GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN

SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL
INSTITUTO SUPERIOR DE FORMACIÓN Y RECURSOS EN RED PARA EL PROFESORADO

REDES DE ÁREA LOCAL EN CENTROS EDUCATIVOS

Ubuntu

Configuración básica

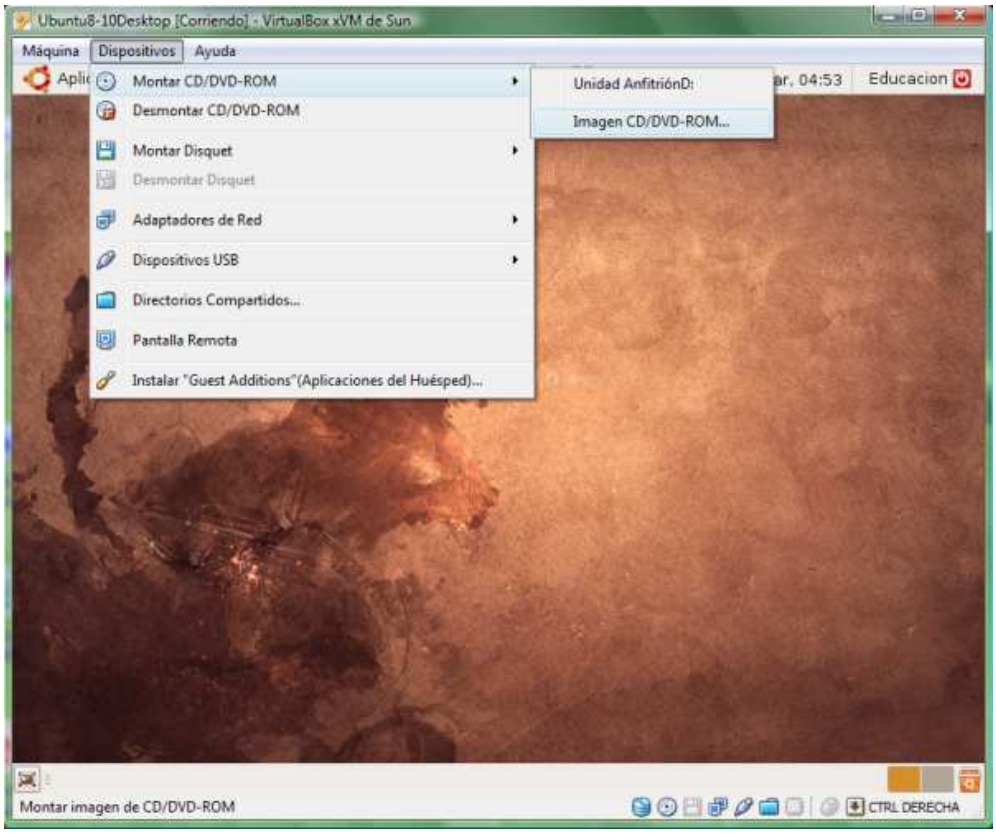
Formación en Red

Configuración básica

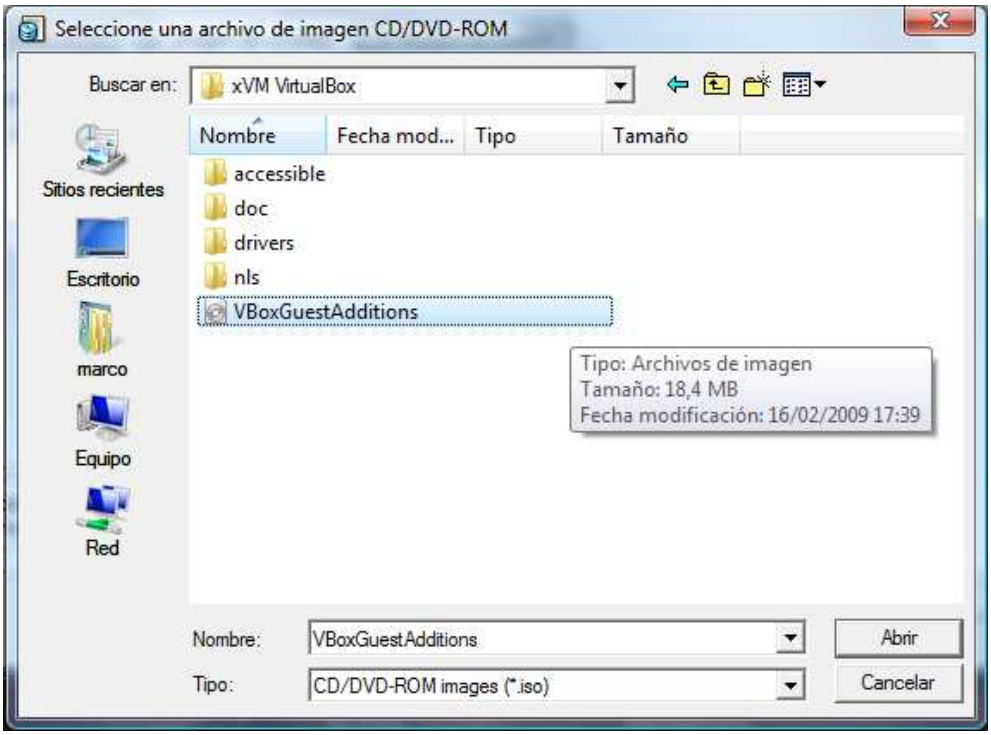
Instalación de las herramientas de VirtualBox

Esta operación sólo deberá realizarla si va a seguir la documentación sobre una máquina virtual. Las VBoxGuestAdditions son un conjunto de programas que mejoran el desempeño de la máquina virtual en lo tocante al rendimiento de la tarjeta gráfica, integración del ratón, carpetas compartidas con el anfitrión, compartición del portapapeles y otras características mejoradas que están descritas en el manual de usuario de VirtualBox.

Para instalar las VBoxGuestAdditions, seleccione la opción de menú **Dispositivos->Montar CD/DVD-ROM->Imagen CD/DVD-ROM...** del menú principal de la máquina virtual de Ubuntu, tal y como se muestra en la siguiente figura.

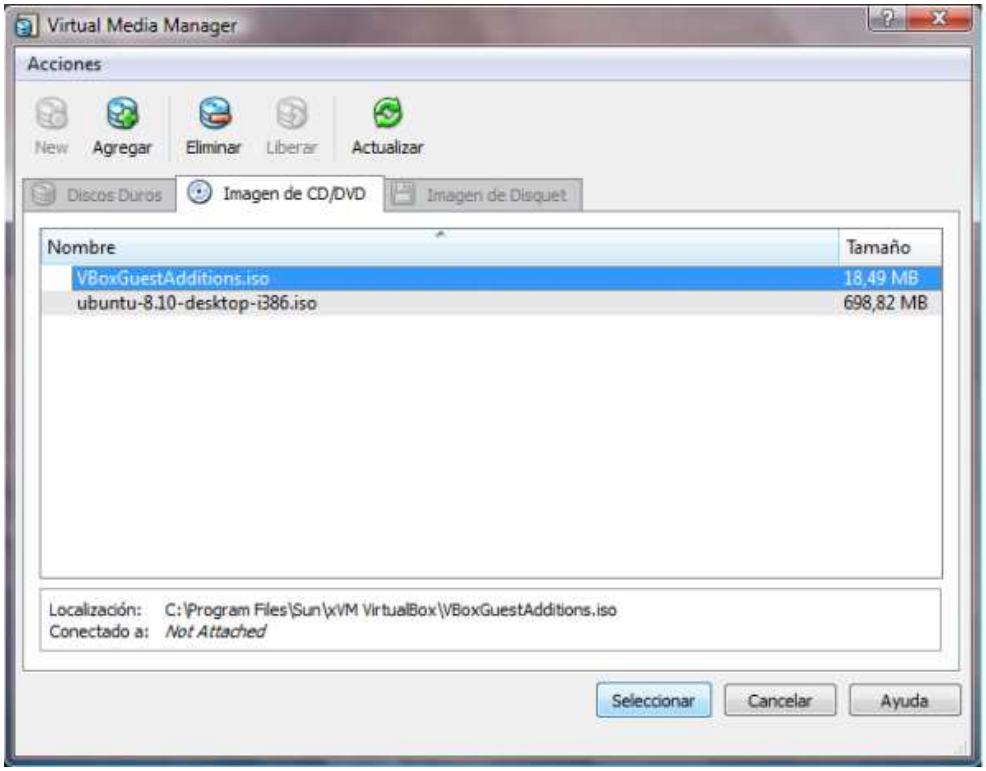


A continuación navegue hasta la carpeta donde se encuentra el fichero **VBoxGuestAdditions.iso**. Este fichero lo encontrará en la carpeta de instalación de VirtualBox. Si ha instalado VirtualBox en la carpeta de instalación por defecto, esta ubicación será **C:\Archivos de programa\Sun\xVM VirtualBox**. Seleccione el mencionado archivo y pulse el botón **Abrir**, tal y como mostramos en la siguiente figura.

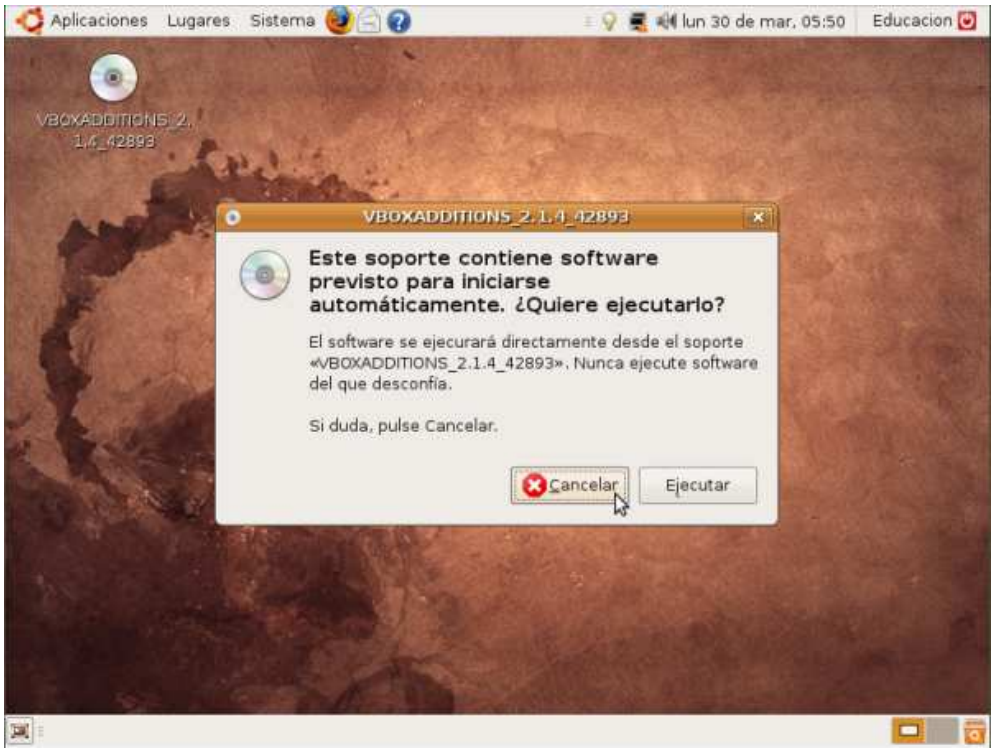


NOTA: Si el sistema operativo anfitrión que está utilizando el lector es una distribución de Linux, obviamente la ruta anterior responderá a una propia de dicho sistema operativo, y no una ruta propia de Windows.

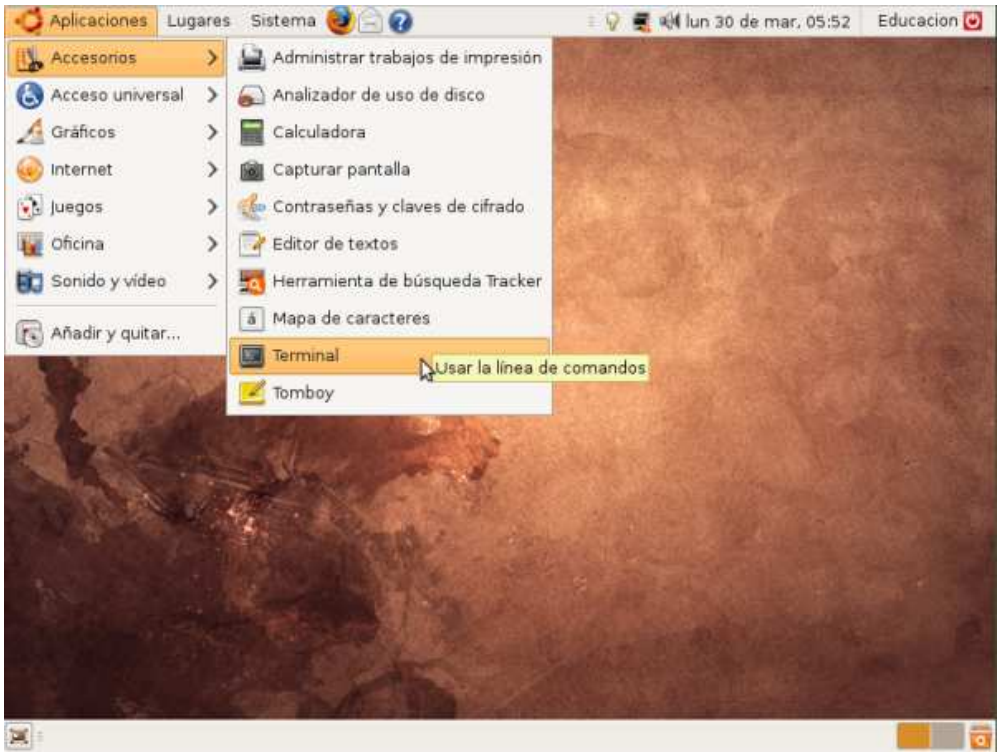
En la siguiente ventana que se nos muestra, seleccionaremos de nuevo la imagen **VBoxGuestAdditions.iso** y pulsamos el botón **Seleccionar**.



A continuación aparecerá una ventana que nos indica que el soporte montado (la imagen ISO seleccionada) contiene software previsto para ejecutarse automáticamente, sin embargo NO pulse el botón **Ejecutar** y seleccione el botón **Cancelar**, tal y como muestra la siguiente figura.



Para instalar correctamente las VBoxGuestAdditions deberá hacerlo desde una línea de comandos. Para ello deberá lanzar una terminal desde el menú **Aplicaciones->Accesorios->Terminal** tal y como se muestra en la siguiente figura.



