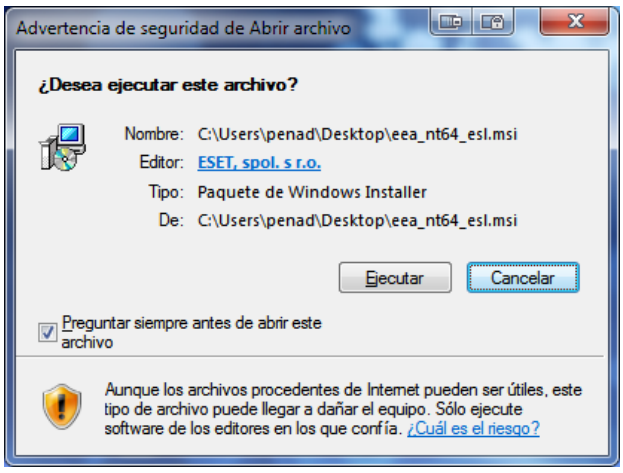

Fig. 1-2

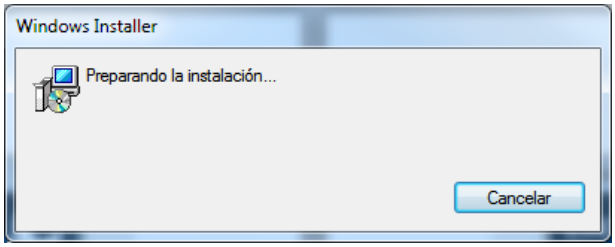

Fig. 1-3

2. En la siguiente ventana aparecerá la ventana del Asistente de configuración de ESET Endpoint Antivirus. Luego presione Siguiente.

Fig. 1-4

3. En la ventana Acuerdo de licencia de usuario final, seleccione la opción ***Acepto las condiciones del acuerdo de licencia,*** para aceptar el acuerdo de licencia de ESET Endpoint Antivirus. Luego presione Siguiente.

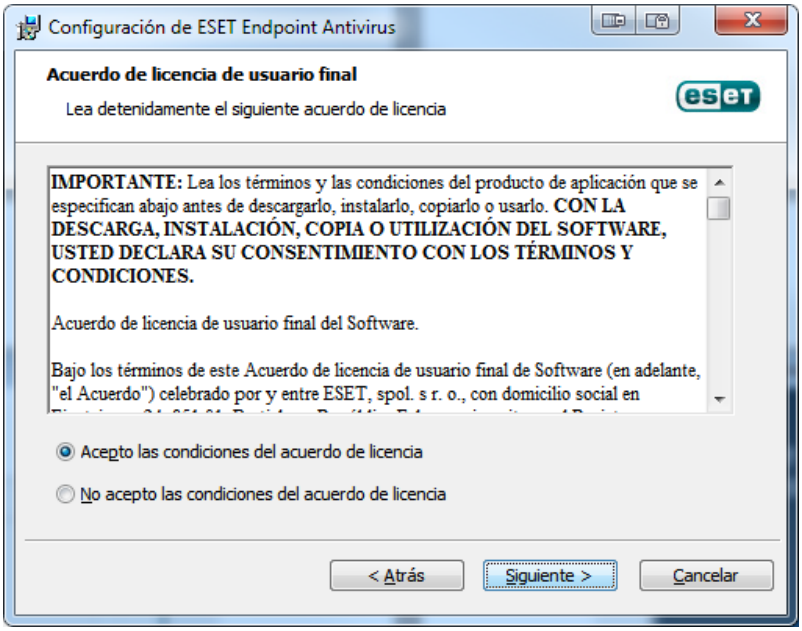

Fig. 1-5

4. En la ventana Modo de instalación, seleccione la opción ***Personalizada (permite una configuración más detallada)*** y luego presione Siguiente.

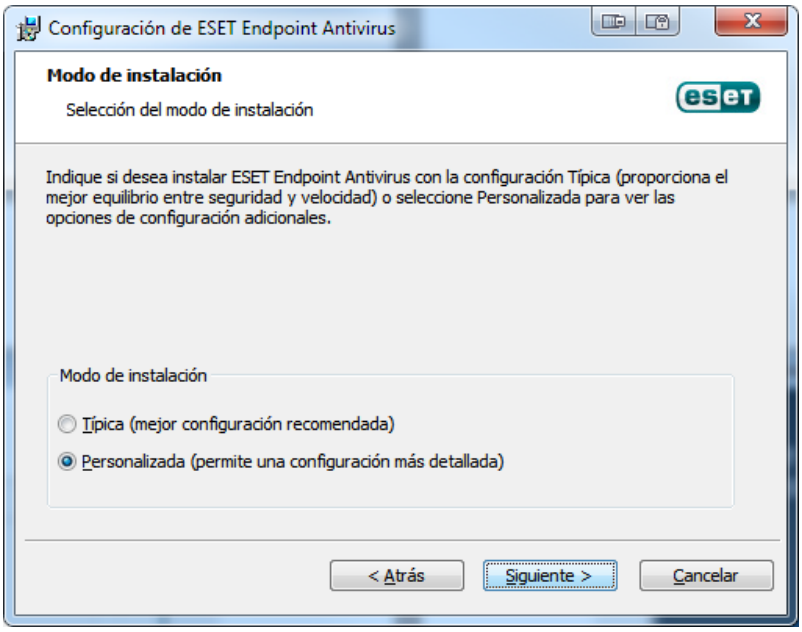

Fig. 1-6

5. En la ventana Seleccionar la carpeta para la instalación, se mostrara ***la carpeta y ruta donde será instalado el Antivirus***. Luego presione Siguiente.

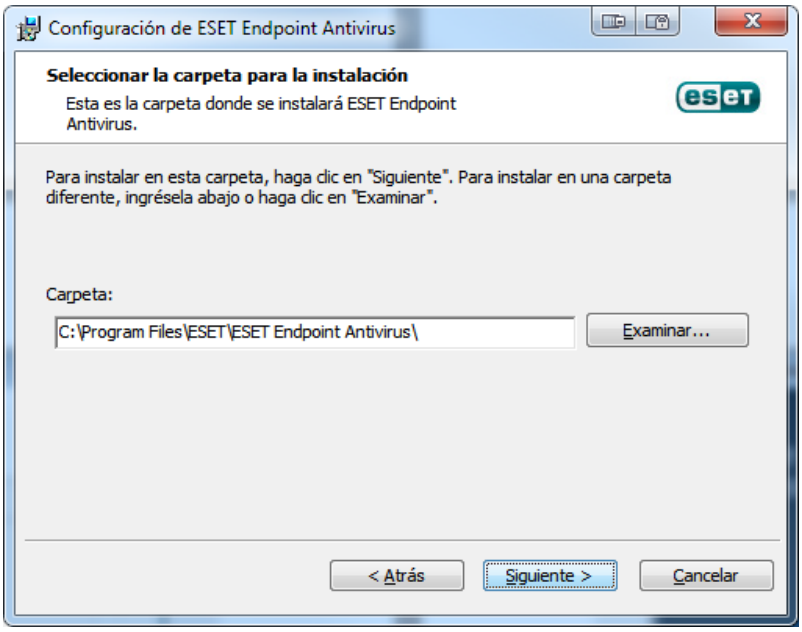

Fig. 1-7

6. En la ventana Actualización automática, tilde la opción ***Establecer los parámetros de actualización luego***. Luego presione Siguiente.

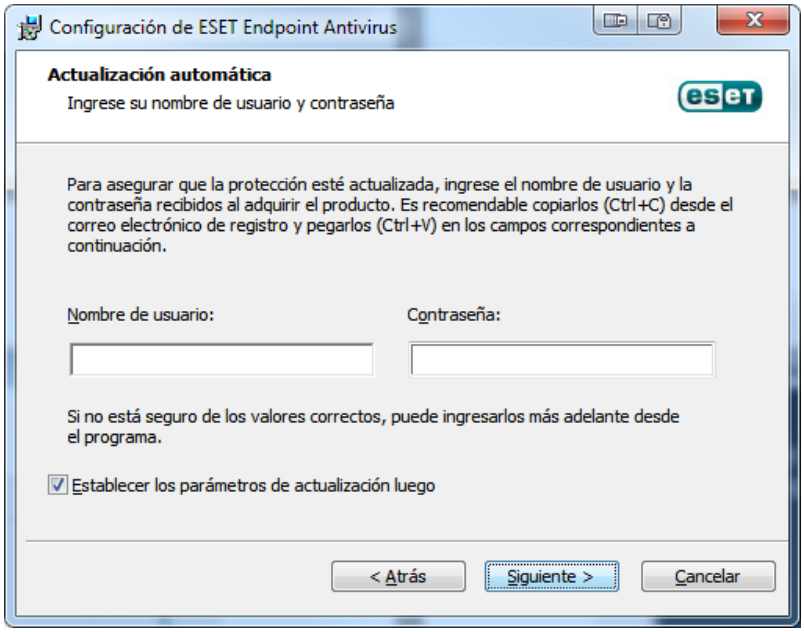

Fig. 1-8

7. En la ventana Conexión a Internet, se mostraran las opciones para configurar la conexión a internet. Seleccione la opción ***Desconozco si mi conexión a Internet usa un servidor proxy… (Recomendado)***. Luego Presione Siguiente.

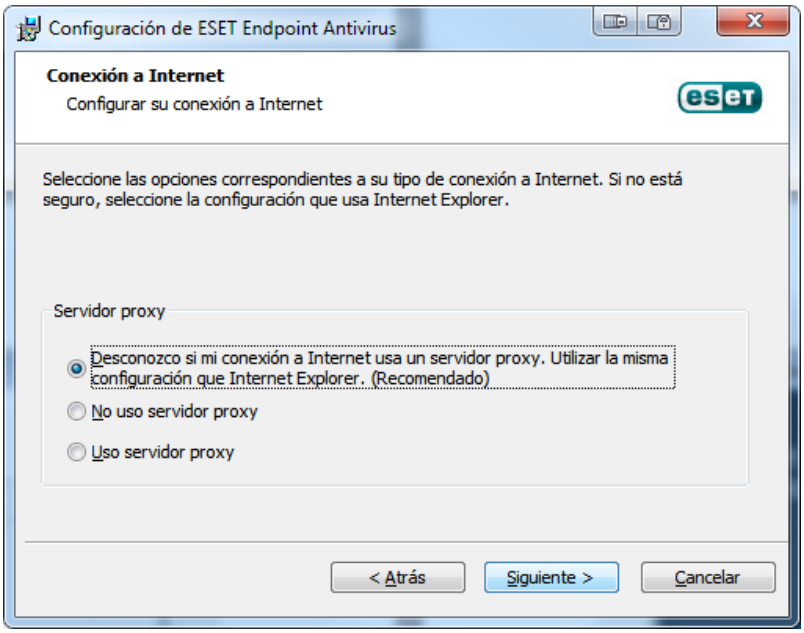

Fig. 1-9

8. En la ventana Actualización automática, se mostraran las opciones para configurar el tipo de actualización del ESET Endpoint Antivirus. Presione ***Cambiar…***

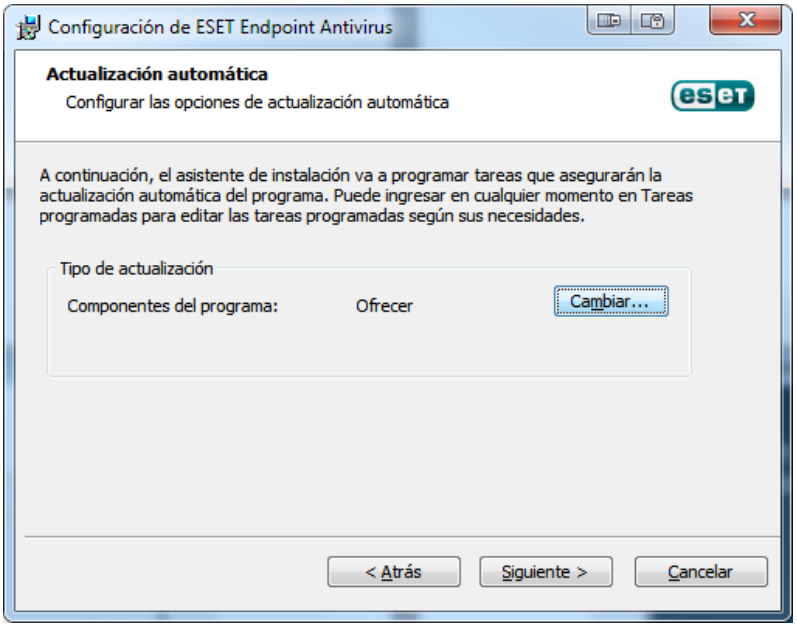

Fig. 1-10

9. Se mostrara la siguiente pantalla, donde se deben seleccionar las opciones ***Siempre actualizar los componentes del programa*** y ***Ofrecer Reiniciar el equipo si es necesario***. Luego presione Aceptar.