En la terminal que aparecerá a continuación deberá escribir secuencialmente los siguientes comandos:

cd /cdrom

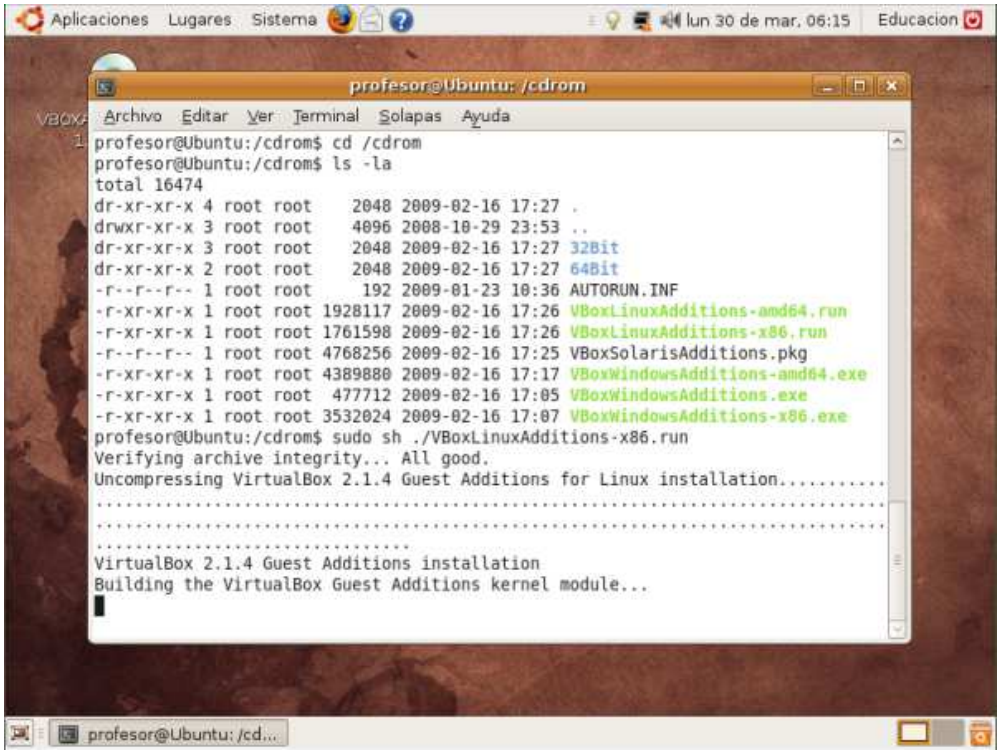
Con este comando se posicionará en la carpeta del disco donde ha sido montada la imagen iso.

ls –la

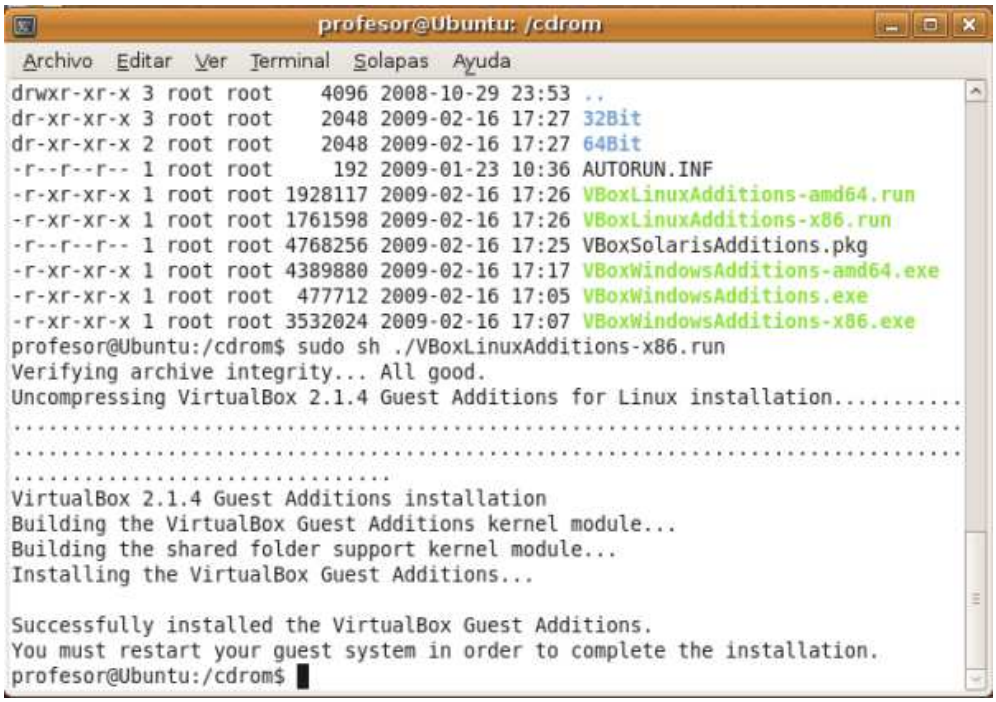
Con este comando observaremos la lista de ficheros y carpetas de la ubicación actual (/cdrom).

sudo sh ./VBoxLinuxAdditions-x86.run

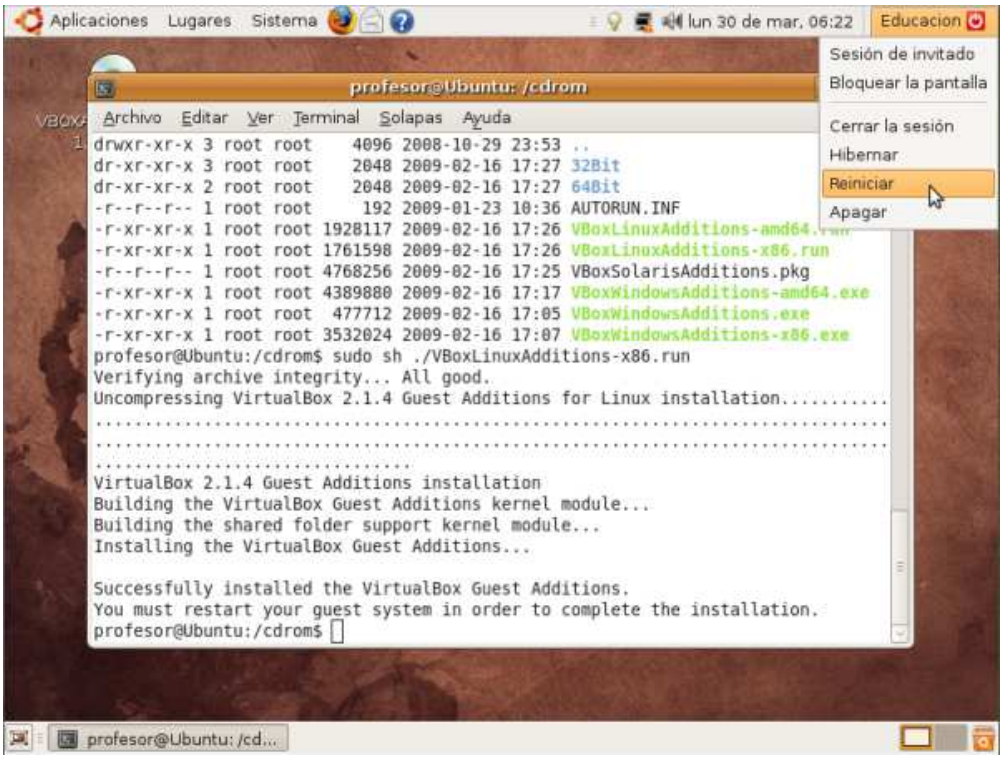
Con este comando ejecutará el script que contiene las VBoxGuestAdditions para Linux. Deberá utilizar el comando **sudo** para ejecutar el script con privilegios de superusuario (root) ya que estamos añadiendo nuevos módulos al kernel (núcleo) de Linux. Más adelante se hablará del comando **sudo**.



Terminada la ejecución del comando anterior se nos mostrará un mensaje indicando que debemos reiniciar el sistema para finalizar la instalación de las VBoxGuestAdditions, tal y como se muestra en la siguiente figura.



Para reiniciar el sistema operativo en nuestra máquina virtual nos dirigimos al icono de apagado y en el menú desplegable seleccionamos **Reiniciar**, tal y como se muestra en la siguiente figura.

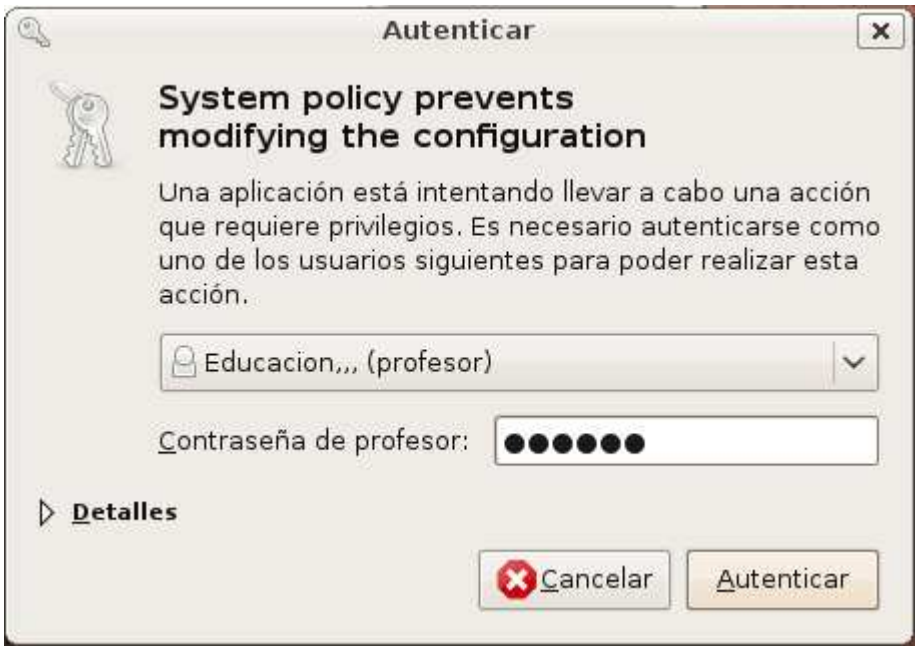


Gestión de usuarios

Para crear un nuevo usuario nos dirigimos al menú **Sistema->Administración->Usuarios y grupos** tal y como podemos ver en la siguiente figura.

A continuación se nos mostrará la ventana de **Configuración de usuarios** que se muestra en la siguiente figura.

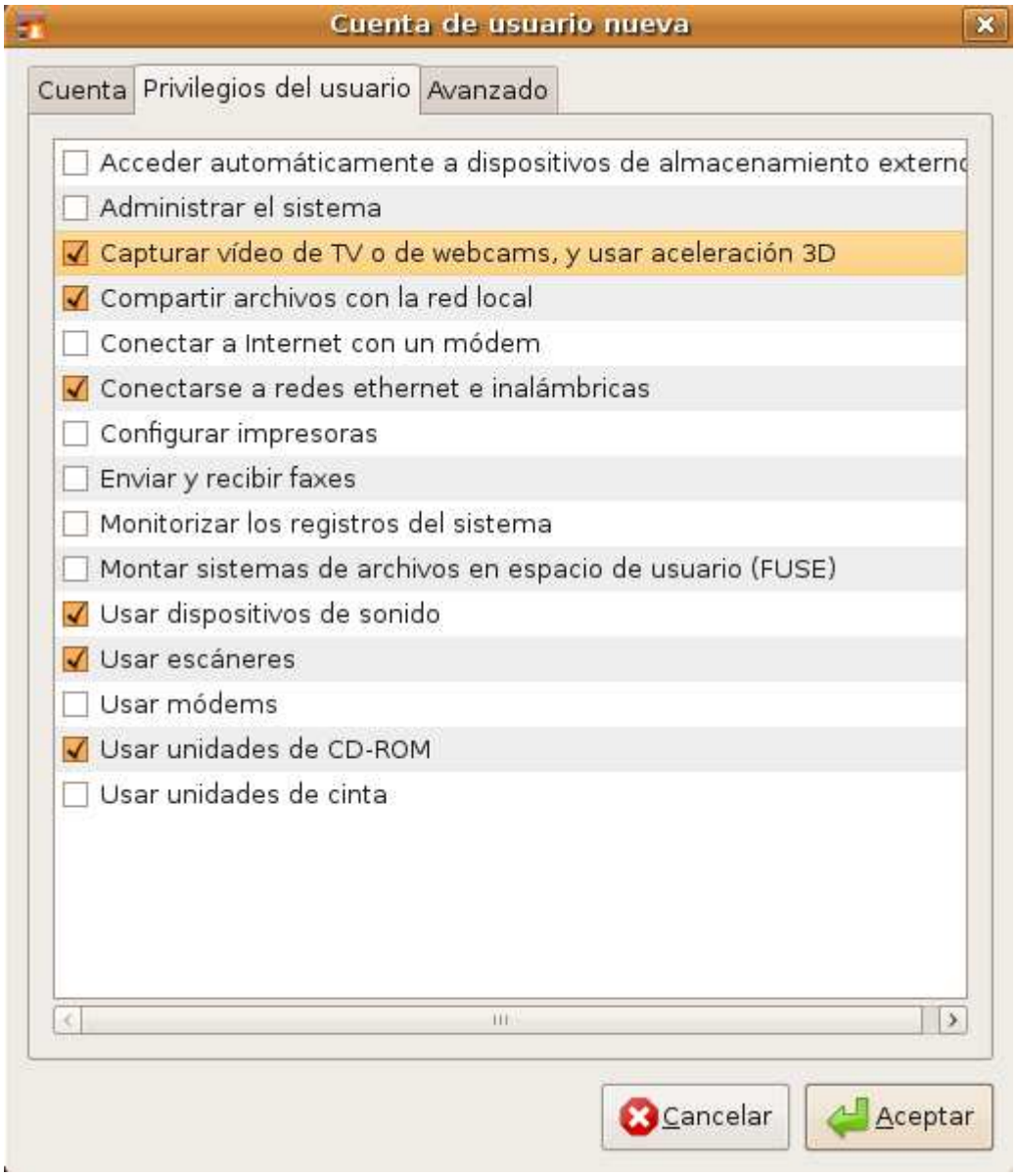
Para poder crear un nuevo usuario deberemos pulsar el botón **Desbloquear**. A continuación se nos mostrará una ventana desde donde se nos advertirá que estamos intentando realizar una acción que requiere privilegios y que necesitamos autentificarnos como un usuario con privilegios de administrador. Hasta ahora en el sistema sólo hay dos usuarios con esos privilegios: el usuario **root** (superusuario por defecto en los sistemas operativos Unix/Linux) y el usuario **profesor** creado durante la etapa 5 del proceso de instalación. Como hemos iniciado sesión con la cuenta **profesor** sólo deberemos introducir la contraseña de éste para que el sistema nos desbloquee la posibilidad de agregar nuevos usuarios.



Una vez introducida la contraseña, se nos muestra la ventana de la aplicación de **Configuración de los usuarios** con los botones de **Añadir usuario** y **Gestionar grupos** desbloqueados. Así mismo podemos ver que la cuenta **root** aparece desbloqueada para poder realizar acciones sobre ella. Pulsaremos sobre el botón **Añadir usuario** para agregar un nuevo usuario.

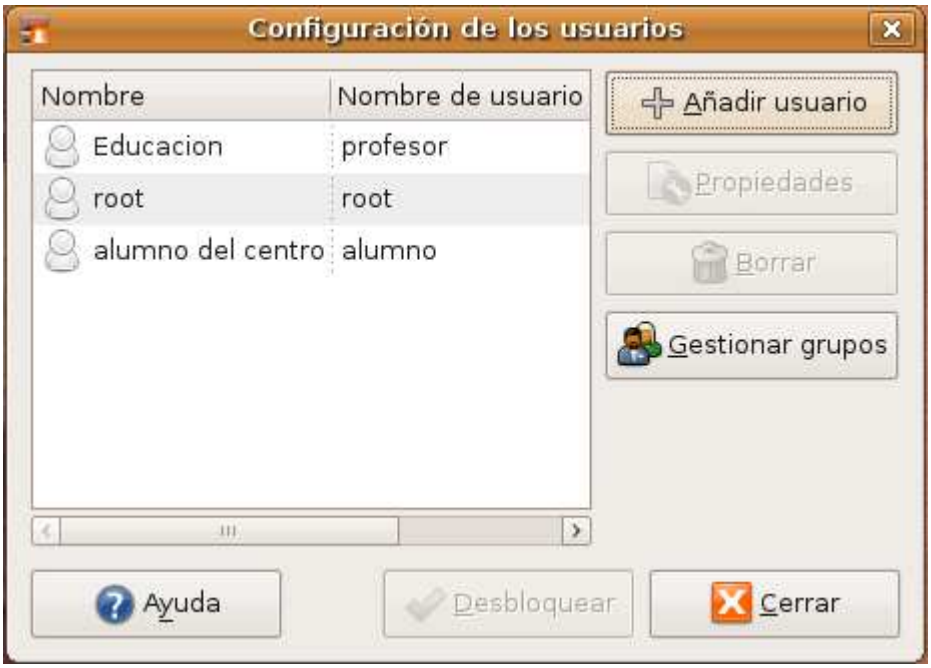
Añadiremos un nuevo usuario sin privilegios de nombre **alumno**. Estableceremos para él una contraseña que deberemos introducir dos veces para comprobar que no se producen errores de tecleo.

En la pestaña **Privilegios del usuario**, estableceremos los privilegios que queramos tenga el nuevo usuario (ej.: usar unidades de CD-ROM, compartir archivos, etc.).

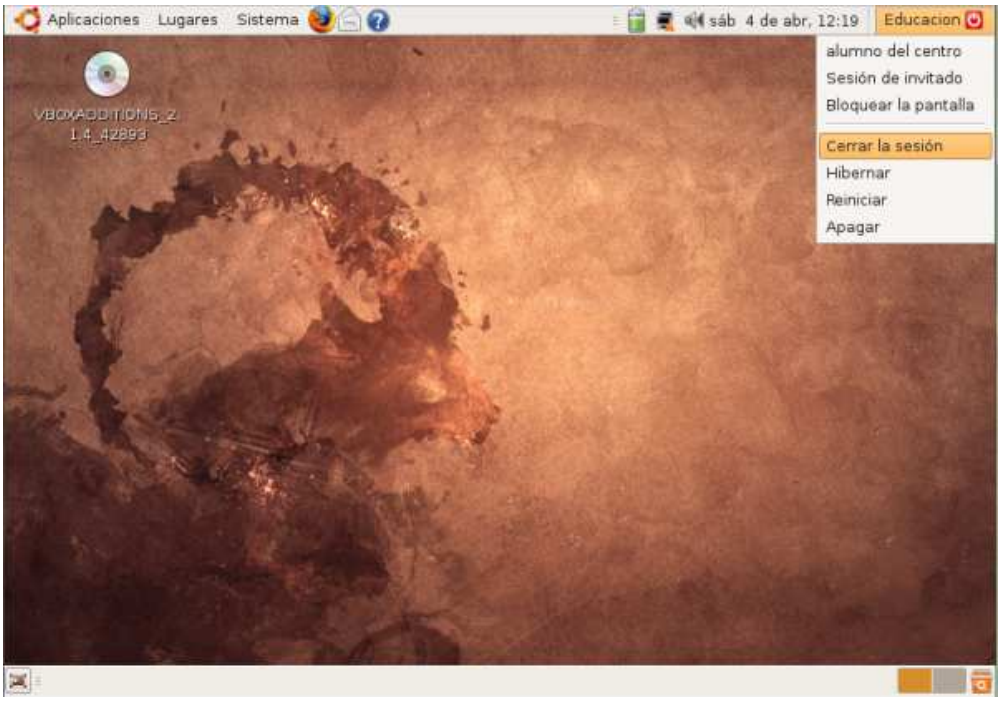


En la pestaña **Avanzado** estableceremos el directorio personal para el nuevo usuario (los directorios personales suelen colgar de la carpeta **/home**), el intérprete de comandos (**/bin/bash**) que se ejecutará cada vez que el usuario lance una terminal, el grupo principal al que pertenecerá el usuario (**users**) y el UID o **número de identificación** del usuario que debe ser único dentro del sistema. Un usuario puede pertenecer a uno o más grupos pero siempre estará asignado a un grupo principal. Algunas de las elecciones que hagamos aquí (contraseña, privilegios, grupo o grupos a los que pertenezca el usuario, entre otros) podrán ser modificadas con posterioridad.

Una vez terminemos de introducir la información del nuevo usuario pulsaremos el botón **Aceptar**. El nuevo usuario aparecerá en la ventana de **Configuración de los usuarios**. Pulsaremos el botón **Cerrar** para salir del programa.



Para probar que hemos creado bien el usuario saldremos de sesión e iniciaremos sesión de nuevo con la cuenta y la contraseña del usuario recién creado (alumno). Para salir de sesión nos dirigiremos al icono de apagado y en el menú desplegable seleccionamos **Cerrar la sesión**, tal y como se muestra en la siguiente figura.



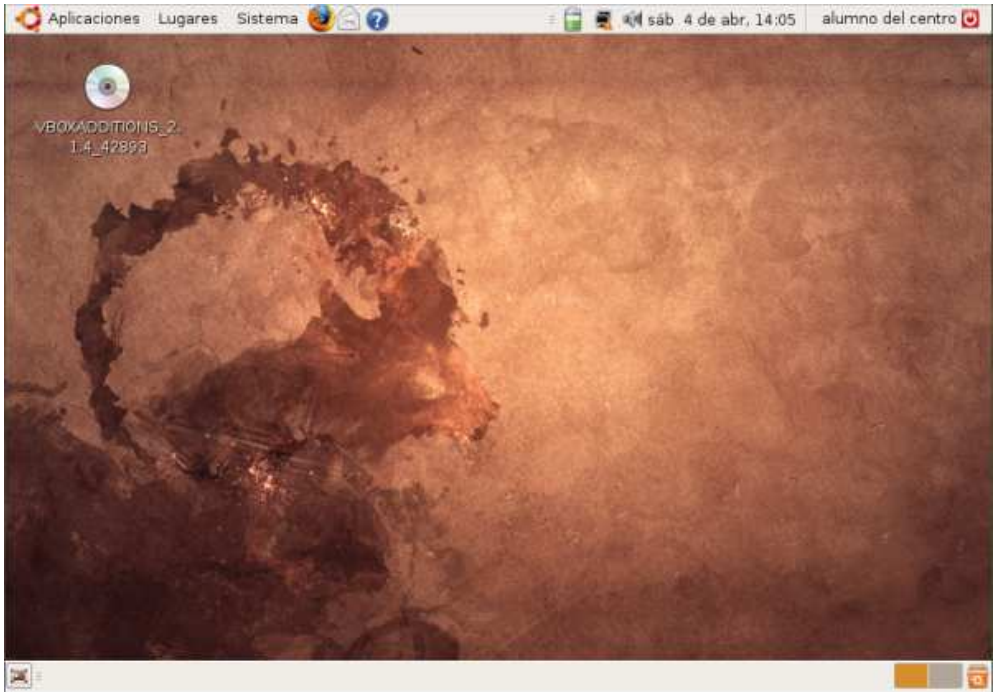
En la pantalla de bienvenida al sistema introduciremos en la caja de texto correspondiente al nombre de usuario el correspondiente al nuevo usuario que acabamos de crear, tal y como se muestra en la siguiente figura.

A continuación introduciremos la contraseña que habíamos seleccionado para el nuevo usuario, tal y como se muestra en la siguiente figura.

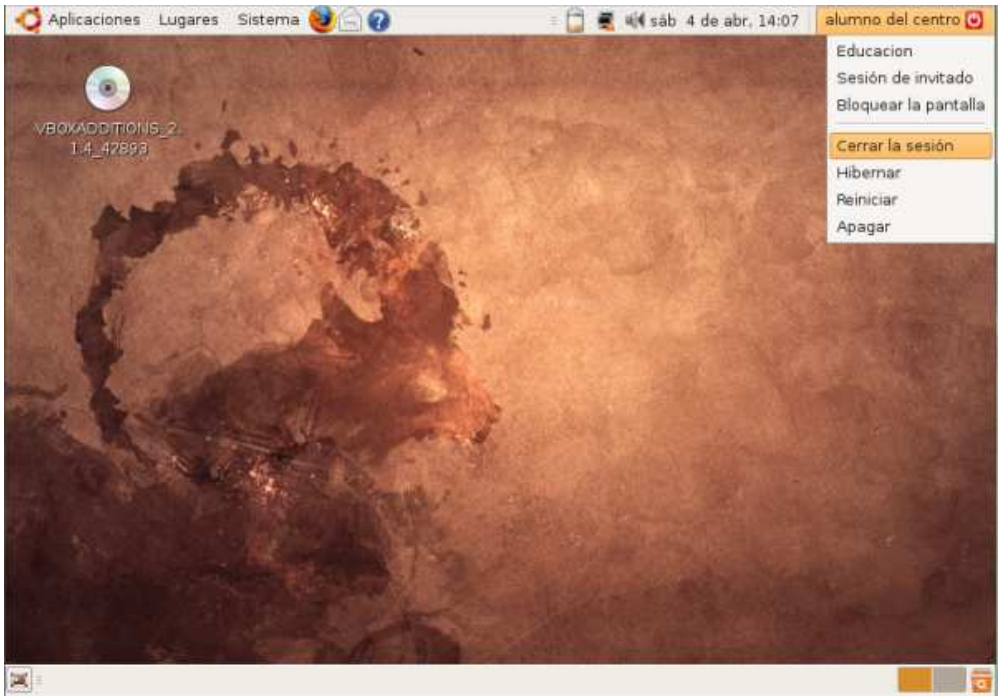
NOTA: Al escribir la contraseña no se muestra el eco de los caracteres tecleados por motivos de seguridad, para que nadie que esté a nuestro alrededor pueda observarla mientras la tecleamos.

Si hemos introducido correctamente la contraseña aparecerá el escritorio del usuario alumno. Vemos que al lado del botón de apagado/encendido aparecerá el nombre del usuario que acaba de iniciar sesión, que será el usuario **alumno**, tal y como podemos ver en la siguiente

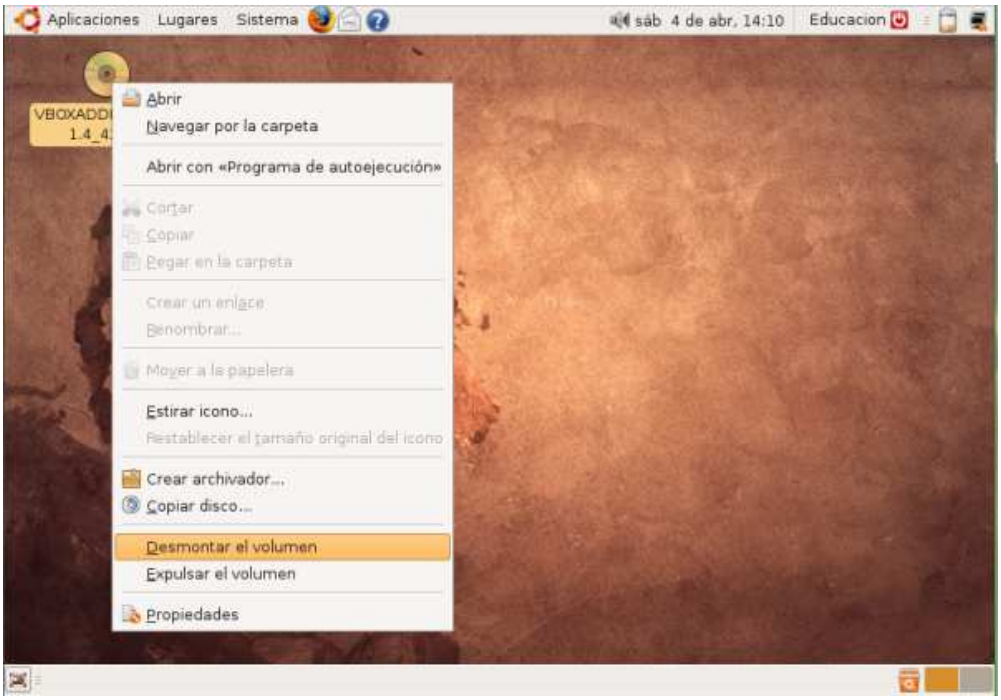
figura.



Una vez comprobado que podemos iniciar sesión con el nuevo usuario sin mayores problemas, saldremos de sesión e iniciaremos sesión de nuevo como usuario **profesor**.