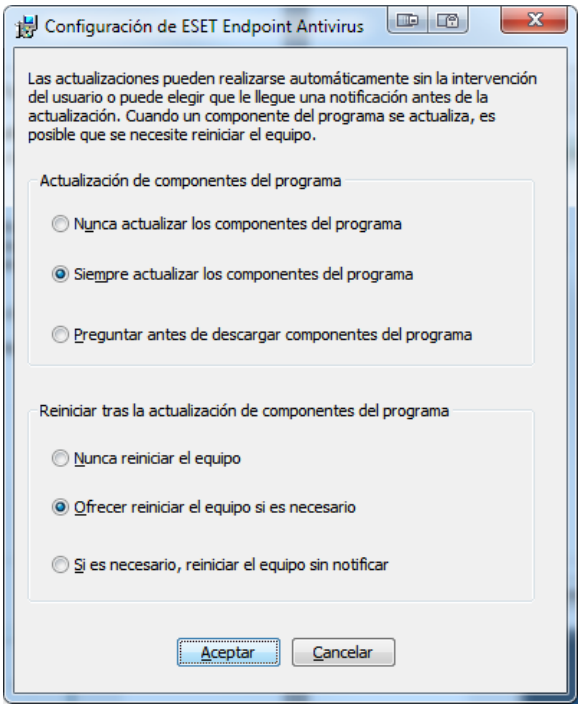

Fig. 1-11

10. En la ventana Configuración de la protección por contraseña, ***no se realiza ningún cambio.*** Luego presione Siguiente.

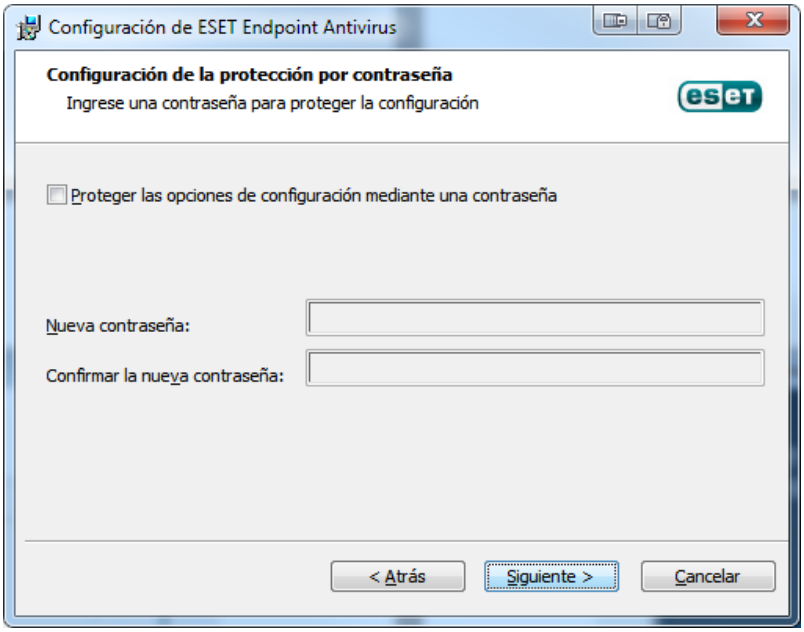

Fig. 1-12

11. En la ventana ESET Live Grid, tilde la opción ***Acepto participar en ESET Live Grid (recomendado)***. Luego presione Siguiente.

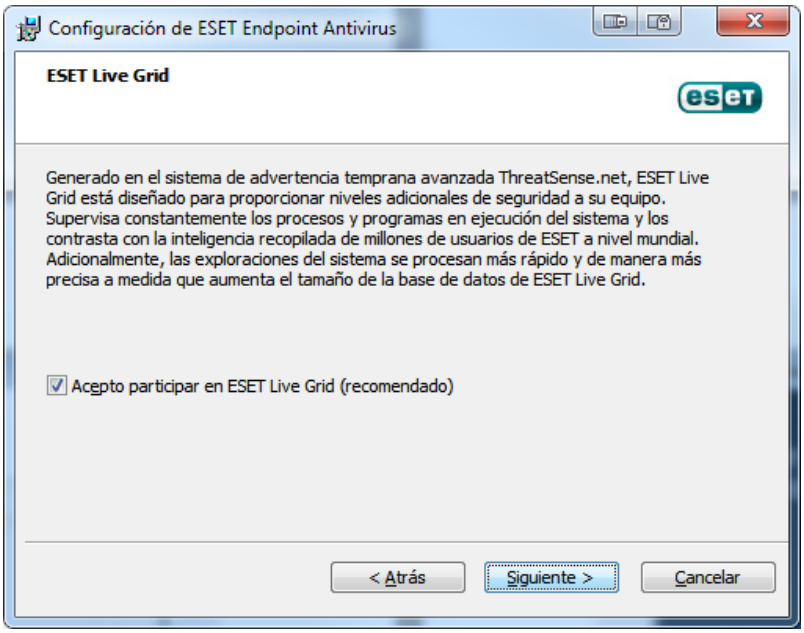

Fig. 1-13

12. En la ventana Detección de aplicaciones potencialmente no deseadas, seleccione la opción ***Habilitar la detección de aplicaciones potencialmente no deseadas***…

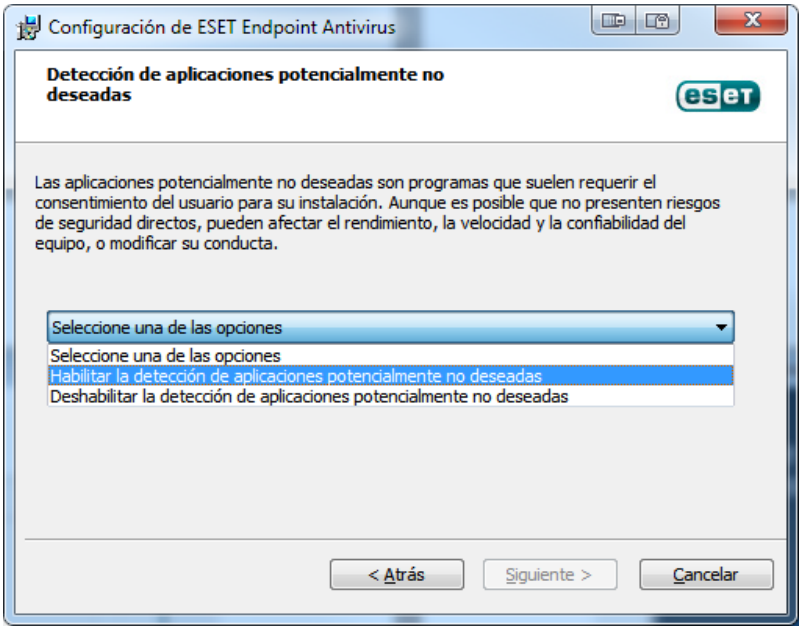

Fig. 1-14

13. Ventana con la opción ***Habilitar la detección de aplicaciones potencialmente no deseadas*** *seleccionada.* Luego presione Siguiente.

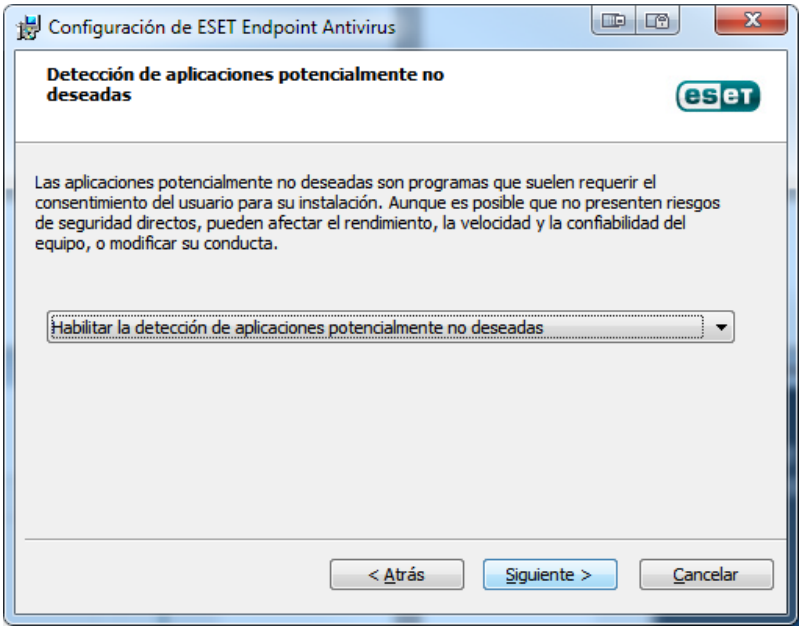

Fig. 1-15

14. En la ventana Preparado para instalar, presione ***Instalar*** para comenzar la instalación de ESET

Fig. 1-16

15. Ventana Instalando ESET Endpoint Antivirus. Esperar que finalice el proceso de instalación.

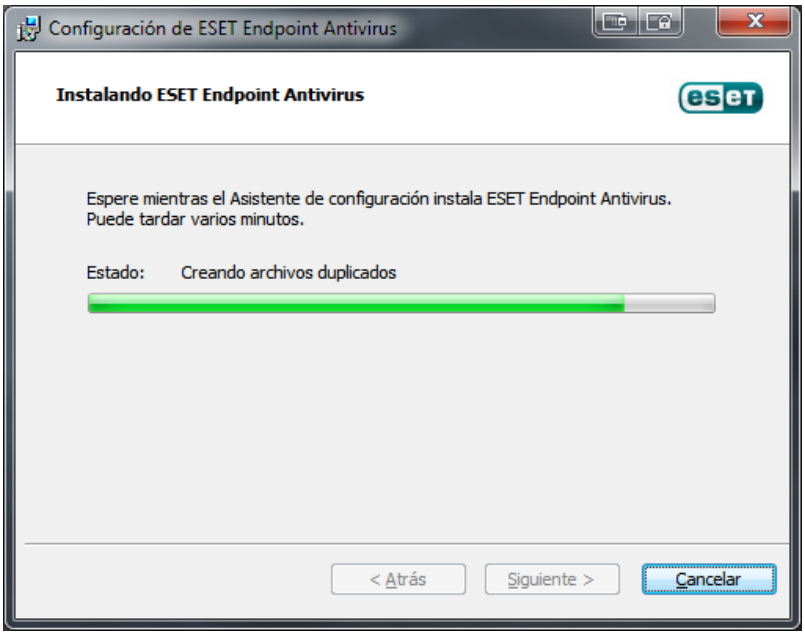

Fig. 1-17

16. Cuando se visualice la ventana Completando el Asistente de configuración de ESET Endpoint Antivirus haga clic en ***Finalizar***.

Fig. 1-18

17. Una vez finalizado correctamente el proceso de Instalación de ESET Endpoint Antivirus, aparecerá el icono en la barra de tareas.

Fig. 1-19

CARGANDO EL ARCHIVO DE CONFIGURACIÓN (.XML) EN EL CLIENTE ANTIVIRUS DE LAS ESTACIONES DE TRABAJO O LAPTOPS.