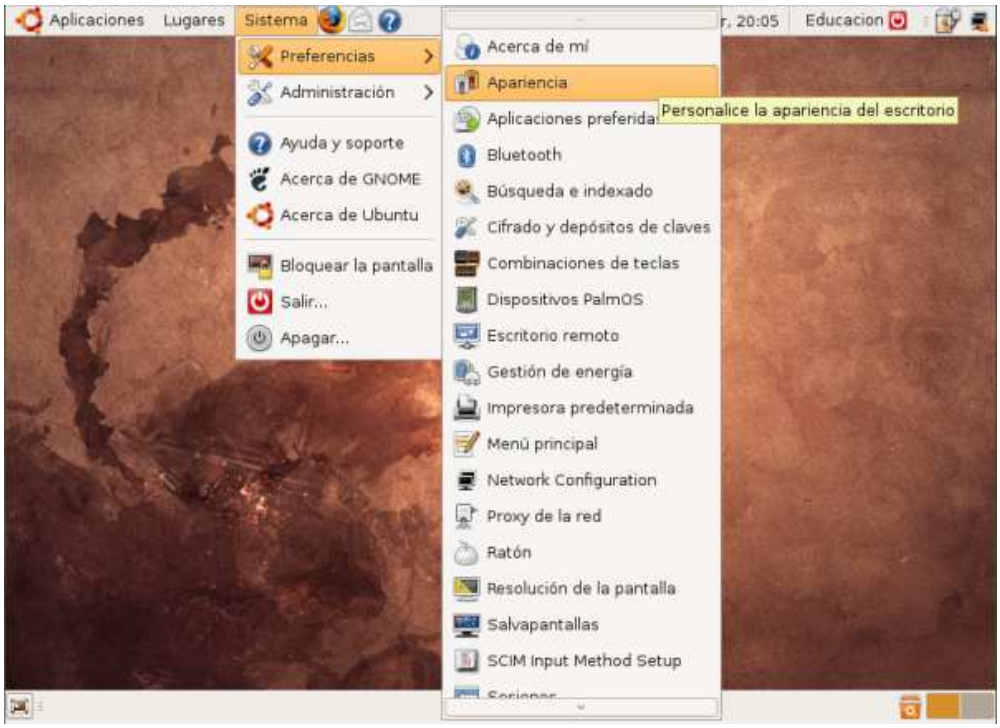
Al iniciar de nuevo sesión como usuario profesor vemos que todavía aparece en el escritorio el icono que representa que tenemos un CD introducido en la bandeja y montado sobre el sistema de ficheros de Ubuntu (concretamente está montado en /cdrom). En nuestro caso no es un CD de verdad sino una imagen ISO de un CD que contiene las VBoxGuestAdditions de VirtualBox para los sistemas operativos Linux. Para expulsar un CD antes tendremos que desmontarlo. Para desmontar el CD hacemos clic con el botón derecho del ratón sobre el icono que representa al CD y aparecerá un menú contextual tal y como se muestra en la siguiente figura. En dicho menú elija la opción **Desmontar el volumen**.



Una vez hecho esto veremos como desaparece el icono anterior del escritorio del usuario **profesor**.

Tras ello configuraremos el entorno de trabajo del usuario con el cual estamos validados en sesión.

En primer lugar sustituiremos la imagen de fondo que por defecto instala Ubuntu por un color de fondo sólido. Para ello acudimos al menú **Sistema->Preferencias->Apariencia**.



Seleccionaremos en la ventana **Preferencias de la apariencia** la pestaña **Fondo** y cogeremos un **Tapiz** sólido (sin tapiz); tras ello en la lista desplegable de **Colores** seleccionaremos **Color sólido** y abriremos la paleta para seleccionar el color que más nos

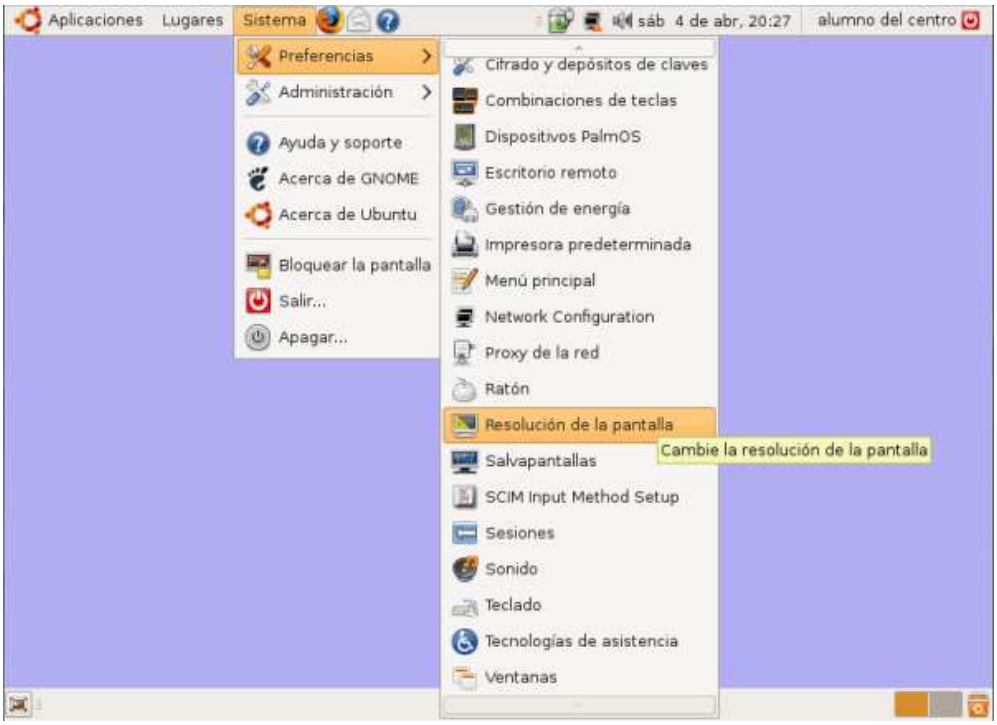
guste como color de fondo. Podremos cambiar el matiz y la saturación del color así como las componentes Rojo, Verde y Azul (RGB). En nuestro caso hemos elegido como color de fondo del escritorio para el usuario profesor un color salmón claro.

Después pulsaremos el botón **Aceptar** y luego el botón **Cerrar** de la ventana de **Preferencias de la apariencia**. Los resultados los podemos observar en la siguiente figura.

Saldremos de sesión como usuario **profesor** e iniciaremos de nuevo sesión como usuario

alumno. Para el usuario alumno cambiaremos su fondo de escritorio por un color sólido como el que se muestra en la siguiente figura.

También podremos cambiar la resolución de la pantalla, para lo cual tendremos que ir al menú **Sistema->Preferencias->Resolución de la pantalla**. En este caso vamos a cambiar la resolución de la pantalla para el usuario alumno.

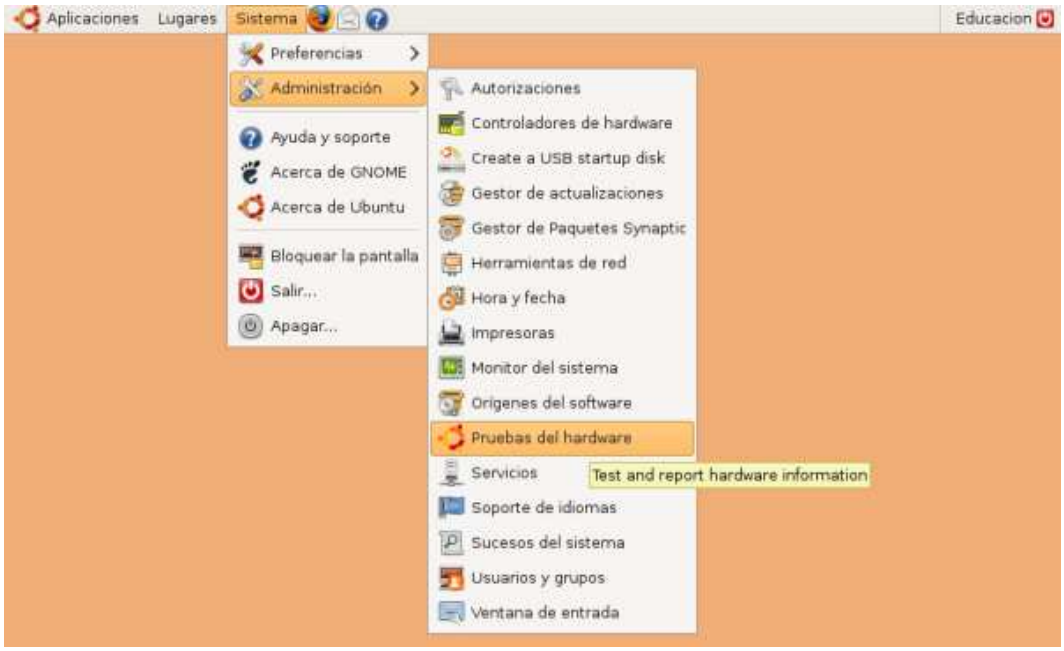


En la ventana de **Opciones de resolución del monitor** aparecen las resoluciones de pantalla soportadas por el hardware gráfico así como sus tasas de refresco. Seleccionaremos en este caso una resolución de pantalla de 1024x768, tal y como se muestra en la siguiente figura.

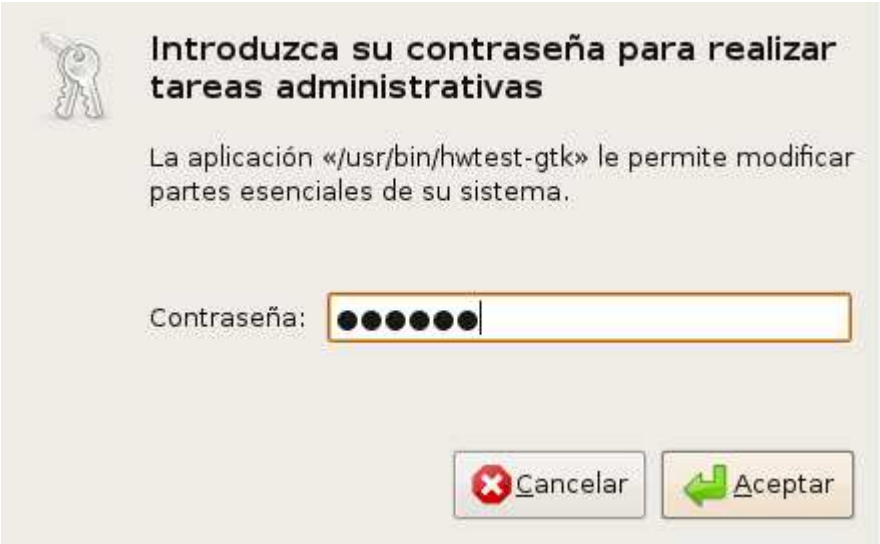
Finalmente cerraremos la sesión del usuario **alumno** y nos autenticaremos con las credenciales del usuario **profesor**.

Instalación del hardware

Otro paso más en la correcta configuración del sistema es la comprobación del correcto funcionamiento del hardware y de los drivers. Ubuntu soporta una gran cantidad de hardware de diferentes fabricantes. Aún así sería bueno comprobar, antes de realizar la instalación, que nuestro hardware está soportado por Ubuntu, cosa que puede hacer en la siguiente dirección: https://wiki.ubuntu.com/HardwareSupport. Para comprobar el correcto funcionamiento del hardware de nuestra máquina seleccionaremos **Sistema->Administración->Pruebas del hardware** tal y como podemos ver en la siguiente figura.



Como la comprobación del hardware es una tarea administrativa, se nos pedirá la contraseña de un usuario con privilegios de administración. La cuenta de usuario **profesor** con la que hemos iniciado sesión es una cuenta con privilegios de administración así que simplemente introduciremos su contraseña.



La aplicación de comprobación del hardware (Hardware Testing) recopila información del hardware que tenemos instalado y a continuación nos propone una serie de pruebas manuales para comprobar que el hardware funciona correctamente. En la siguiente pantalla pulsaremos sobre el botón **Siguiente** para comenzar las pruebas.

Una de las pruebas consiste en verificar si está instalado el driver para la tarjeta de sonido y ésta funciona adecuadamente. Se reproducirá un sonido y si lo escucha adecuadamente pulsará sobre la opción **Sí**, en caso contrario deberá pulsar sobre la opción **No**. Si lo desea puede **Omitir** la prueba y continuar con la siguiente, aunque no vemos razones para que lo haga a menos que el lector no cuente con altavoces en su equipo.

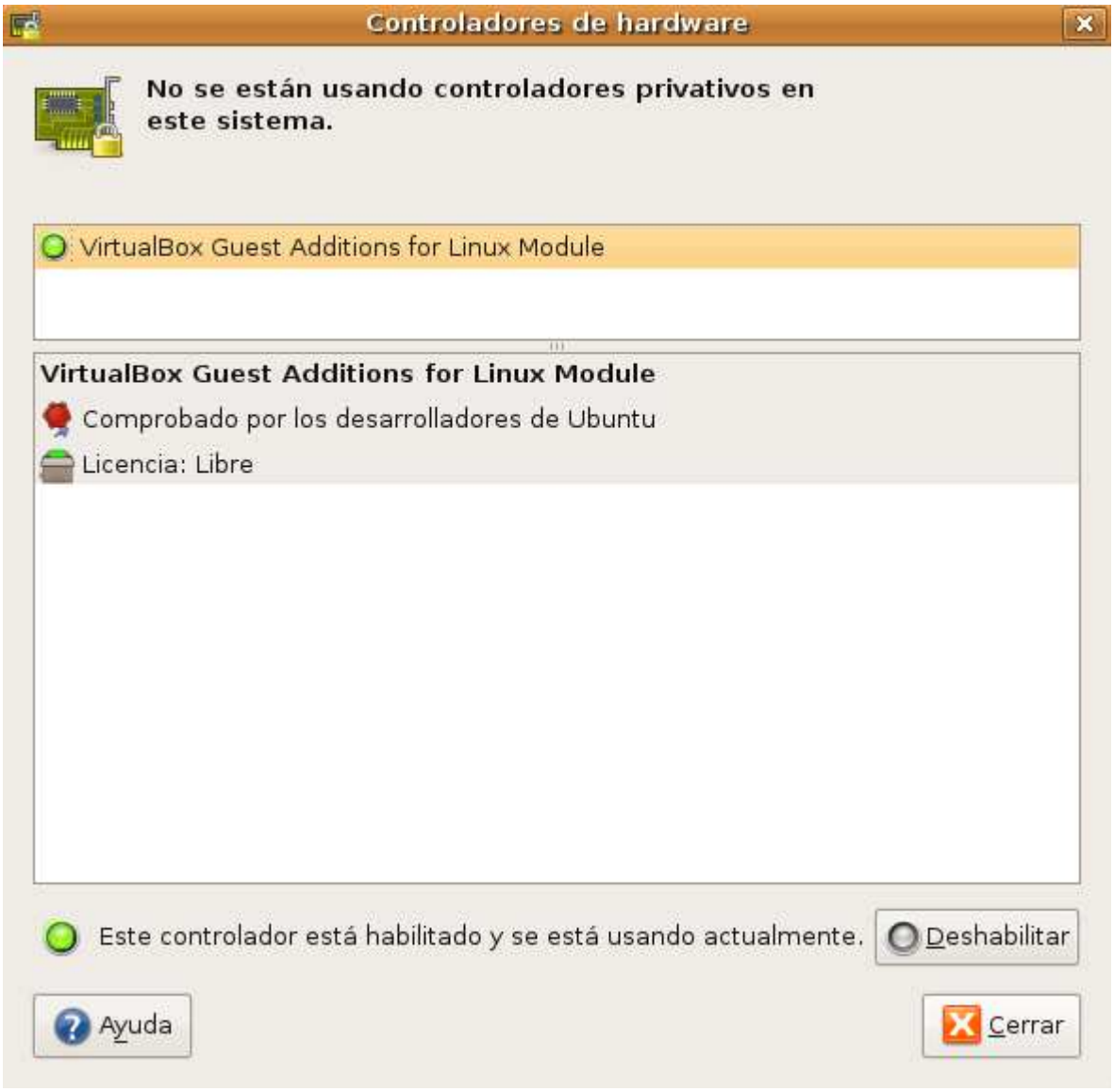
Otra de las pruebas consiste en comprobar la resolución de la pantalla, como se puede

apreciar en la siguiente figura.

Cuando todas las pruebas de hardware hayan concluido, se le mostrará un informe de resultados y la posibilidad de enviar dicho informe a LaunchPad que es un sitio web que permite recopilar la información sobre errores o incompatibilidades del hardware y/o drivers.

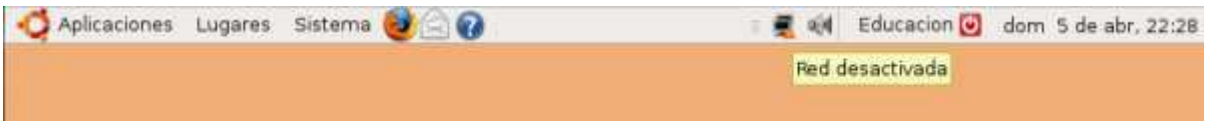
Para comprobar el correcto funcionamiento de los drivers instalados por Ubuntu para el hardware detectado durante el proceso de instalación nos dirigiremos a **Sistema->Administración->Controladores de hardware** tal y como mostramos en la siguiente figura.

Este programa nos muestra los controladores (drivers) instalados y su estado de funcionamiento. En nuestro caso, al hacer la instalación sobre una máquina virtual en VirtualBox, los drivers detectados son los instalados previamente con las VirtualBoxGuestAdditions, los cuales se encuentran funcionando correctamente en el sistema. Sin embargo, en una instalación de Ubuntu sobre máquina física los drivers detectados y su estado de funcionamiento serán distintos a los aquí presentados.



Un elemento especialmente importante es la configuración del interfaz de red.

Cuando se definió la máquina virtual sobre la que estamos desarrollando los contenidos del material, se la dotó de un interfaz de red virtual. De la misma manera, es de esperar, que si el lector desea seguir la documentación realizando la instalación de los Sistemas Operativos en una máquina física, ésta cuente con un interfaz o tarjeta de red. En la siguiente figura se muestra que el icono que representa la aplicación de gestión de la red (Network Manager) nos indica que la red está desactivada.



Para configurar la tarjeta de red seleccionamos en el menú principal **Sistema->Preferencias->Network Configuration** tal y como se muestra en la siguiente figura.

A continuación se mostrará la ventana de **Conexiones de red**. En ella se muestran los interfaces (tarjetas) de red instalados en el sistema. Seleccionaremos el interfaz de red **eth0** y pulsaremos sobre el botón **Editar**.

Dado que en nuestro caso asumiremos que NO disponemos de un servidor DHCP en nuestra red, deberemos especificar manualmente el direccionamiento IP oportuno para que el equipo que estamos configurando pueda navegar por Internet, seleccionando en la pestaña **Ajustes de IPv4** de la ventana de la imagen inferior la opción "**Manual**" en el desplegable correspondiente, e indicando a continuación la "**Dirección IP**", "**Máscara de red**", "**Puerta de enlace predeterminada**" y "**Servidores DNS**" oportunos que nos permitan navegar en el

entorno en el que estemos instalando este equipo.

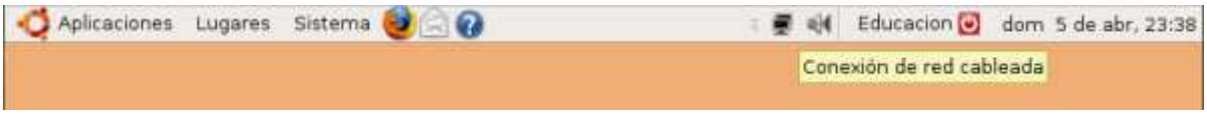
En nuestro caso, tal y como vemos en la ventana de la imagen superior hemos utilizado los siguientes valores:

	Datos Configuración Equipo Red Usuario
Dirección IP	192.168.1.100
Máscara de Red	255.255.255.0 (máscara de 24 bits)
Puerta de Enlace	192.168.1.254
Servidores DNS	194.179.1.101 195.55.30.16

Después de realizar la configuración del adaptador **eth0** pulsaremos el botón **Aceptar**.

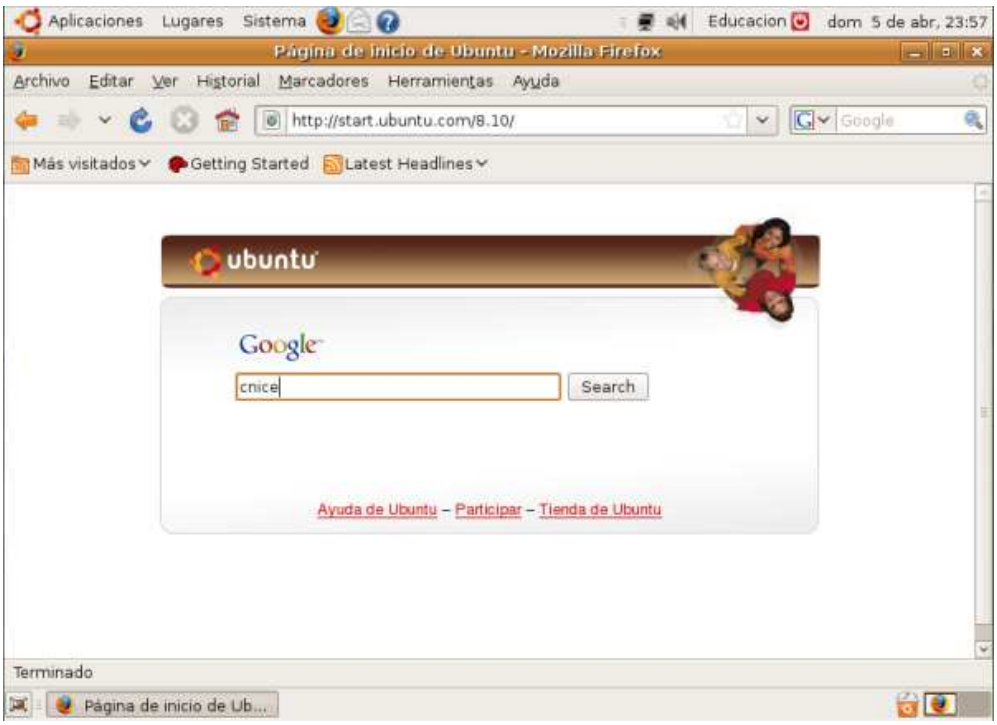
NOTA: Evidentemente los valores especificados en la ventana anterior NO serán válidos en el entorno de trabajo del lector, así pues se deberá realizar una traslación de las direcciones IP especificadas en la ventana de la imagen anterior, a las direcciones IP que tiene que asociar para seguir los contenidos del material; para disponer de un mayor conocimiento del entorno en el cual utiliza el material, puede ejecutar desde otro equipo cualquiera de su red (o desde el equipo anfitrión en caso de estar utilizando máquinas virtuales) en una ventana de la aplicación "Terminal" el comando "ifconfig –a" ("ipconfig /all" en una ventana de DOS de Windows), para obtener información relativa a la "**Dirección IP**", "**Máscara de subred**", "**Puerta de enlace predeterminada**" y "**Servidores DNS**" que debe indicar al adaptador de red **eth0** de Linux, a partir de la información obtenida de la ejecución del comando anterior sobre dicho equipo de su red. Básicamente deberá mantener los parámetros "**Máscara de subred**", "**Puerta de enlace predeterminada**" y "**Servidores DNS**", y modificar el parámetro "**Dirección IP**", con una dirección IP del mismo rango, pero que no esté ocupada en este instante.

Después de hacer los ajustes anteriores veremos que el icono de gestión de red (Network Manager) ya no aparece con el símbolo de advertencia lo cual nos indica que la red está activada.



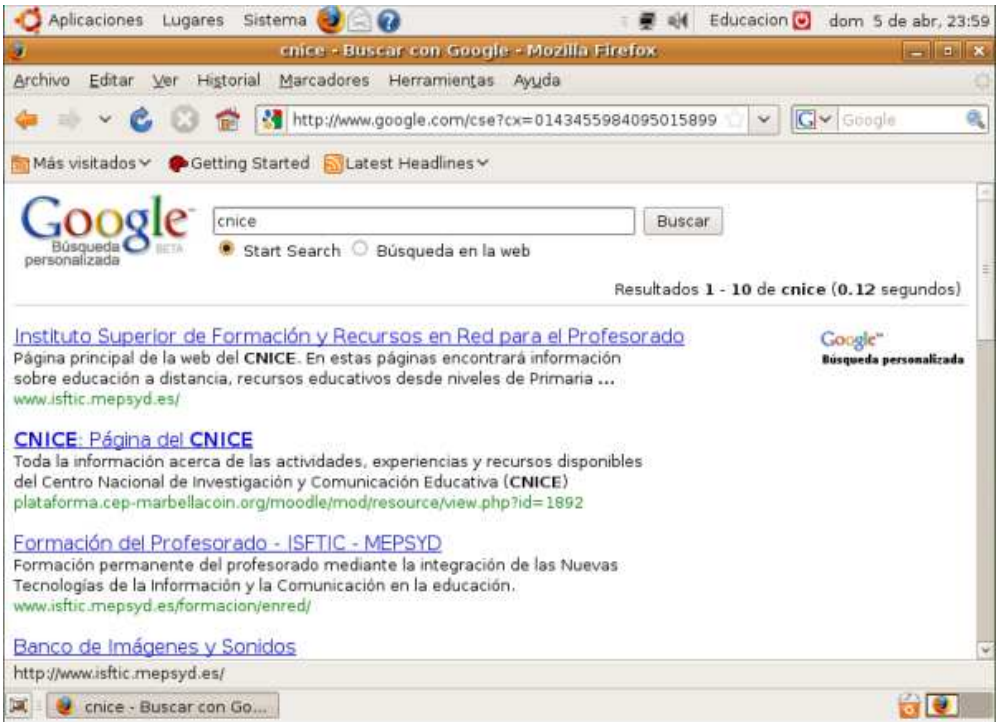
Para probar que la red funciona y que tenemos acceso a Internet localizaremos al navegador web Firefox en la barra de menús.

Haremos clic sobre el icono de la aplicación Firefox e inmediatamente a continuación aparecerá la ventana del navegador que podemos ver en la siguiente figura.



NOTA: Si no se cargase por defecto la página web reseñada, podríamos probar a navegar una dirección URL cualquiera, por ejemplo "http://www.google.es".

Al cargarse la página anterior podemos asegurar que la conexión de red está perfectamente configurada y que tenemos acceso a Internet. Desde la página web que se carga por defecto introduciremos la palabra "cnice" como expresión de búsqueda de Google y pulsamos sobre el botón **Search**. En pocos instantes aparecerá la lista de enlaces devueltos por el buscador ante la expresión de búsqueda anterior.

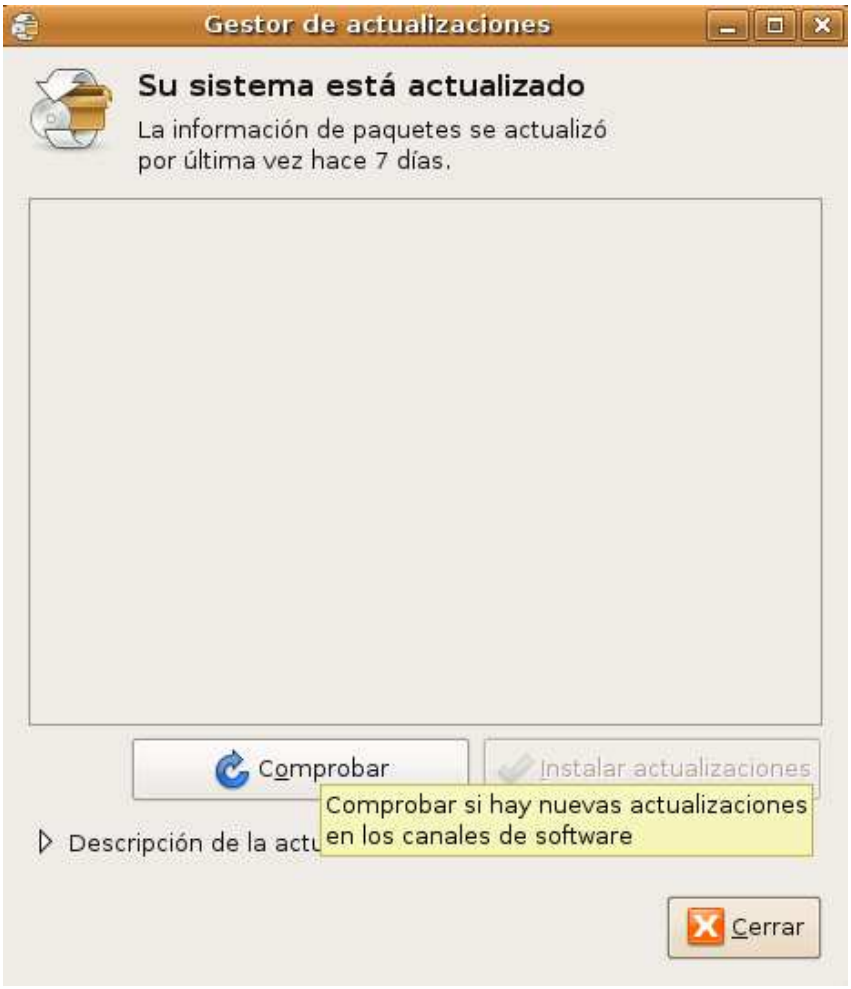


Pulsaremos sobre el primer enlace y se cargará al poco la página web del IFSTIC (antiguo CNICE).