1. Abrir ESET Endpoint Antivirus.

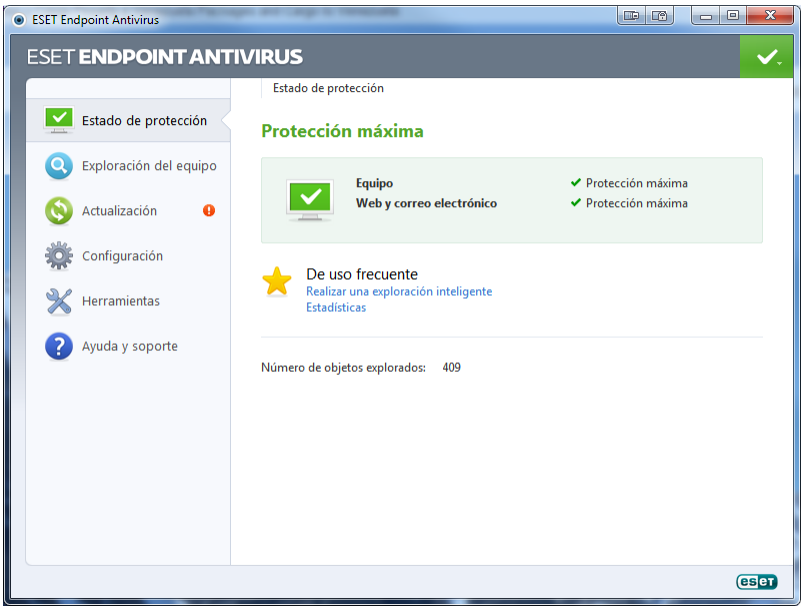

Fig. 1-1

2. En la ventana principal del ESET Endpoint Antivirus, en el panel de opciones ubicado en el lado izquierdo, presionar ***Configuración*** → ***Importar o exportar la configuración…***

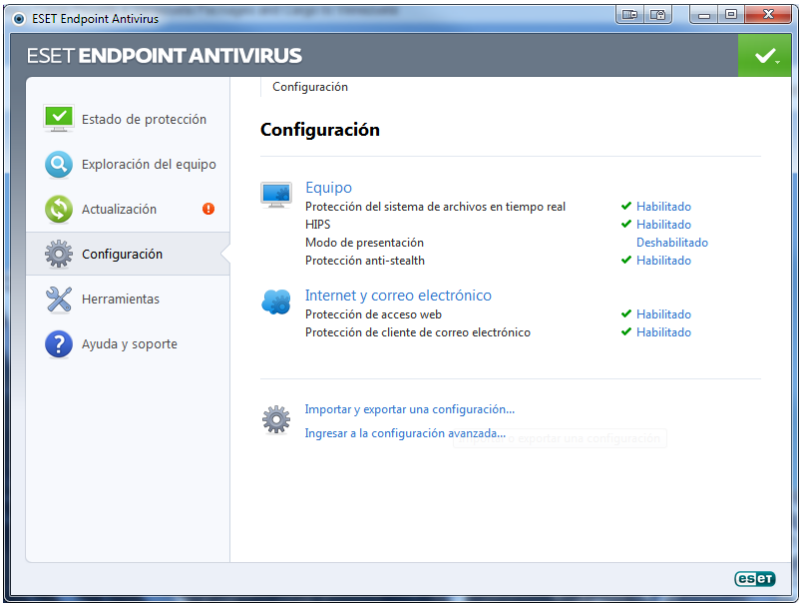

Fig. 1-2

3. En la ventana Importar y Exporta una configuración, presionar el botón **...** para ubicar la ruta donde se almaceno el archivo de configuración (.xml) previamente elaborado con el ***Editor de configuración de ESET.***

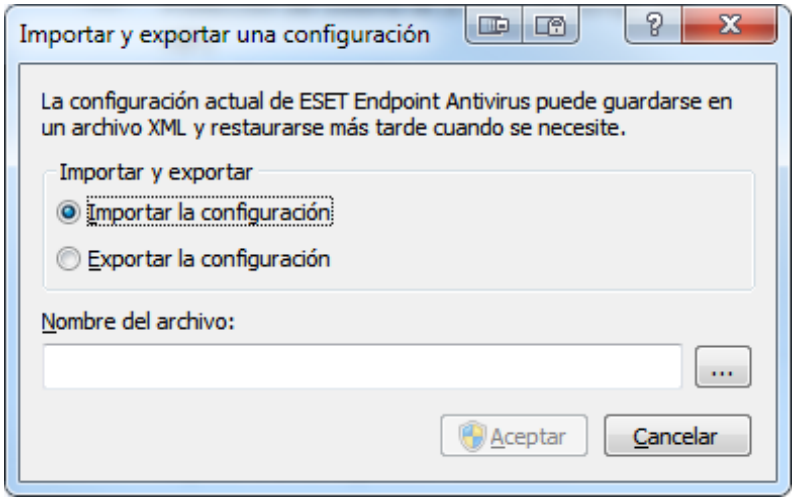

Fig. 1-3

4. En la ventana Abrir, seleccionar el archivo de configuración (.xml) que será cargado en el cliente de ESET Endpoint Antivirus. Luego presionar Abrir.

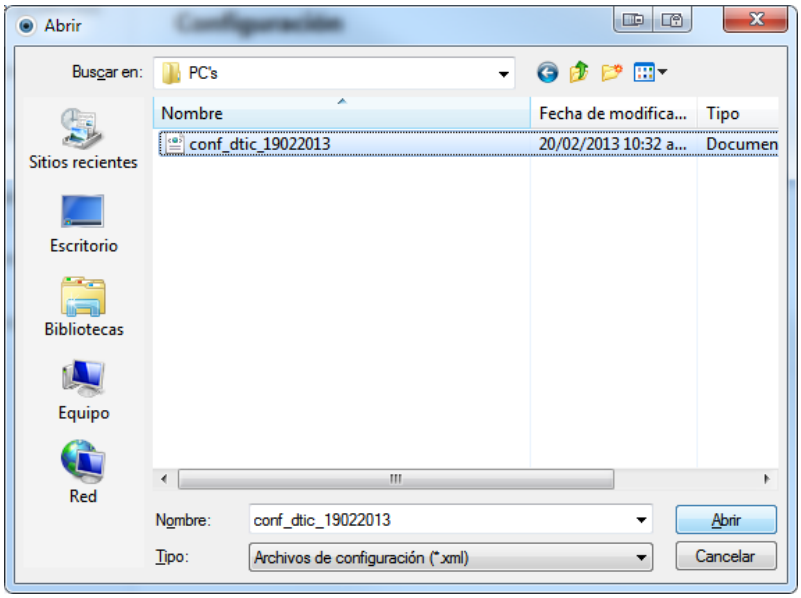

Fig. 1-4

5. En la siguiente ventana se mostrará la ruta de donde se seleccionó el archivo de configuración (.xml). Luego presionar Aceptar.

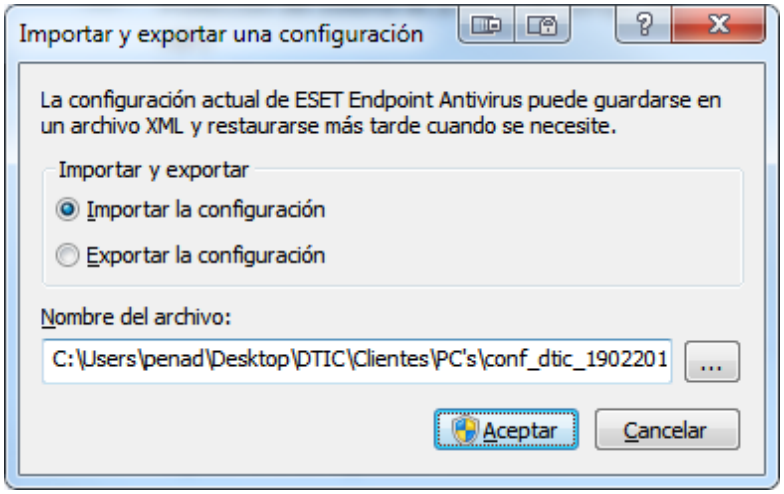

Fig. 1-5

6. Una vez que se ha cargado el Archivo de configuración (.xml), se procede a realizar la ***Actualización*** de la base de firmas de virus del ESET Endpoint Antivirus.

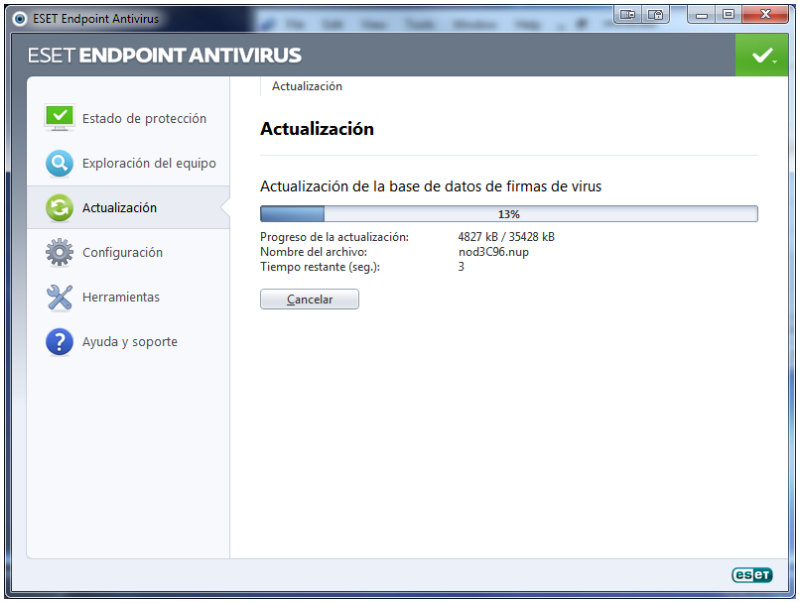

Fig. 1-6

7. En la siguiente ventana, se mostrará que el proceso de actualización se realizó satisfactoriamente.

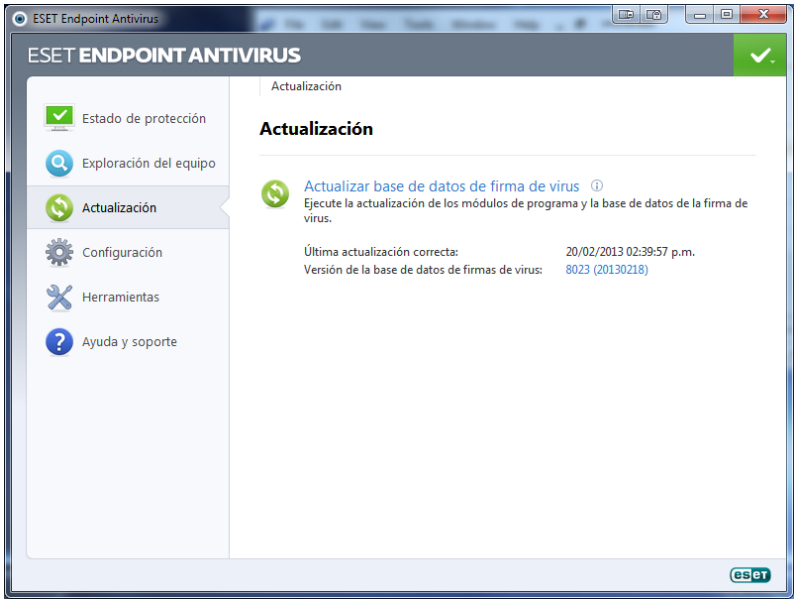

Fig. 1-7

CONFIGURANDO LAS TAREAS PROGRAMADAS DEL CLIENTE ANTIVIRUS EN LAS ESTACIONES DE TRABAJO O LAPTOPS.

1. Abrir ESET Endpoint Antivirus.

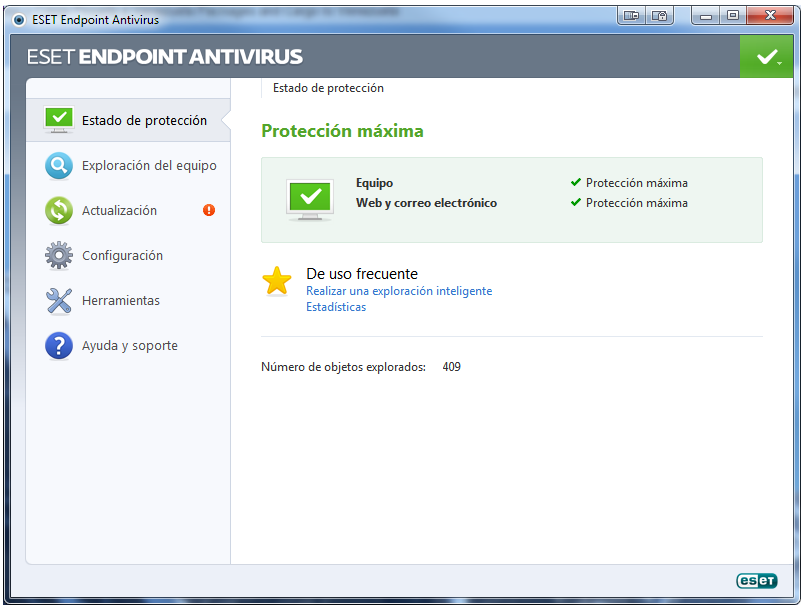

Fig. 1-1

2. En la ventana principal del ESET Endpoint Antivirus, en el panel de opciones ubicado en el lado izquierdo, presionar ***Herramientas*** → ***Tareas programadas***.