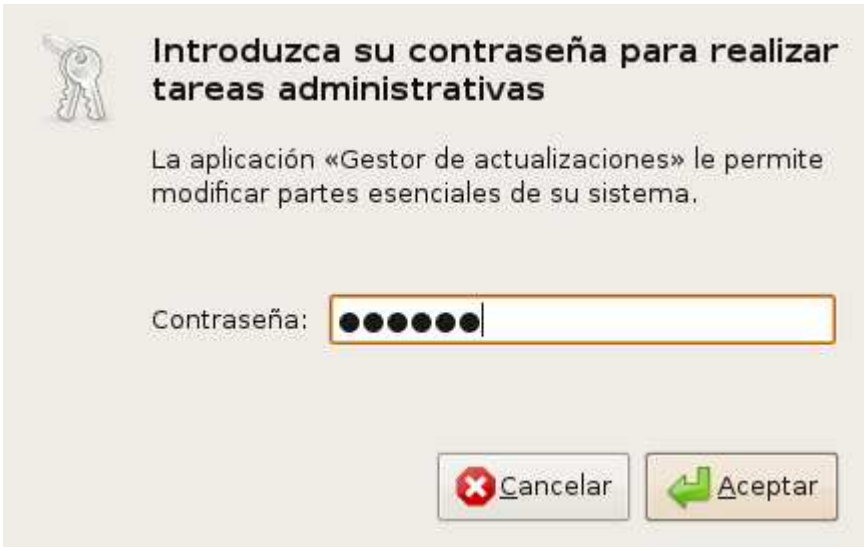
Actualizaciones

Una de las tareas a realizar en el proceso de post-instalación del sistema operativo es la actualización de las aplicaciones instaladas. Todas las aplicaciones suelen tener pequeños errores (bugs) que se suelen ir corrigiendo a medida que salen nuevas versiones. En otras ocasiones aparecen parches (conocidos como service packs en Windows) que arreglan errores reportados por los usuarios. Ubuntu integra un gestor de actualizaciones software que instala de forma automática las actualizaciones existentes para las aplicaciones instaladas en el sistema. Para acceder al **Gestor de actualizaciones** deberá seleccionar la opción de menú principal **Sistema->Administración->Gestor de actualizaciones** tal y como puede verse en la siguiente figura.

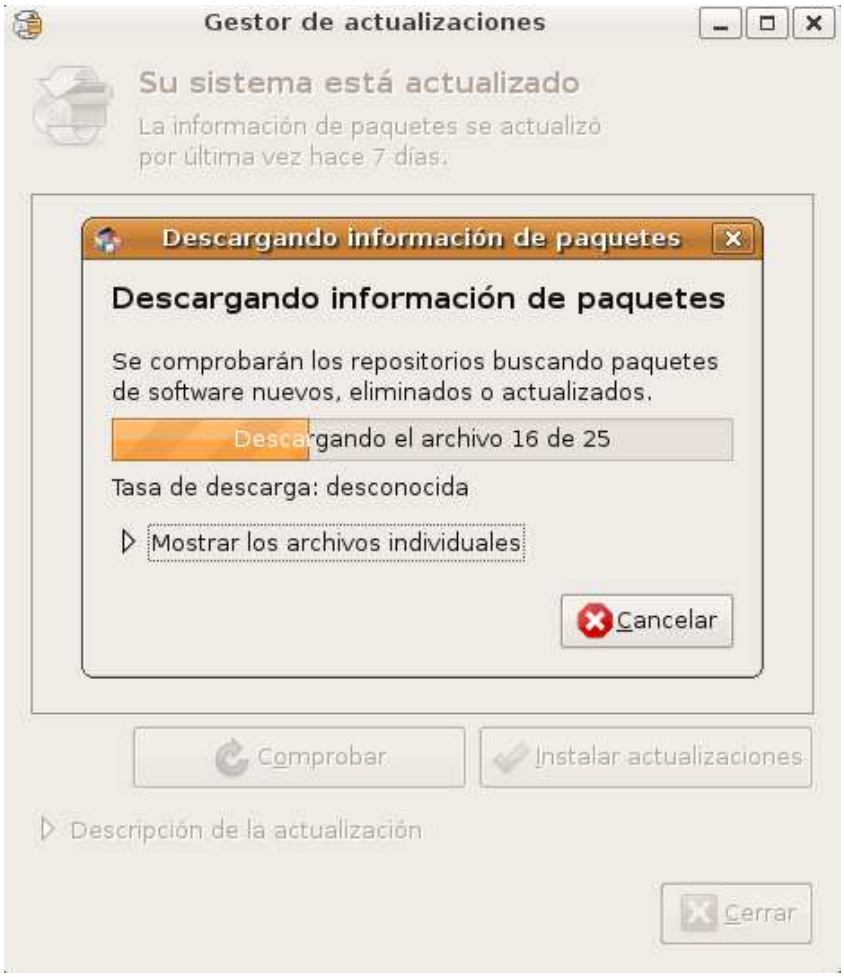
Al lanzarse el gestor de actualizaciones nos mostrará la última vez que se lanzó y podremos verificar si hay nuevas actualizaciones para instalar en el equipo si pulsamos el botón **Comprobar**, tal y como se muestra en la siguiente figura.



Al ser una tarea administrativa la instalación de las actualizaciones de software, se nos pedirá la contraseña de un usuario con privilegios de administración. Como el usuario **profesor** es un usuario con privilegios de administración, introduciremos directamente su contraseña.



A continuación el software de **Gestión de actualizaciones** se conectará vía Internet con los repositorios de software de Ubuntu. Si se detectan versiones actualizadas de paquetes de software instalados, se procederá a descargar la información de dichos paquetes desde los repositorios de Internet.



Una vez descargadas las actualizaciones a nuestro equipo, podremos elegir cuál o cuáles de ellas se instalarán, simplemente marcando o desmarcando la casilla de verificación que se encuentra a la izquierda del nombre de cada una de ellas. Junto con cada actualización viene una pequeña descripción a cerca de su cometido. Una vez haya elegido las actualizaciones a instalar pulse el botón **Instalar actualizaciones** para que dé comienzo el proceso.

La instalación de las actualizaciones comienza con la descarga de los paquetes. Este proceso podrá ser más o menos largo dependiendo del número de paquetes a actualizar y de la tasa de descarga, pero normalmente no bajará de 10 minutos.

Después de la descarga de los paquetes comenzará el proceso de actualización. Este proceso, al igual que el anterior, podrá tardar varios minutos dependiendo de los paquetes a actualizar, pero normalmente tampoco bajará de 10 minutos.

Una vez terminado el proceso de instalación de paquetes, se mostrará un mensaje indicándonos que es necesario reiniciar el sistema.

Una vez reiniciemos el sistema el proceso de actualización se habrá completado.

Si deseamos configurar desde qué repositorios de software se descargan las aplicaciones y las actualizaciones del software instalado tendremos que seleccionar **Sistema -> Administración -> Orígenes del software**.

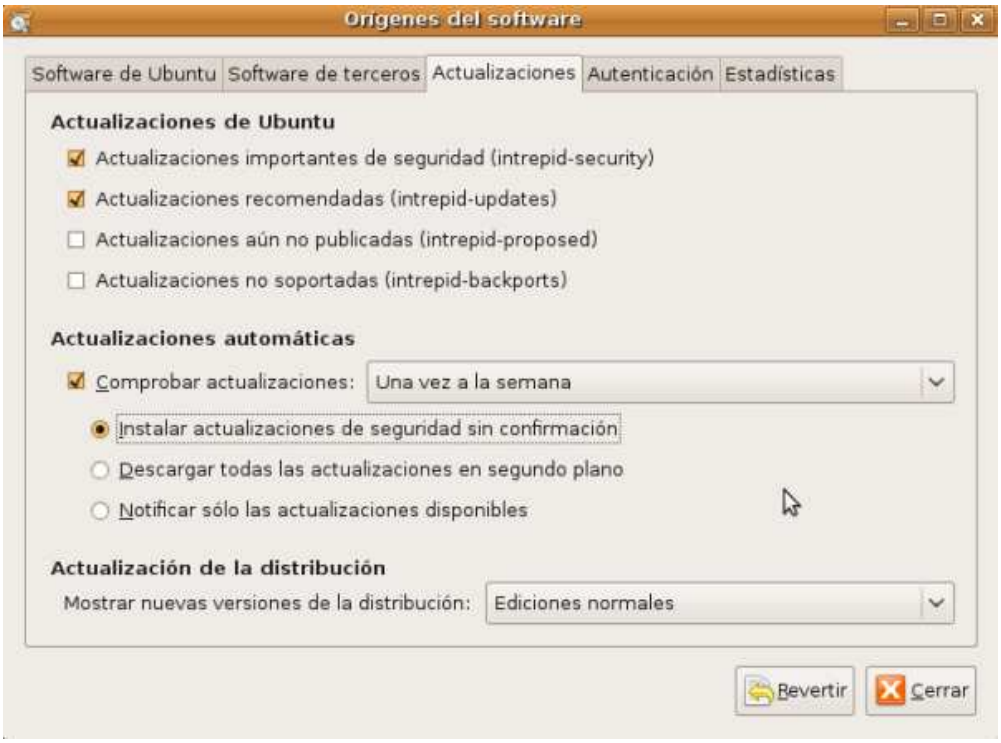
Hay miles de programas disponibles que permiten satisfacer las necesidades de los usuarios de Ubuntu. Muchos de estos programas se almacenan en archivos de software comúnmente denominados repositorios. Los repositorios hacen que sea muy fácil de instalar nuevo software en Ubuntu usando una conexión a Internet, al tiempo que proporcionan un alto nivel de seguridad, ya que cada uno de los programas disponibles en los repositorios está ampliamente probado y construido específicamente para cada versión de Ubuntu.

Los repositorios de software de Ubuntu se organizan en cuatro áreas o "componentes", según el nivel de apoyo ofrecido por Ubuntu, y si el programa en cuestión se ajusta o no a la filosofía se software libre de Ubuntu. Estas áreas son:

- **Principal**: Software oficialmente soportado.
- **Restringido**: Software soportado que no está disponible bajo una licencia completamente.
- **Universal**: Software mantenido por la comunidad de usuarios de Ubuntu y que no es software oficialmente soportado.
- **Multiverso**: Software que no es libre.

El DVD de instalación de Ubuntu contiene software de los repositorios Principal y Restringido. Si nuestro sistema tiene conexión a Internet podrá acceder a muchos otros programas. Utilizando la herramienta de gestión de paquetes ya instalada en nuestro sistema, podremos buscar, instalar y actualizar cualquier programa directamente desde Internet sin la necesidad de tener el DVD de Ubuntu.

En nuestro caso nos ubicaremos sobre la pestaña "Actualizaciones", y modificaremos la frecuencia de la descarga, seleccionando en el desplegable correspondiente por la opción "Una vez a la semana", y seleccionando además el radio botón "Instalar actualizaciones de seguridad sin confirmación", tal y como vemos en la siguiente figura, tras lo cual pulsaremos sobre el botón "Cerrar".



NOTA: Desde la aplicación de **Orígenes de software** podremos seleccionar los componentes que vamos a instalar (Principal, Universal, Restringido, Multiverso) y desde qué servidores, todo ello desde la pestaña **Software de Ubuntu**. Desde la pestaña **Software de terceros** podrá añadir orígenes de software de terceros ubicados en Internet o bien software de terceros ubicado en CD/DVD. Desde la pestaña **Actualizaciones** podremos indicar qué actualizaciones de software deseamos instalar, si se habilitan o no las actualizaciones automáticas y con qué frecuencia se realiza la comprobación de actualizaciones, y si el software se instala automáticamente o bien si se pide confirmación al usuario antes de instalarlo.

Instalar un cortafuegos

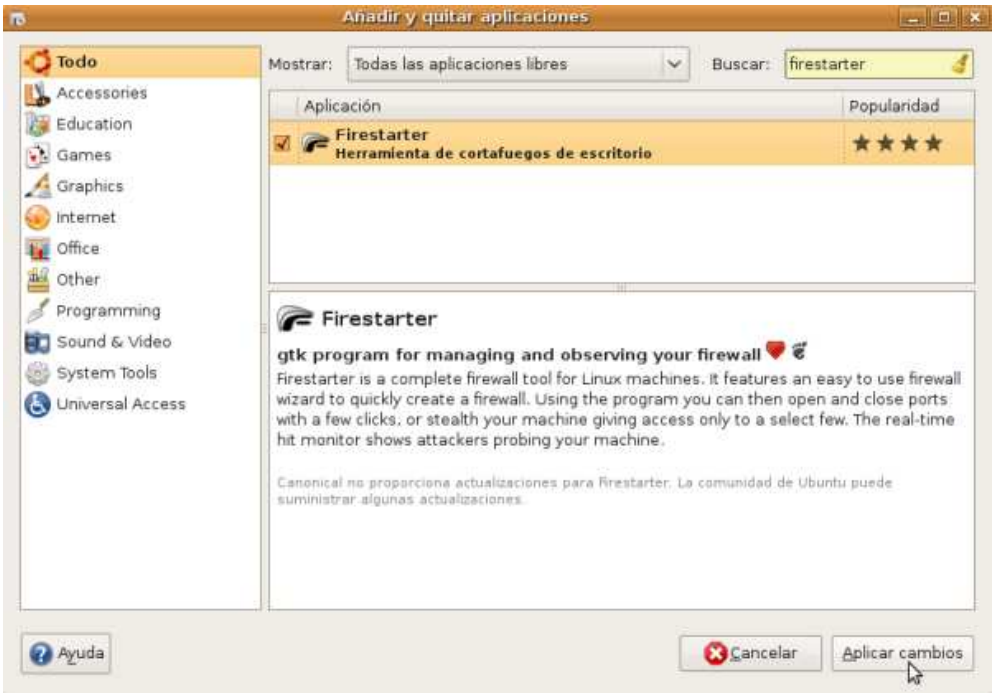
Para proteger nuestro sistema de ataques desde la red, deberemos instalar un cortafuegos (firewall). En nuestro caso instalaremos un cortafuegos personal. El cortafuegos personal es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre dicho ordenador y el resto de la red, y viceversa. El principio de funcionamiento del cortafuegos es permitir el tráfico de red saliente que determine el usuario y denegar el tráfico de red entrante que pueda comprometer la seguridad de nuestro sistema.

Para instalar el software del cortafuegos utilizaremos el **Gestor de aplicaciones.** Para ello seleccionaremos la opción **Aplicaciones->Añadir y quitar...** de la barra de menús, tal y como se muestra en la siguiente figura.

Desde el **Gestor de aplicaciones** seleccionaremos en el desplegable **Mostrar** la opción **Todas las aplicaciones libres**, y tras ello escribiremos en la caja de texto **Buscar** el nombre de la aplicación que deseamos instalar. En nuestro caso esta aplicación se denomina **Firestarter**. Firestarter es una herramienta cortafuegos completa para sistemas operativos Linux. Esta herramienta incluye un asistente que nos permite crear y configurar rápidamente un cortafuegos. Utilizando este programa se pueden abrir o cerrar puertos, y comprobar los intentos de acceso que se están realizando en tiempo real.