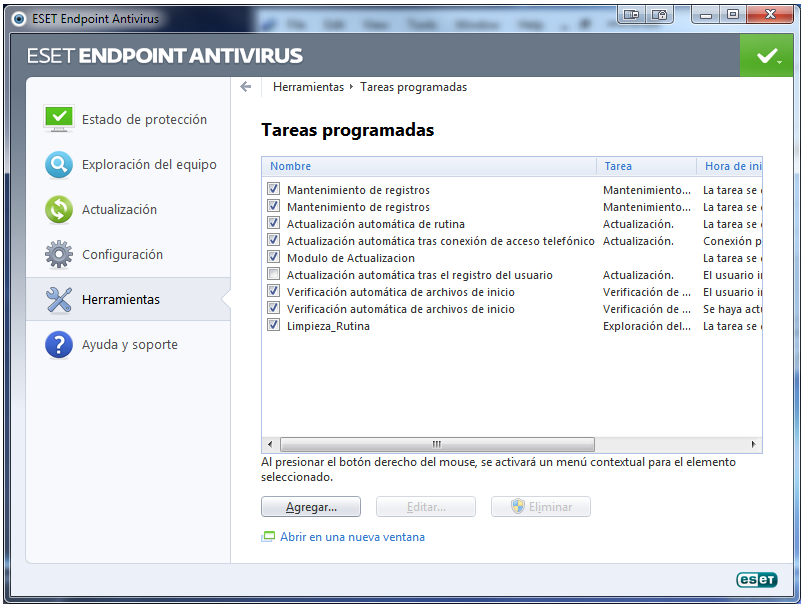

Fig. 1-2

3. Luego seleccionar la opción de ***Actualización automática de rutina*** y presionar Editar.

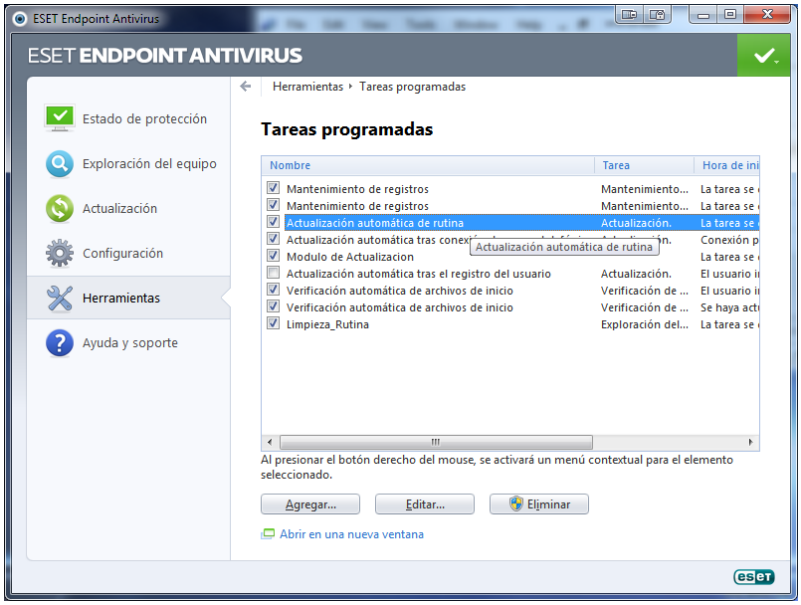

Fig. 1-3

4. En la ventana Protección de la configuración, se debe ingresar la contraseña que fue establecida previamente en la creación del archivo de configuración (.xml). Luego presionar Aceptar.

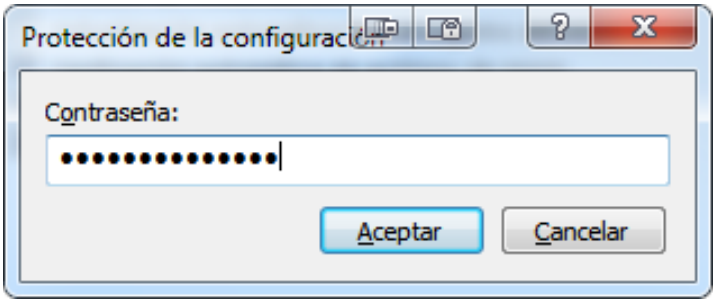

Fig. 1-4

5. En la ventana Editar tarea, seleccionar la opción de ***Actualización***. Luego presionar Siguiente.

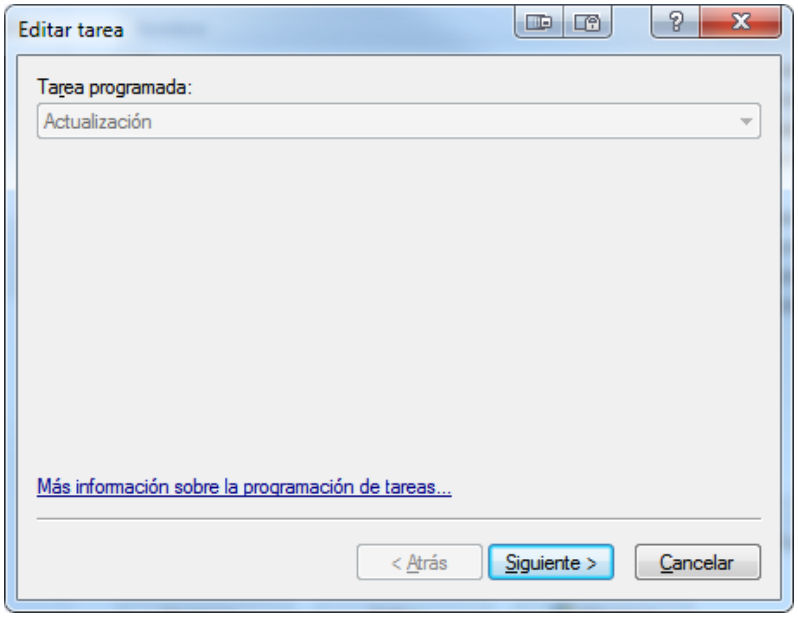

Fig. 1-5

6. En la ventana Editar tarea, verificar que el ***Nombre de la tarea*** sea ***Actualización automática de rutina***, en ***Ejecutar la tarea*** verificar que la opción ***Reiteradamente*** se encuentre seleccionada***.*** Luego presionar Siguiente.

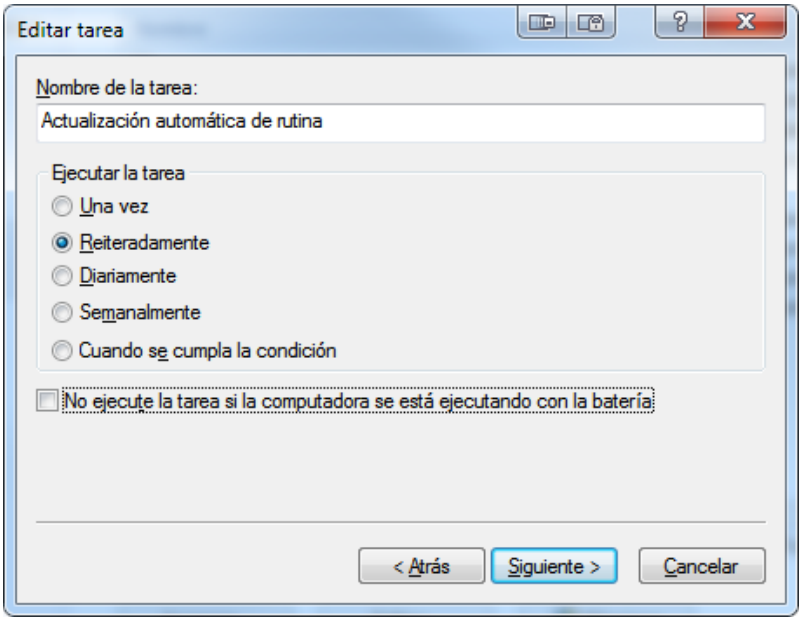

Fig. 1-6

7. En la siguiente ventana, verificar que el ***Intervalo entre ejecución de tareas (minutos):*** sea ***60***. Luego presionar Siguiente.

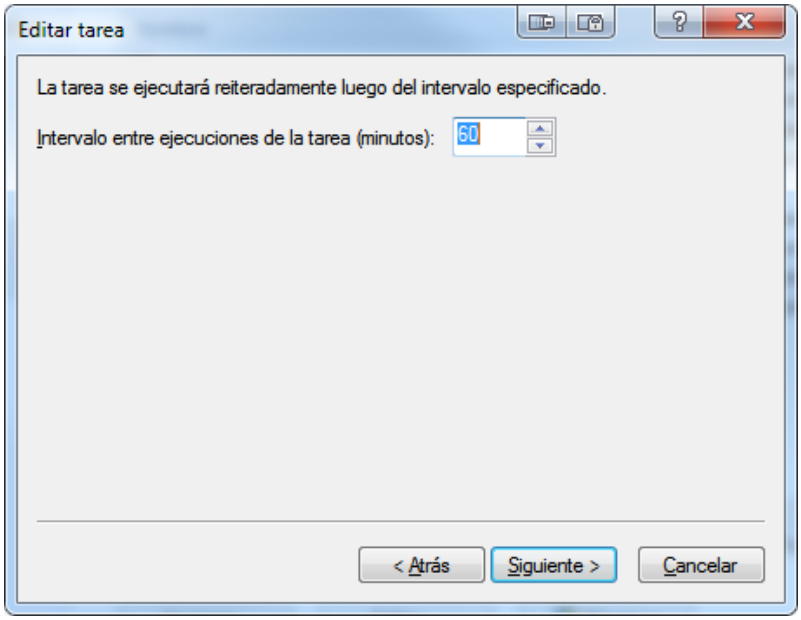

Fig. 1-7

8. En la siguiente ventana de Editar tarea, verificar que la opción ***Esperar hasta la próxima activación programada*** se encuentre seleccionada. Luego presionar Siguiente.

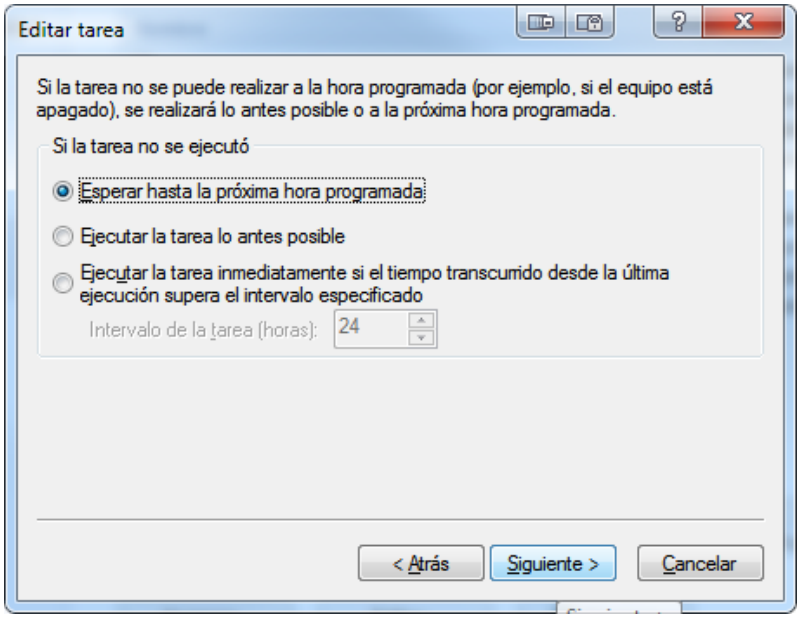

Fig. 1-8

9. En la siguiente ventana finalmente, se muestra un resumen general de los detalles de la tarea programada. Luego presionar Finalizar.