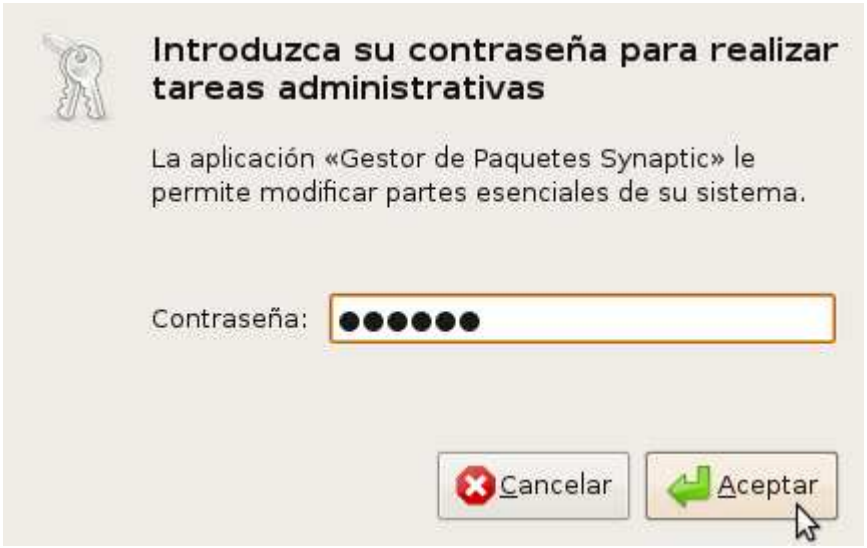
Si hacemos clic sobre la casilla de selección a la izquierda del nombre de la aplicación **Firestarter** veremos una pantalla como la de la siguiente figura.

En ella se nos informa que la comunidad de usuarios de Ubuntu proporciona soporte y actualizaciones de seguridad, las cuales también se habilitarán. Pulsaremos sobre el botón activar y veremos una pantalla semejante a la de la siguiente figura.



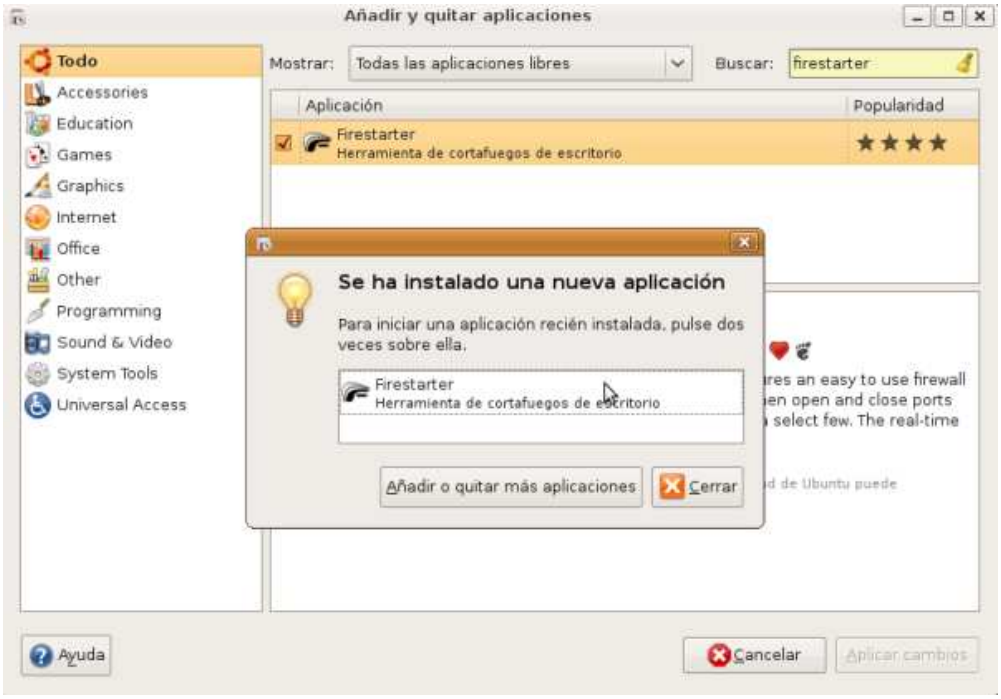
Si pulsamos sobre el botón **Aplicar cambios** comenzará el proceso de instalación del cortafuegos personal. Se nos pedirá primero confirmación sobre las aplicaciones que van a ser instaladas, que en este caso es una sola (**Firestarter**). Pulsaremos sobre el botón **Aplicar**.

Como la instalación del cortafuegos es una tarea administrativa de la máquina, a continuación se nos pedirá la contraseña del usuario **profesor** para realizar esta tarea, tal y como mostramos en la siguiente figura.

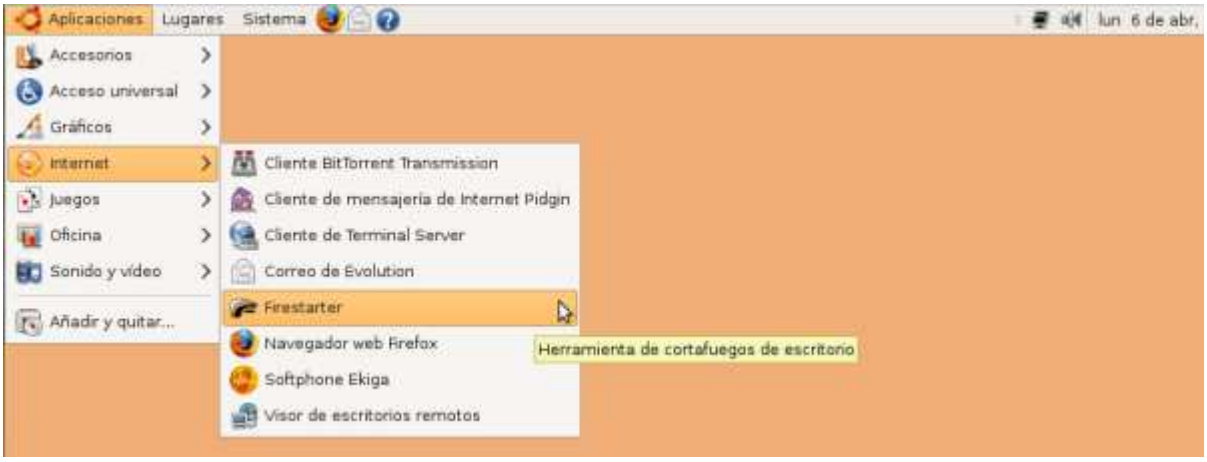


Una vez introducida la contraseña del usuario **profesor**, comenzará el proceso de instalación de la misma con la descarga e instalación de los paquetes que la componen.

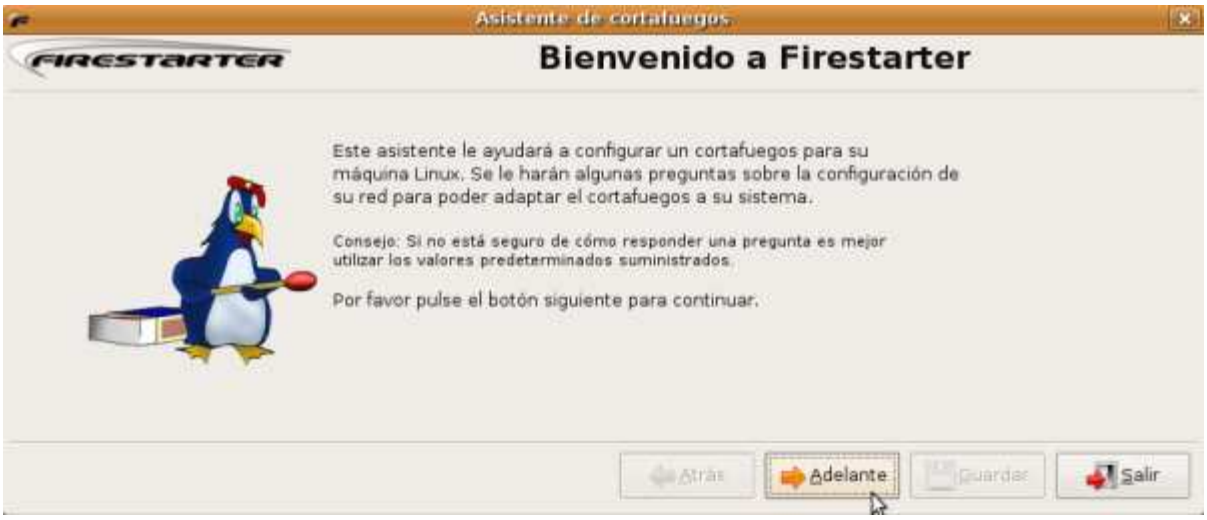
Una vez terminado el proceso de instalación, veremos una pantalla como la siguiente. Pulse el botón **Cerrar** para cerrar la ventana y salir del **Gestor de aplicaciones**.



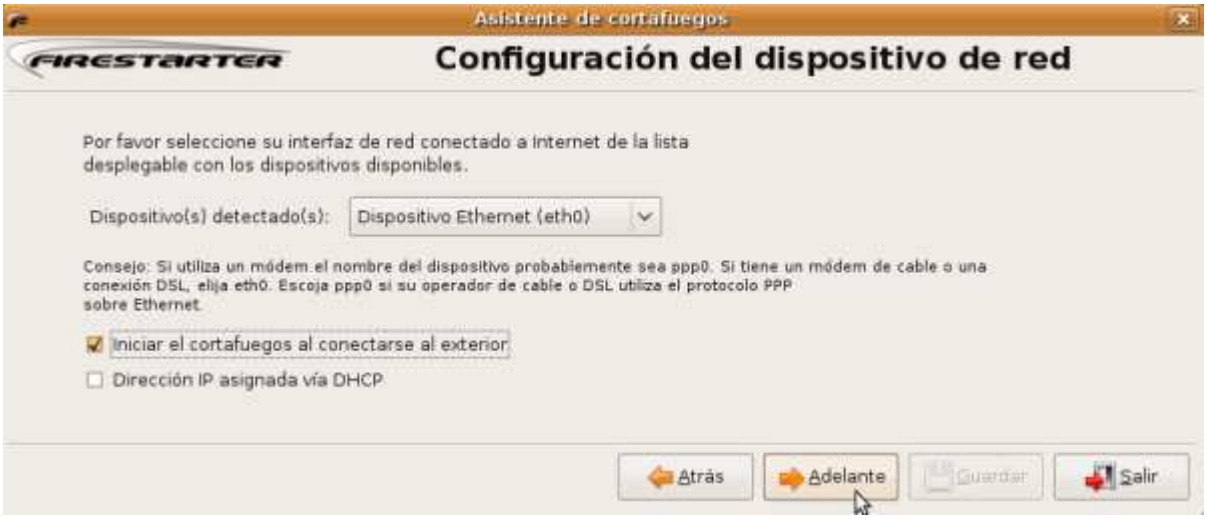
El software de cortafuegos recién instalado se agregará a la categoría **Internet** del menú de **Aplicaciones**. Para lanzarlo seleccionamos **Aplicaciones->Internet->Firestarter**.



A continuación aparecerá el asistente que nos permitirá configurar el cortafuegos para adaptarlo a nuestra máquina Linux. Pulsaremos el botón **Adelante** para continuar.

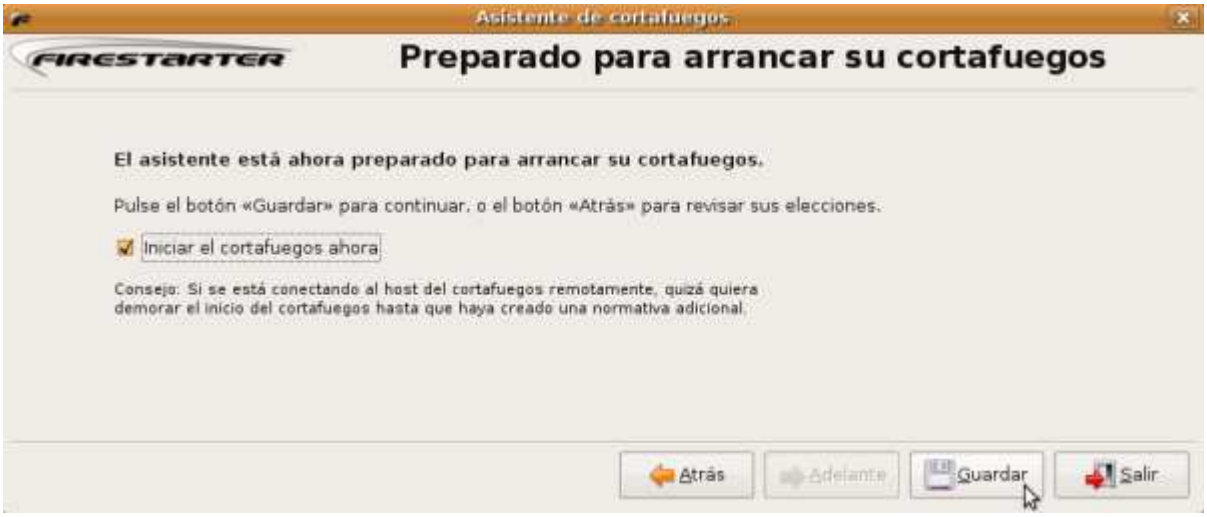


A continuación seleccionaremos sobre qué dispositivo de red deseamos activar el cortafuegos. En nuestro caso dicho dispositivo será la tarjeta de red identificada como **Dispositivo Ethernet (eth0)**. También marcaremos la opción de **Iniciar el cortafuegos al conectarse al exterior** y dejaremos desmarcada la opción **Dirección IP asignada vía DHCP**, ya que en nuestro caso configuramos una dirección IP estática para el equipo.



Una vez hecho esto pulsaremos el botón **Adelante**. En la siguiente pantalla NO marcamos **Activar la compartición de la conexión a Internet**, y pulsaremos directamente en ella sobre el botón **Adelante**.

Finalmente, en la última pantalla del asistente marcaremos la opción **Iniciar el cortafuegos ahora** y pulsaremos el botón **Guardar**.