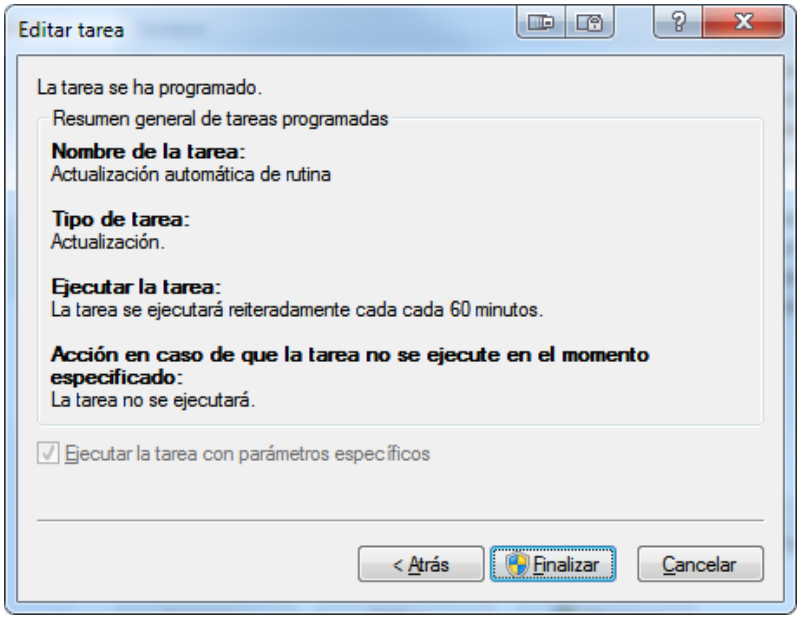

Fig. 1-9

10. En la ventana Actualizar perfiles, se deben seleccionar los ***perfiles*** tanto para el ***perfil primario*** como para el ***perfil secundario*** que serán utilizados en la ***Actualización***.

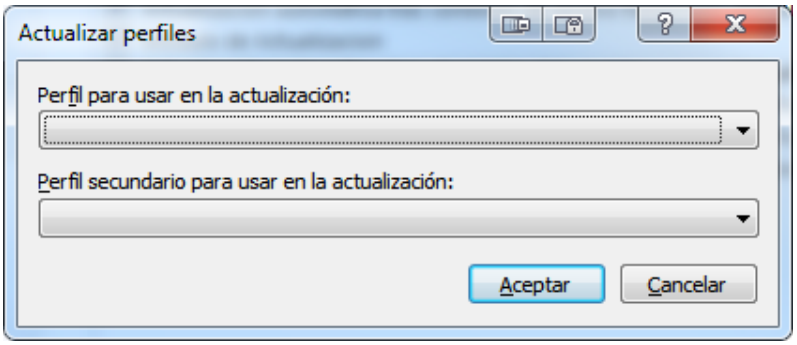

Fig. 1-10

11. En la opción ***Perfil para usar en la actualización:*** seleccionar ***Mi perfil***.

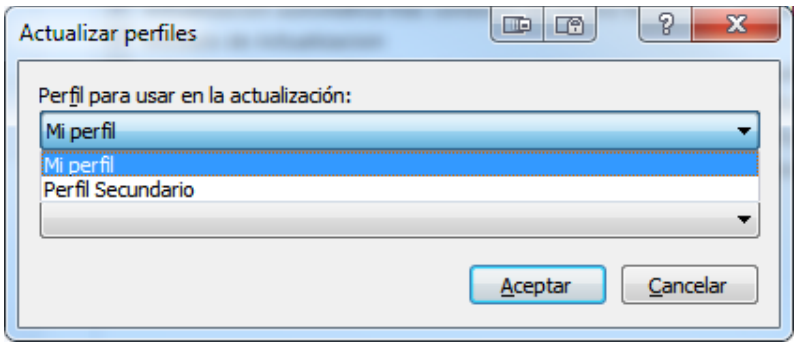

Fig. 1-11

12. En la opción ***Perfil secundario para usar en la actualización:*** seleccionar ***Perfil Secundario***.

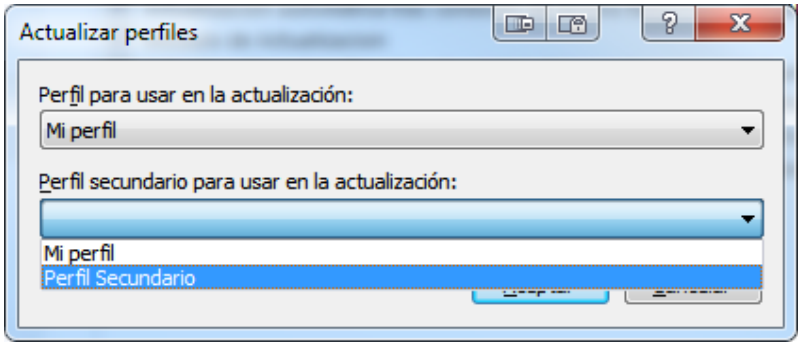

Fig. 1-12

13. En la ventana de Actualizar perfiles, una vez que han sido seleccionados ***ambos perfiles***, Finalmente, presionar Aceptar.

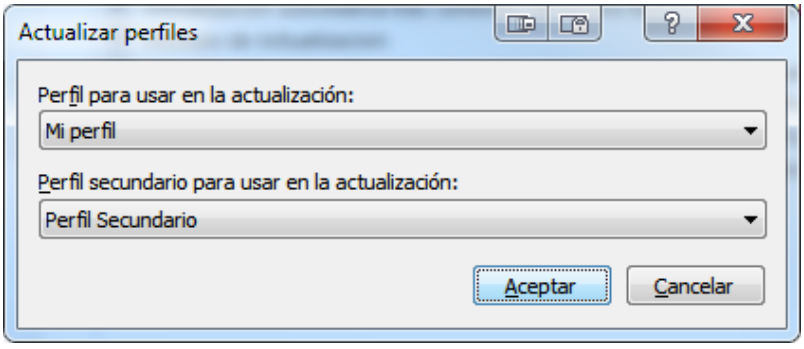

Fig. 1-13

14. Una vez seleccionados los perfiles de actualización, se procede a Verificar que se realice el proceso de ***Actualización*** de la base de firmas de virus del ESET Endpoint Antivirus.

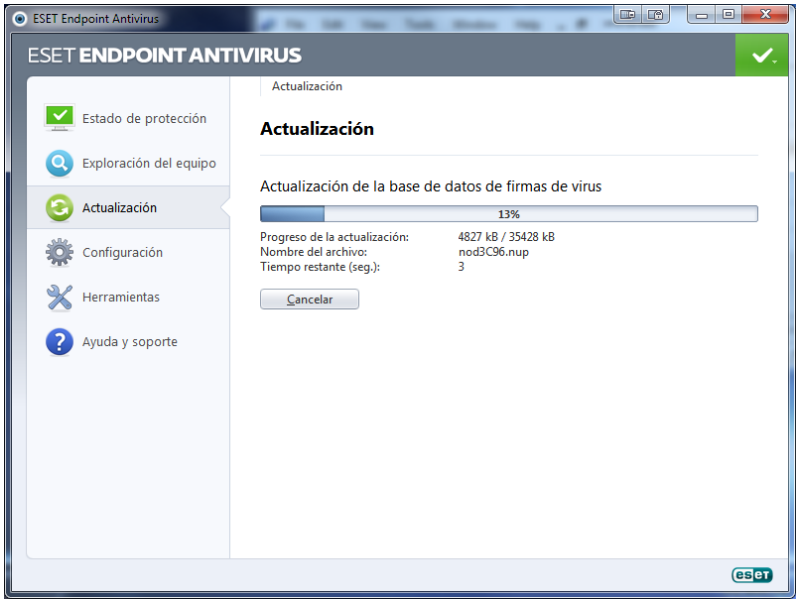

Fig. 1-14

15. En la siguiente ventana, se muestra que el proceso de actualización se realizó satisfactoriamente.

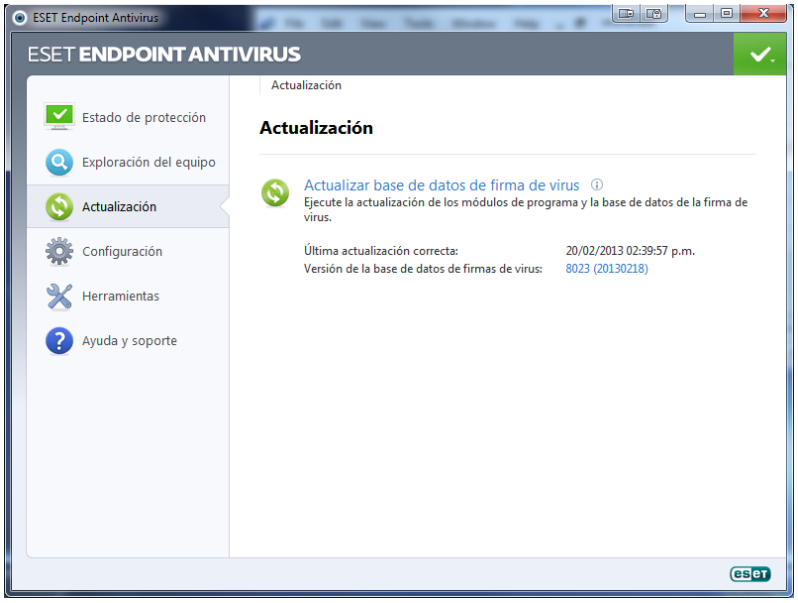

Fig. 1-15

INSTALANDO MYSQL SERVER 5.1.

NOTA: OBVIAR ESTE PASO PARA EL PROCEDIEMINTO DE ACTUALIZACIÓN, SOLO SE APLICA CUANDO SE LLEVA A CABO UNA INSTALACIÓN INICIAL.

En primer lugar, es necesario disponer del programa de instalación de MySQL Server, el cual se puede descargar gratuitamente del siguiente URL: http://dev.mysql.com/downloads/mysql/.

La versión de MySQL Server que se hace referencia en este instructivo es MySQL 5.1.

Una vez que se ha descargado el archivo instalador, se procede a ejecutarlo.

1. Se mostrará la ventana Welcome to the Setup Wizard for MySQL Server 5.1. Luego presionar el botón **Next**.

Fig. 1-1

2. En la Ventana Setup Type, seleccionar la opción **Typical** y Luego presionar el botón **Next**.

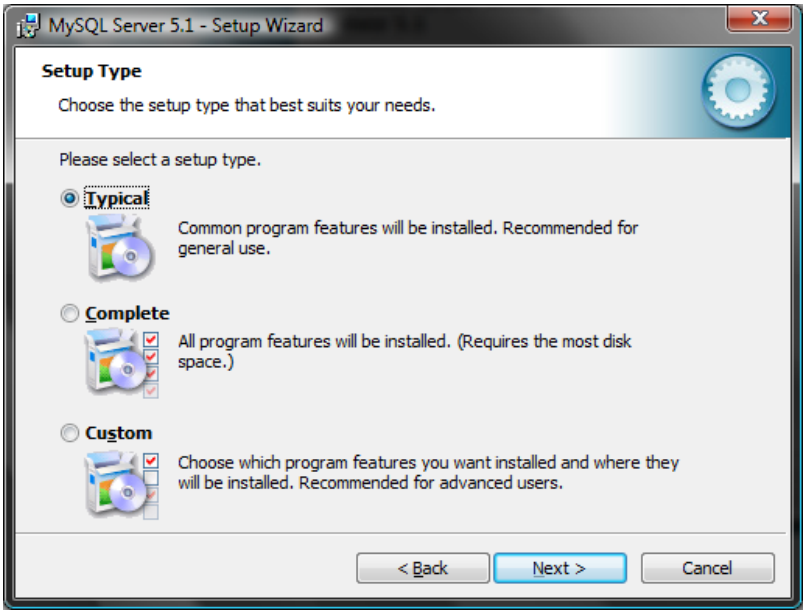

Fig. 1-2

3. En la ventana Ready to Install the Program, se mostrará un breve resumen de la instalación. Luego presionar el botón **Install**.

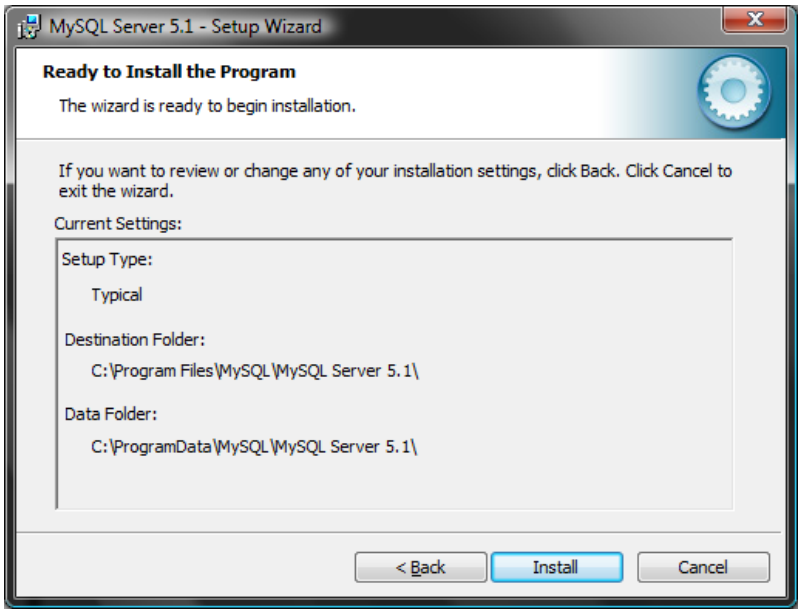

Fig. 1-3

4. En la ventana Wizard Completed, tildar la opción ***Configure the MySQL Server now*** y des tildar la opción ***Register the MySQL Server now***. Luego presionar el botón **Finish**.

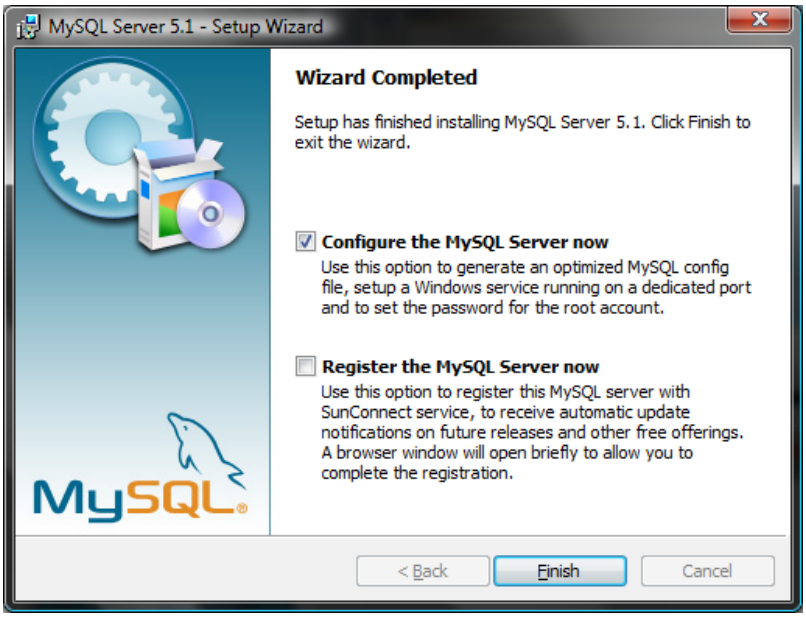

Fig. 1-4

5. En la ventana Welcome to the MySQL Server Instance Configuration Wizard 1.0.16.0. Se procede a realizar la configuración de ***MySQL Server Instance.*** Luego presionar el botón **Next**.

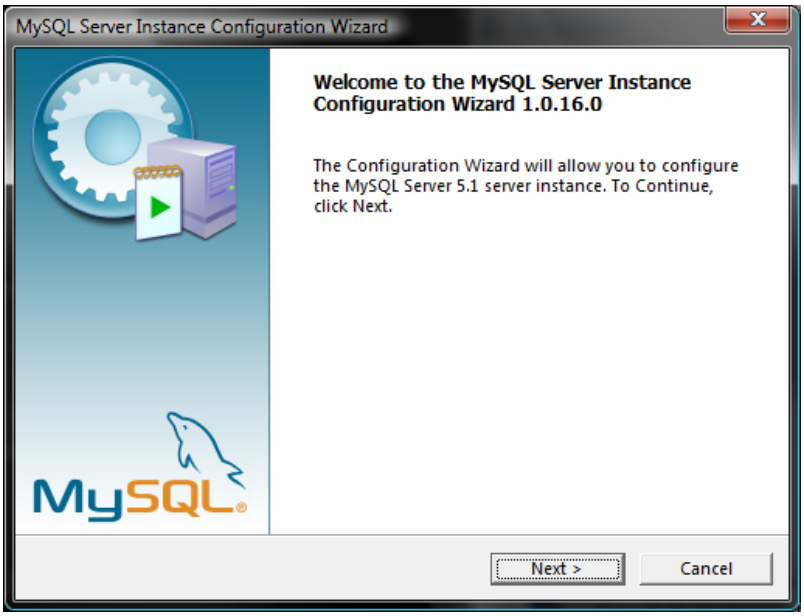

Fig. 1-5

6. En la ventana MySQL Server Instance Configuration, seleccionar la opción ***Standard Configuration*** y Luego presionar el botón **Next**.

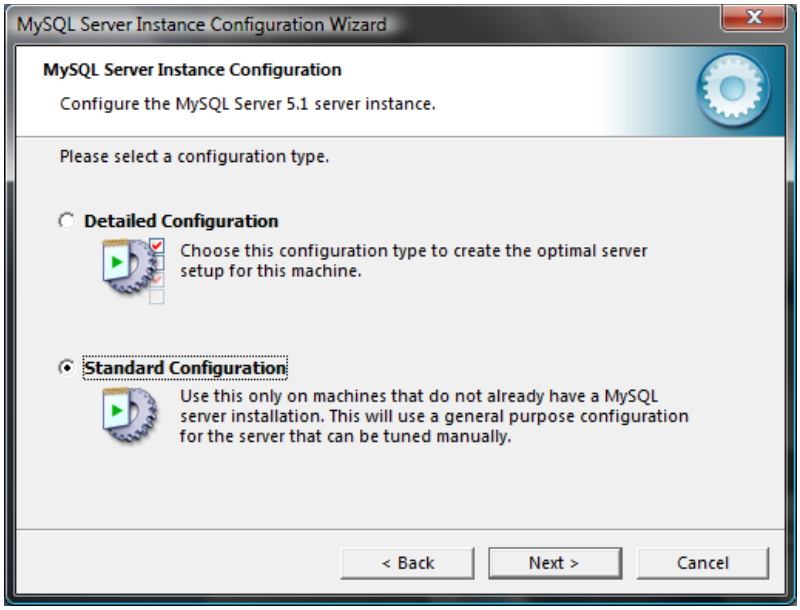

Fig. 1-6

7. En la siguiente ventana de MySQL Server Instance Configuration, tildar la opción ***Install As Windows Service.*** Luego presionar el botón **Next**.

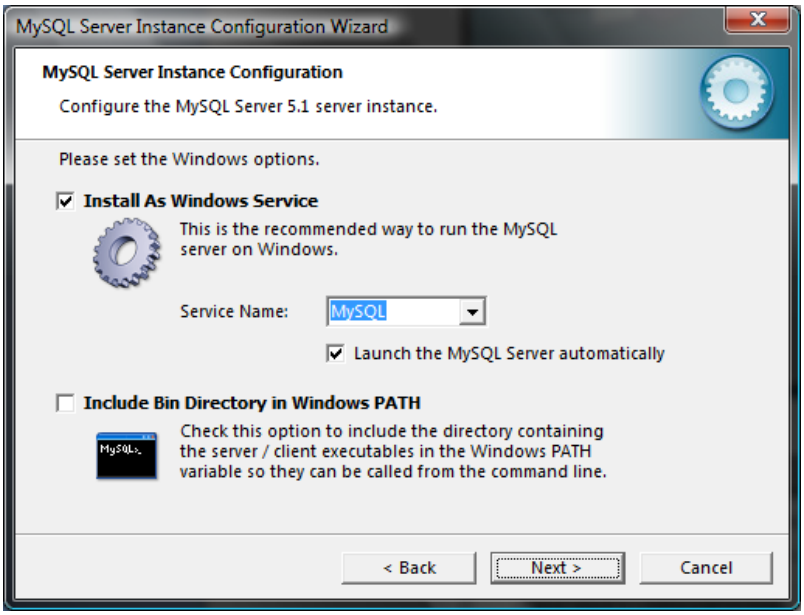

Fig. 1-7

8. En la siguiente ventana de MySQL Server Instance Configuration, tildar la opción ***Modify Security Settings*** e ingresar y confirmar el ***password*** para el usuario ***root de MySQL***. Luego presionar el botón **Next**.

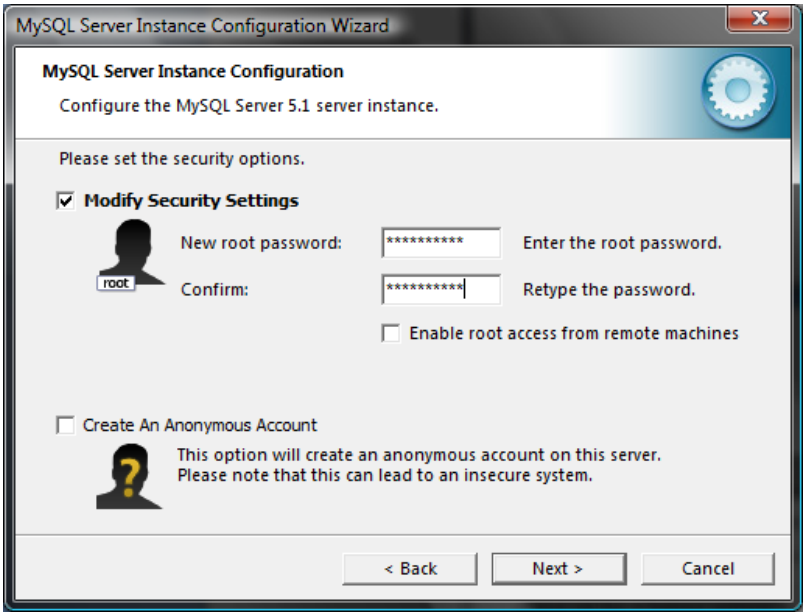

Fig. 1-8

9. En la siguiente ventana de MySQL Server Instance Configuration, verificar que la instalación fue exitosa como se muestra en la figura. Luego presionar el botón **Finish**.

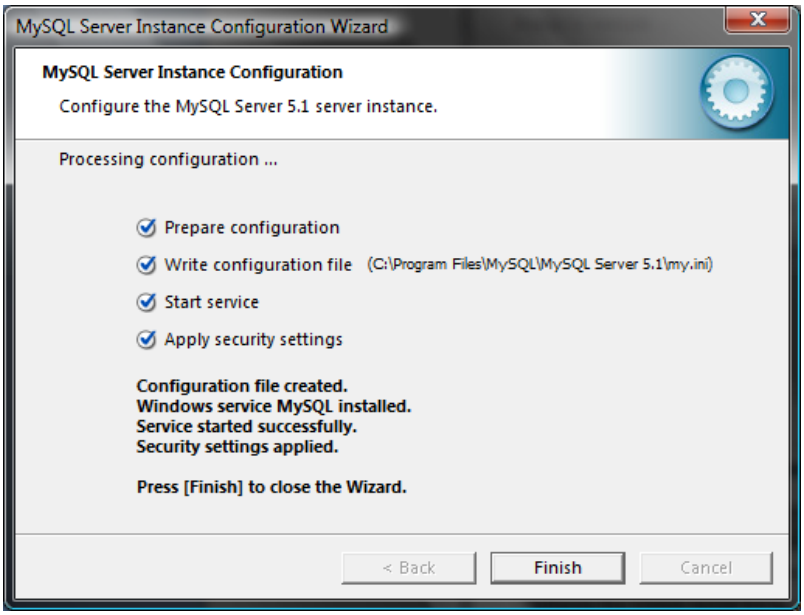

Fig. 1-9

INSTALANDO MYSQL SERVER INSTANCE CONFIG WIZARD

NOTA: OBVIAR ESTE PASO PARA EL PROCEDIEMINTO DE ACTUALIZACIÓN, SOLO SE APLICA CUANDO SE LLEVA A CABO UNA INSTALACIÓN INICIAL.

1. Hacer click en ***Start – MySQL – MySQL Server 5.1 - MySQL Server Instance Config Wizard***.

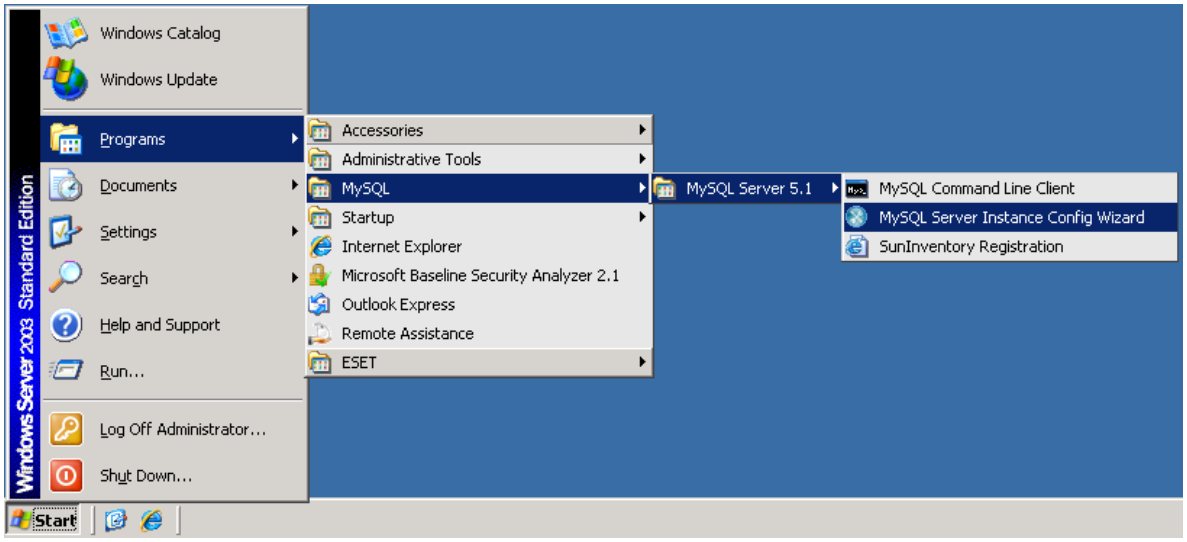

Fig. 1-1

2. Se mostrará la ventana Welcome to the setup wizard for MySQL Connector/ODBC 5.1. Presionar el botón **Next**.

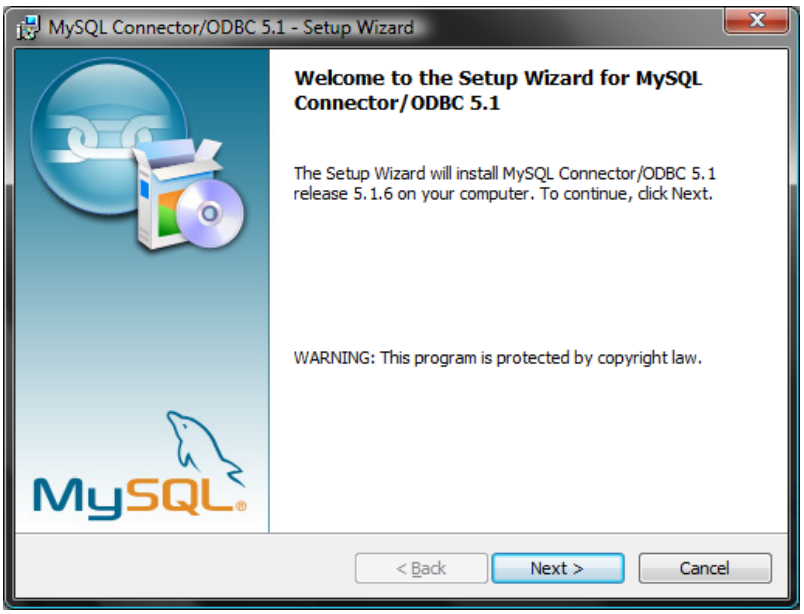

Fig. 1-2

3. En la ventana Setup Type, seleccionar la opción ***Typical***. Luego presionar el botón **Next**.

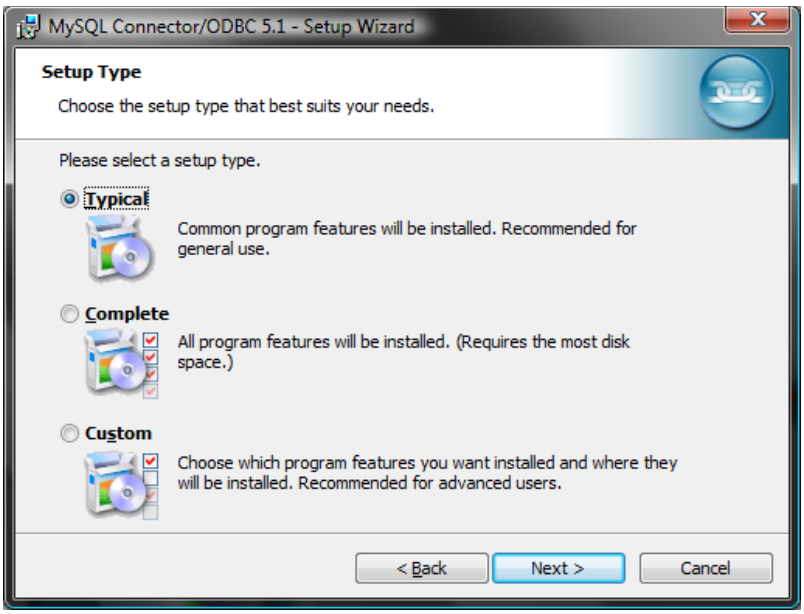

Fig. 1-3

4. En la ventana Ready to Install the program, presionar el botón ***Install para comenzar con la instalación del conector ODBC***.

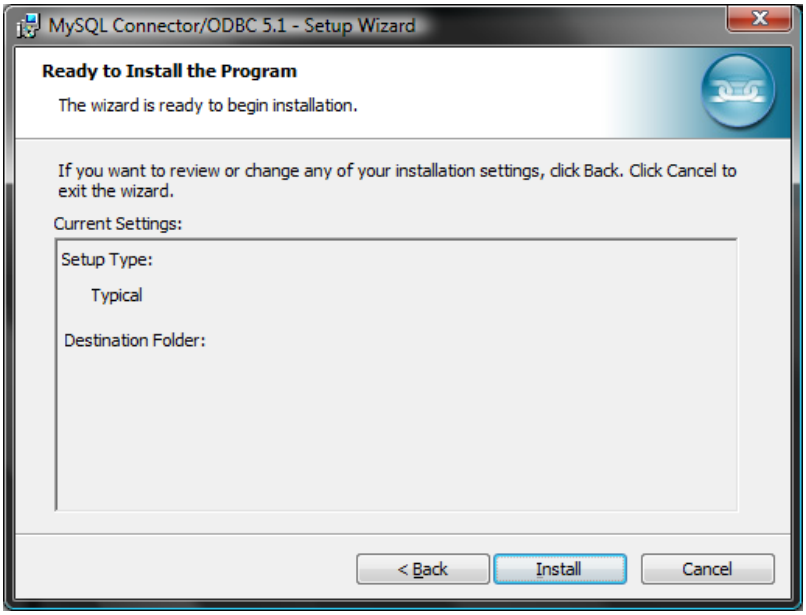

Fig. 1-4

5. En la ventana Wizard Completed, presionar el botón **Finish**.

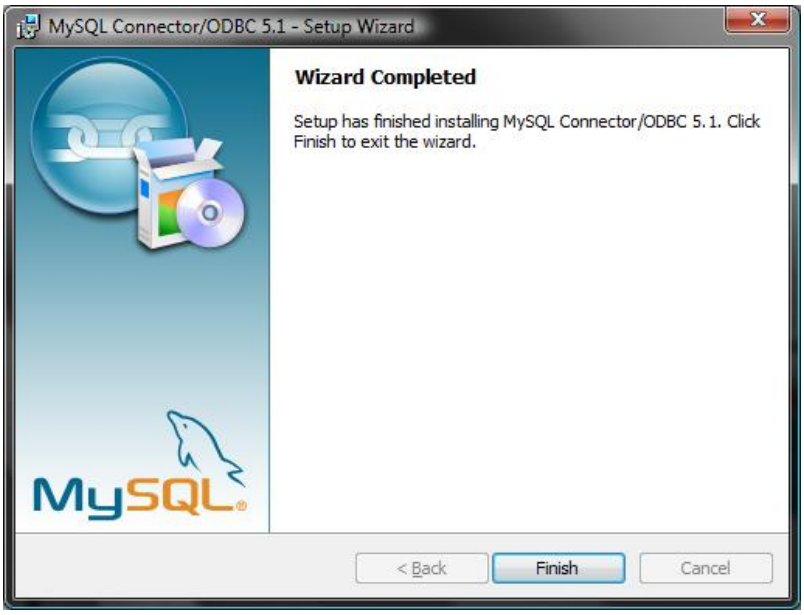

Fig. 1-5

INSTALANDO MYSQL CONNECTOR ODBC

NOTA: OBVIAR ESTE PASO PARA EL PROCEDIEMINTO DE ACTUALIZACIÓN, SOLO SE APLICA CUANDO SE LLEVA A CABO UNA INSTALACIÓN INICIAL.

En primer lugar, es necesario disponer del archivo de instalación de MySQL Connector ODBC, el cual se puede descargar gratuitamente del siguiente URL: ***http://dev.mysql.com/downloads/connector/odbc/5.1.html***.

La versión de MySQL Connector ODBC que se hace referencia en este instructivo es MySQL Connector/ODBC 5.1.

Una vez que se ha descargado el archivo instalador, se procede a ejecutarlo:

1. En la ventana Welcome to the setup Wizard for MySQL Connector/ODBC 5.1, Presionar el botón **Next**.

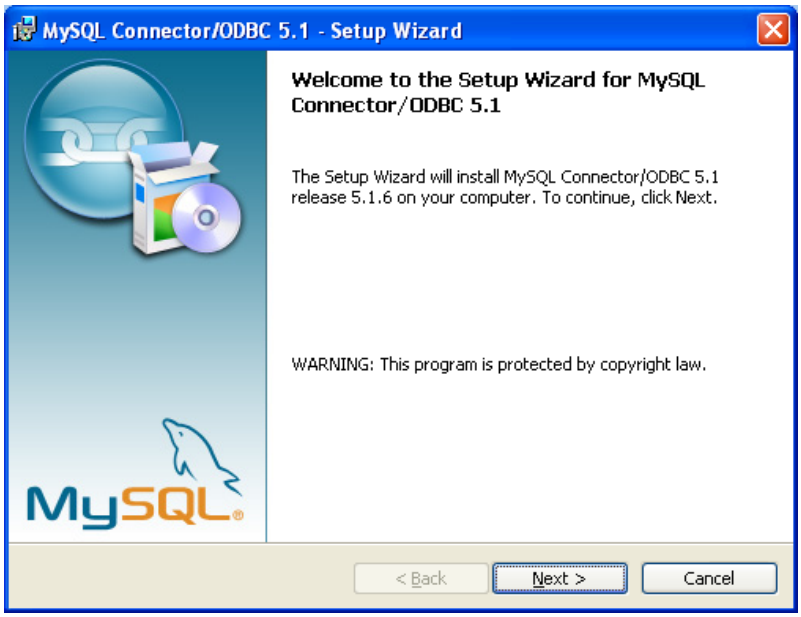

Fig. 1-1

2. En la ventana Setup Type, seleccionar la opción ***Typical*** y luego presionar el botón **Next**.

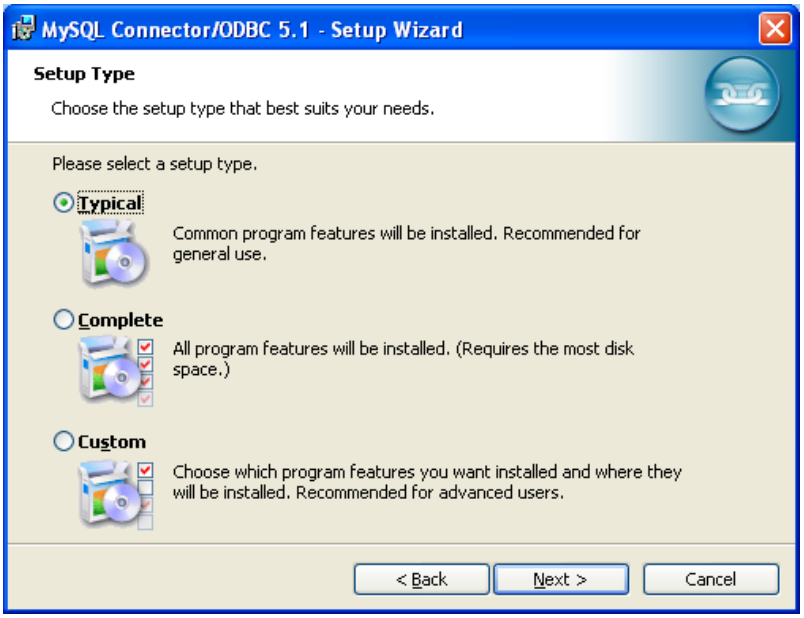

Fig. 1-2

3. En la ventana Ready to Install The Program, presionar el botón **Install**.

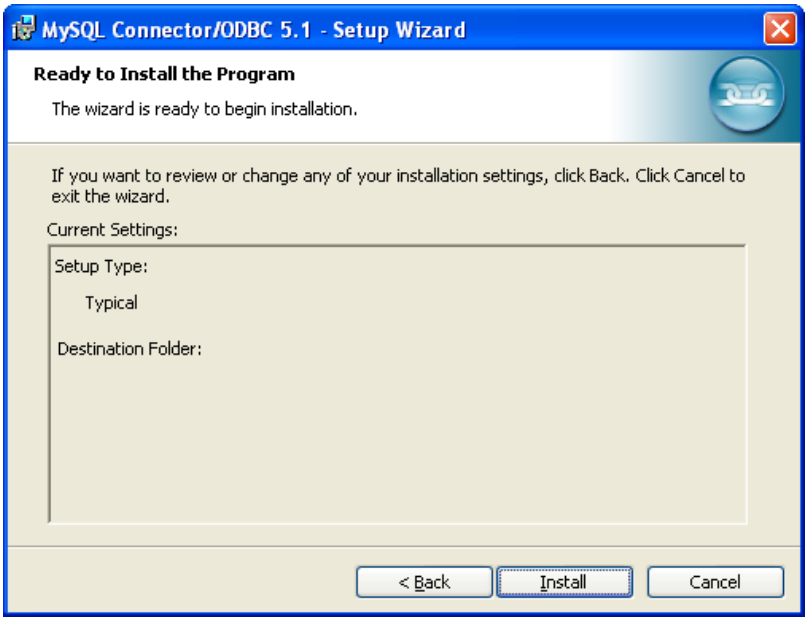

Fig. 1-3

4. En la ventana Wizard Complete, presionar el botón **Finish**.

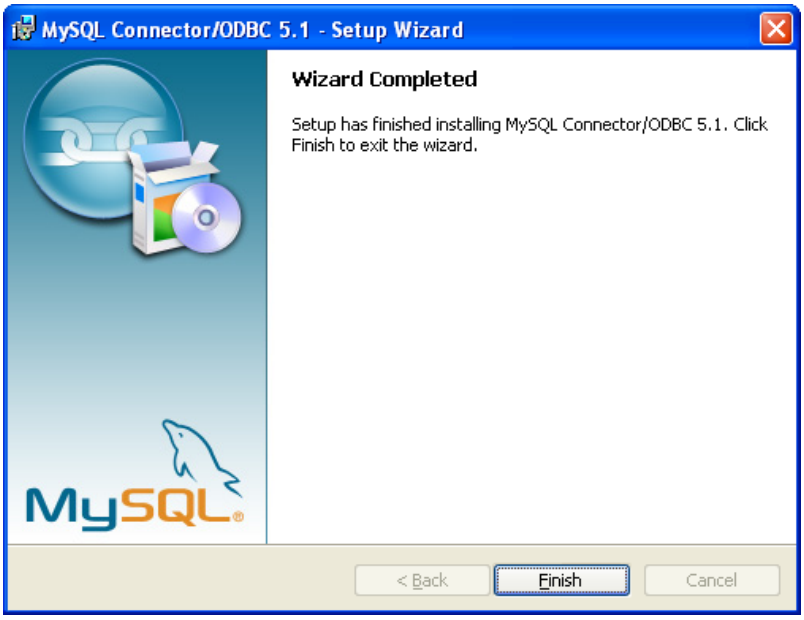

Fig. 1-4

GLOSARIO
TIPOS DE AMENAZAS

Una amenaza es un software malicioso que intenta entrar en la estación de trabajo, laptops o servidor de un usuario y dañarlo.

1. ***Virus:*** un virus informático es una amenaza que daña los archivos del ordenador. Su nombre se debe a los virus biológicos, ya que usan técnicas similares para pasar de un ordenador a otro.

   Los virus informáticos atacan principalmente a los archivos y documentos ejecutables. Para reproducirse, un virus adjunta su "cuerpo" al final de un archivo de destino. En resumen, así es cómo funciona un virus informático: después de la ejecución del archivo infectado, el virus se activa (antes de la aplicación original) y realiza la tarea que tiene predefinida. Después, se ejecuta la aplicación original. Un virus no puede infectar un ordenador a menos que un usuario (bien accidental o deliberadamente) ejecute o abra el programa malintencionado.

   Los virus informáticos pueden tener diversos fines y niveles de gravedad. Algunos son muy peligrosos, debido a su capacidad para eliminar archivos del disco duro de forma deliberada. Sin embargo, otros virus no causan daños reales, solo sirven para molestar al usuario y demostrar las capacidades técnicas de sus autores.

   Es importante mencionar que los virus (si se comparan con los troyanos o el spyware) son cada vez menos habituales, ya que no son atractivos desde un punto de vista comercial para los autores de software malintencionado. Además, el término "virus" se utiliza incorrectamente con mucha frecuencia para abarcar todo tipo de amenazas. Este término está desapareciendo gradualmente y se está sustituyendo por el término "malware" (software malicioso), que es más preciso.

   Si su ordenador se infecta con un virus, debe restaurar los archivos infectados a su estado original, es decir, desinfectarlos con un programa antivirus.

   Ejemplos de virus: oneHalf, Tenga y Yankee Doodle.

2. ***Gusanos:*** un gusano informático es un programa que contiene código malicioso que ataca a los ordenadores host y se extiende a través de una red. La principal diferencia entre un virus y un gusano es que los gusanos tienen la capacidad de reproducirse y viajar solos, no dependen de archivos host (o sectores de inicio). Los gusanos se extienden por las direcciones de correo electrónico de la lista de contactos o explotan las vulnerabilidades de seguridad de las aplicaciones de red.

   Los gusanos son mucho más viables que los virus informáticos; dada la gran disponibilidad de Internet, se pueden extender por todo el mundo en cuestión de horas, o incluso minutos, desde su lanzamiento. Esta capacidad para reproducirse de forma independiente y rápida los hace más peligrosos que otros tipos de código malicioso.

   Un gusano activado en un sistema puede causar una serie de problemas: puede eliminar archivos, degradar el rendimiento del sistema o incluso desactivar algunos programas. Además, su naturaleza le permite servir de "medio de transporte" para otros tipos de amenazas.

   Si el ordenador está infectado con un gusano, es recomendable eliminar los archivos infectados, pues podrían contener código malicioso.

   Ejemplos de gusanos conocidos: lovsan/Blaster, Stration/Warezov, Bagle y Netsky.

3. ***Troyanos:*** históricamente, los troyanos informáticos se han definido como una clase de amenaza que intenta presentarse como un programa útil, engañando así a los usuarios para que permitan su ejecución. Sin embargo, es importante señalar que esto era así en el caso de los caballos troyanos del pasado; hoy en día, ya no necesitan disfrazarse. Su único fin es infiltrarse lo más fácilmente posible y cumplir sus malintencionados objetivos. "Troyano" se ha convertido en un término muy general para describir cualquier amenaza que no entre en ninguna clase de amenaza específica.

   Dado que se trata de una categoría muy amplia, con frecuencia se divide en muchas subcategorías:

   - **Descargador:** programa malintencionado con capacidad para descargar otras amenazas de Internet.
   - **Lanzador:** troyano diseñado para lanzar otros tipos de código malicioso en ordenadores vulnerables.

- **Puerta trasera:** aplicación que se comunica con atacantes remotos y les permite acceder a los sistemas para tomar su control.
- **Registrador de pulsaciones:** programa que registra cada pulsación que escribe el usuario y envía la información a atacantes remotos.
- **Marcador:** los marcadores son programas diseñados para conectar con números de tarifa con recargo. Es casi imposible que un usuario note que se ha creado una conexión. Los marcadores solo pueden causar daño a los usuarios que tienen módems de marcación, que ya casi no se utilizan.

Normalmente, los troyanos adoptan la forma de archivos ejecutables con la extensión .exe. Si se detecta un archivo como troyano en su ordenador, es recomendable que lo elimine, ya que lo más probable es que contenga código malicioso.

Ejemplos de troyanos conocidos: netBus, Trojandownloader, Small.ZL y Slapper.

4. ***Rootkits:*** los rootkits son programas malintencionados que conceden a los atacantes de Internet acceso ilimitado a un sistema, al tiempo que ocultan su presencia. Una vez que han accedido al sistema (normalmente explotando alguna vulnerabilidad del mismo), usan funciones del sistema operativo para evitar su detección por parte del antivirus: ocultan procesos, archivos y datos de registro de Windows, etc. Por este motivo, es casi imposible detectarlos con las técnicas de detección normales.

   Hay dos niveles de detección disponibles para evitar los rootkits:

   - Cuando intentan acceder a un sistema. Aún no están presentes y, por tanto, están inactivos. La mayoría de los sistemas antivirus pueden eliminar rootkits en este nivel (suponiendo que realmente detectan dichos archivos como infectados).
   - Cuando se ocultan en el proceso normal de análisis. Los usuarios de ESET File Security tienen la ventaja de la tecnología Anti-Stealth, que también puede detectar y eliminar rootkits activos.

5. ***Adware:*** es la abreviatura del término inglés utilizado para el software relacionado con publicidad. Los programas que muestran material publicitario se incluyen en esta categoría. Normalmente, las aplicaciones de adware abren

automáticamente una ventana emergente nueva con anuncios en el navegador de Internet o cambian la página de inicio del navegador. La aplicación de adware suele instalarse con programas gratuitos, lo que permite a los creadores de esos programas gratuitos cubrir los costes de desarrollo de sus aplicaciones (normalmente útiles).

La aplicación de adware no es peligrosa en sí, pero molesta a los usuarios con publicidad. El peligro reside en el hecho de que la aplicación de adware también puede realizar funciones de seguimiento (al igual que las aplicaciones de spyware).

Si decide utilizar un producto gratuito, preste especial atención al programa de instalación. La mayoría de los programas de instalación le informarán sobre la instalación de un programa de adware adicional. Normalmente, podrá cancelarlo e instalar el programa sin esta aplicación de adware.

Sin embargo, algunos programas no se instalarán sin la aplicación de adware, o su funcionalidad será limitada. Esto significa que la aplicación de adware puede acceder al sistema de manera "legal" a menudo, pues los usuarios así lo han aceptado. En estos casos, es mejor prevenir que curar. Si se detecta un archivo de adware en el ordenador, es recomendable eliminarlo, pues existen muchas probabilidades de que contenga código malicioso.

6. ***Spyware:*** esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento o conocimiento del usuario. El spyware usa funciones de seguimiento para enviar diversos datos estadísticos, como una lista de sitios web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista de palabras escritas.

   Los autores de spyware afirman que el objetivo de estas técnicas es averiguar más sobre las necesidades y los intereses de los usuarios, así como mejorar la gestión de la publicidad. El problema es que no existe una distinción clara entre las aplicaciones útiles y las malintencionadas, de modo que nadie puede estar seguro de que no se hará un mal uso de la información recuperada. Los datos obtenidos por aplicaciones spyware pueden contener códigos de seguridad, códigos PIN, números de cuentas bancarias, etc. Con frecuencia, el spyware se envía junto con versiones gratuitas de programas para generar ingresos o para ofrecer un incentivo para comprar el software. A menudo, se informa a los usuarios sobre la presencia de spyware durante la instalación de un programa para ofrecerles un incentivo para la adquisición de una versión de pago.

Algunos ejemplos de productos gratuitos conocidos que se envían junto con spyware son las aplicaciones cliente de redes P2P (peer to peer). Spyfalcon o Spy Sheriff (y muchos más) pertenecen a una subcategoría específica de spyware: parecen programas antispyware, pero en realidad son aplicaciones de spyware.

Si se detecta un archivo de spyware en su ordenador, es aconsejable que lo elimine, ya que es muy posible que contenga código malicioso.

7. ***Aplicaciones potencialmente peligrosas:*** existen muchos programas legítimos que sirven para simplificar la administración de ordenadores en red. Sin embargo, si caen en las manos equivocadas, podrían utilizarse con fines maliciosos. ESET File Security proporciona una opción para detectar estas amenazas.

   "Aplicaciones potencialmente peligrosas" es la clasificación utilizada para el software comercial legítimo. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban todas las teclas pulsadas por un usuario).

   Si averigua que hay una aplicación potencialmente peligrosa ejecutándose en su ordenador (y no la ha instalado usted), consulte al administrador de la red o elimine la aplicación.

8. ***Aplicaciones potencialmente indeseables:*** las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa. Estas aplicaciones suelen necesitar el consentimiento del usuario para su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontraba antes de la instalación). Los cambios más importantes son:
   - Se abren ventanas nuevas que no se habían visto anteriormente.
   - Activación y ejecución de procesos ocultos.
   - Mayor uso de los recursos del sistema.
   - Cambios en los resultados de búsqueda.
   - La aplicación se comunica con servidores remotos.