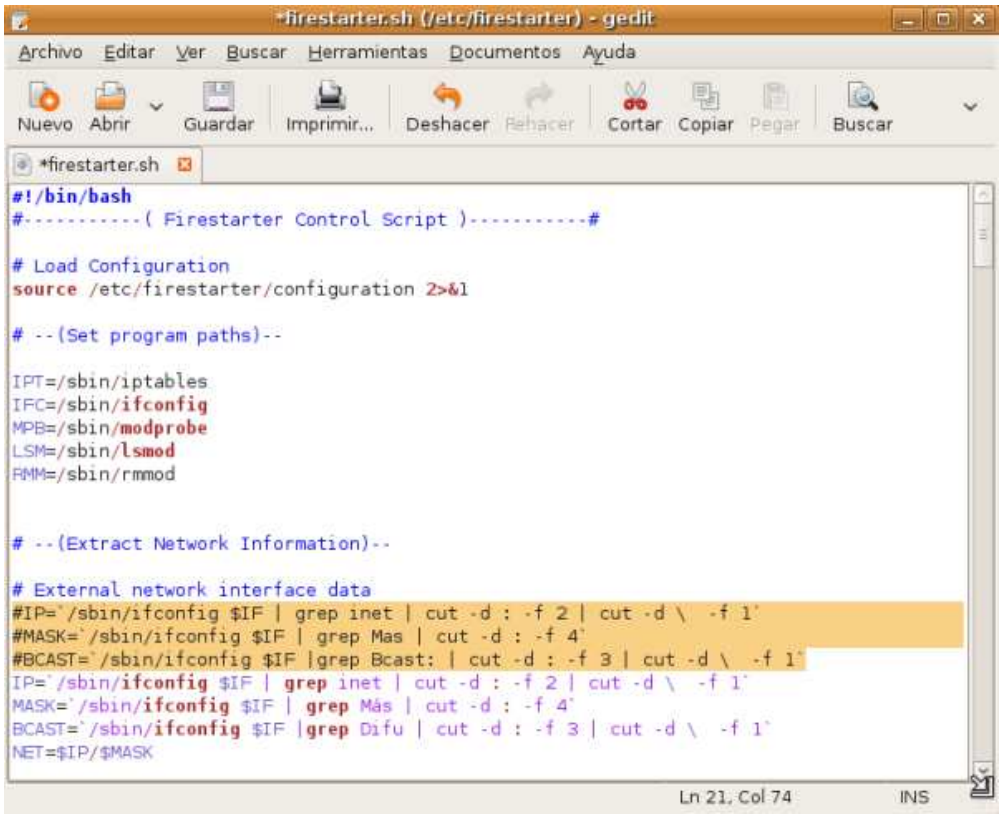
Desafortunadamente aparece una ventana que nos muestra un error indicándonos que no se pudo arrancar el cortafuegos debido a que el dispositivo **eth0** (la denominación de Ubuntu para nuestra tarjeta de red) no está preparado. Realmente la tarjeta de red se encuentra preparada y funciona correctamente pero todo ello se debe a un error de un script de configuración del software de cortafuegos.

Para subsanar este problema necesitamos modificar el script de Firestarter que se encuentra en **/etc/firestarter** denominado **firestarter.sh.** Este es un fichero de texto y debemos editarlo con un editor de texto como por ejemplo el **gedit.** Al tratarse el fichero **firestarter.sh** de un fichero que sólo tiene permisos de edición para el usuario **root**, debemos de utilizar el comando **gksu** para asumir privilegios de administración. Para ello lanzaremos una Terminal y desde ella invocaremos el siguiente comando:

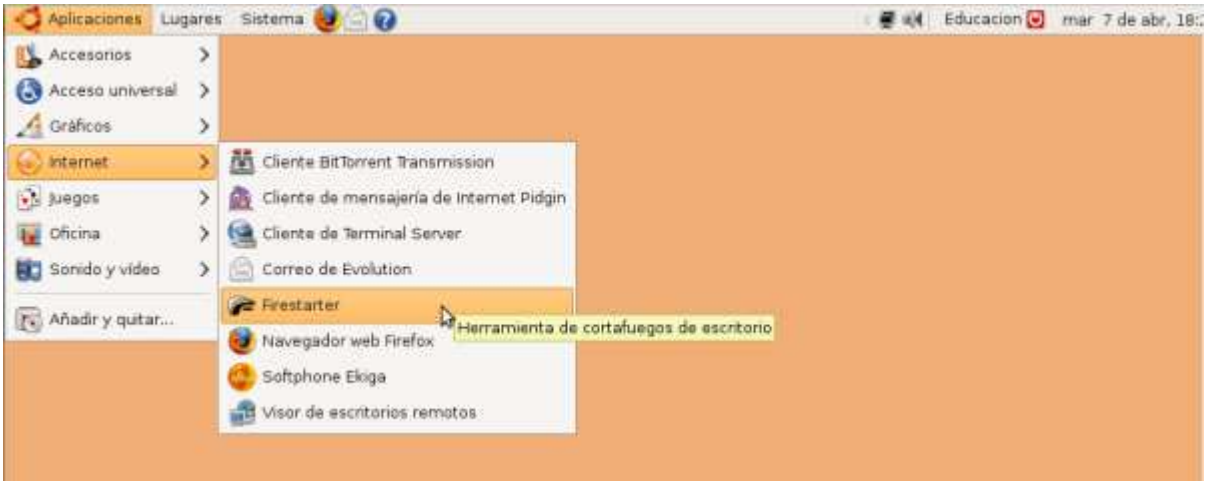
gksu gedit /etc/firestarter/firestarter.sh

Aparecerá la ventana del editor que se muestra a continuación con el fichero mencionado cargado en la misma. Localice las líneas que aparecen resaltadas en la siguiente figura. En el fichero original aparecerán sin el carácter **#** como primer carácter de las mismas. Copie esas tres líneas y péguelas inmediatamente a continuación de la última. Añada el carácter **#** al comienzo de las tres líneas originales y en la segunda de las líneas localice la palabra **Mas** y sustitúyala por la palabra **Más**; en la tercera de las líneas copiadas localice la palabra **Bcast** y

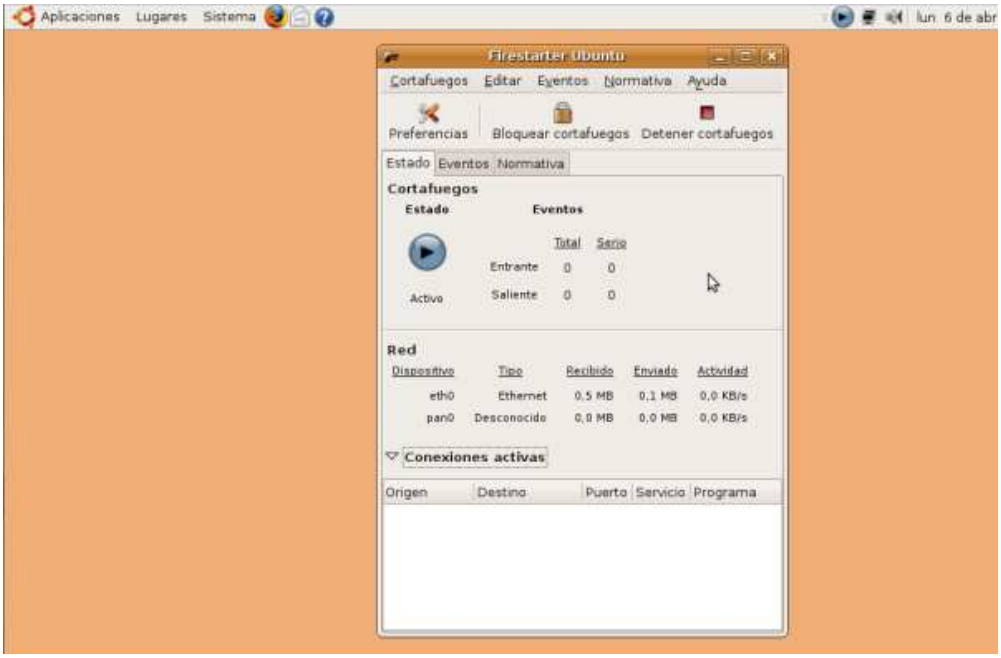
sustitúyala por **Difu**. Después de realizar los cambios el fichero debe de quedar como se muestra en la siguiente figura.



Una vez hecho esto, guarde el archivo pulsando sobre el icono del disquete en la barra de herramientas y cierre la ventana. Vuelva de nuevo a iniciar la aplicación de **Firestarter** tal y como se muestra en la siguiente figura.

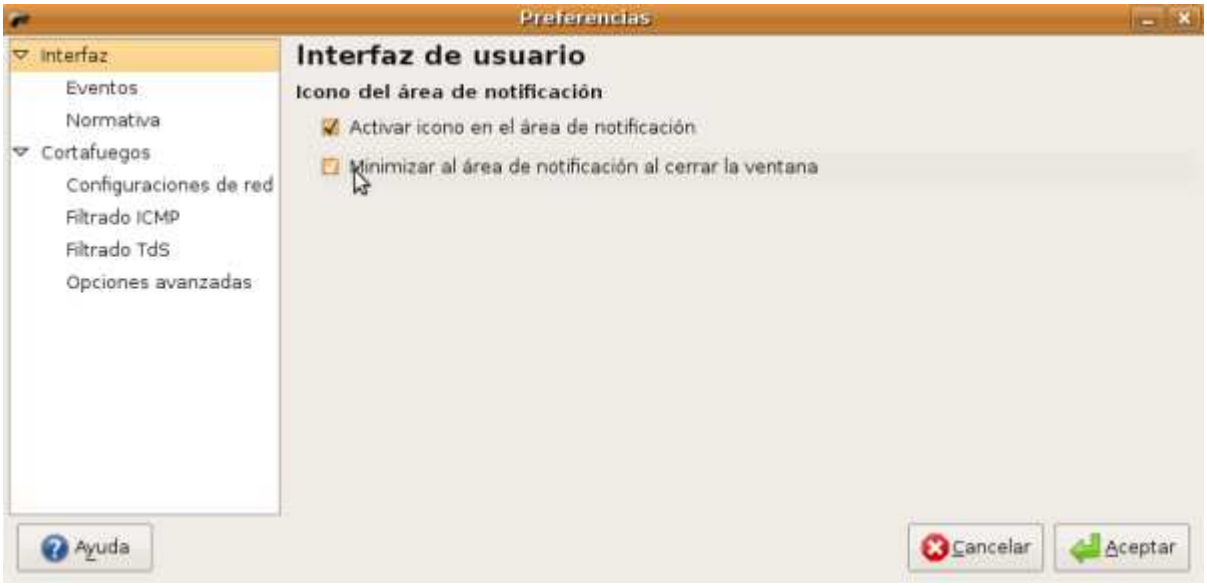


Como se muestra en la siguiente figura, esta vez sí se lanzará el Firestarter sin errores.



Esta vez, como podemos comprobar, el cortafuegos está activo. Para configurarlo pulsaremos sobre el icono **Preferencias** del menú de herramientas de la aplicación.

En la ventana de preferencias, dentro del apartado **Interfaz**, activaremos la casilla **Minimizar al área de notificación al cerrar la ventana**, para que al cerrar ésta no se cierre el programa de cortafuegos, sino que quede minimizado en el área de notificación.



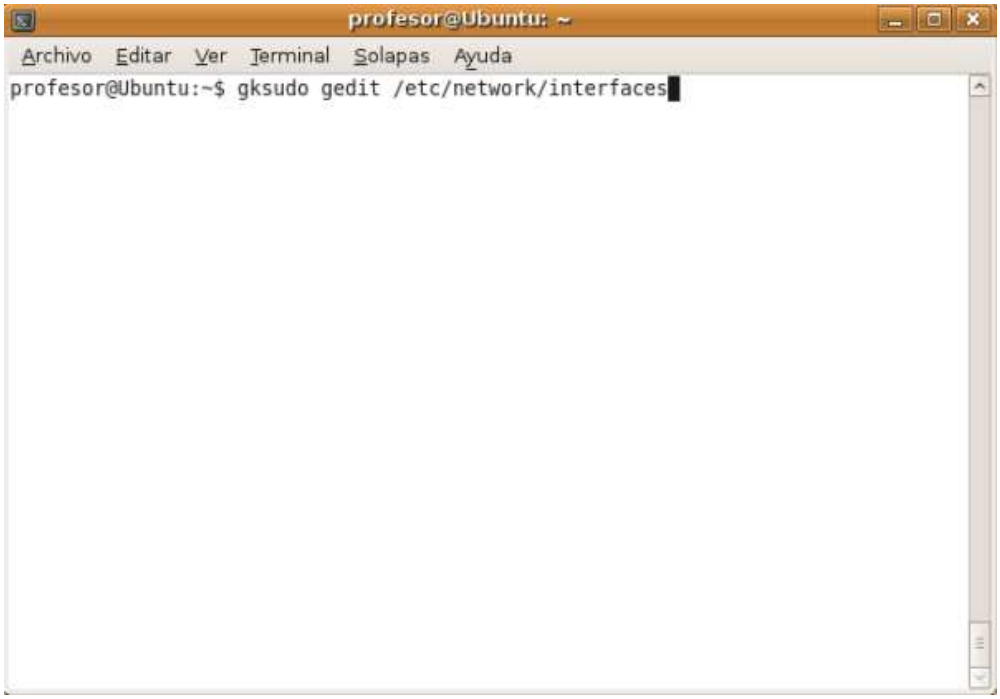
Después seleccionaremos, dentro del menú Cortafuegos, la opción **Filtrado ICMP**. El filtrado **ICMP** (Protocolo de Mensajes de Control de Internet) nos va a permitir restringir la llegada de mensajes de control impidiendo potenciales ataques DoS (Denegación de Servicio). Dentro de las opciones de configuración del **Filtrado ICMP** marcaremos la casilla **Activación filtrado ICMP** y marcaremos las excepciones de filtrado que se muestran en la siguiente figura.

Después pulsaremos **Aceptar**. Para más información sobre las opciones de configuración del este cortafuegos le recomendamos dirigirse a la ayuda de Ubuntu.

Tal y como tenemos configurado nuestro cortafuegos, una vez que salgamos de sesión, éste dejará de funcionar, al ser una aplicación que lanza manualmente el usuario. Sin embargo, para realizar una protección efectiva de nuestro sistema querremos que el cortafuegos entre

en servicio tan pronto como se inicie el Sistema Operativo y que ningún usuario que no tenga privilegios de administración pueda detenerlo, dejando vulnerable a nuestro equipo. Aunque Firestarter está preparado para lanzarse como servicio al inicio durante el proceso de inicialización del sistema operativo, no se lanza debido a una serie de factores. Para lograrlo deberemos realizar una serie de ajustes. En primer lugar modificaremos el fichero **/etc/network/interfaces** para indicar al sistema durante el proceso del arranque qué interfaces de red se iniciarán y con qué direccionamiento IP cada uno. Este proceso lo realiza el comando **ifup**, el cual es lanzado por los scripts de inicio de los niveles de ejecución de Linux en los que la red está habilitada. Este comando cuando se lanza con la opción **–a** desde dichos scripts inicializa todos los interfaces de red configurados como **auto** en el fichero **/etc/network/interfaces.** De esta manera lo que intentamos realizar es que la asignación de IP a la interfaz de red sea una configuración de sistema más que una configuración de usuario. Para ello abriremos una Terminal y en ella escribiremos el siguiente comando.

gksu gedit /etc/network/interfaces



Aparecerá la ventana del editor que se muestra a continuación con el contenido actual del fichero **/etc/network/interfaces** cargado en la misma. Añada las siguiente líneas:

auto eth0

iface eth0 inet static

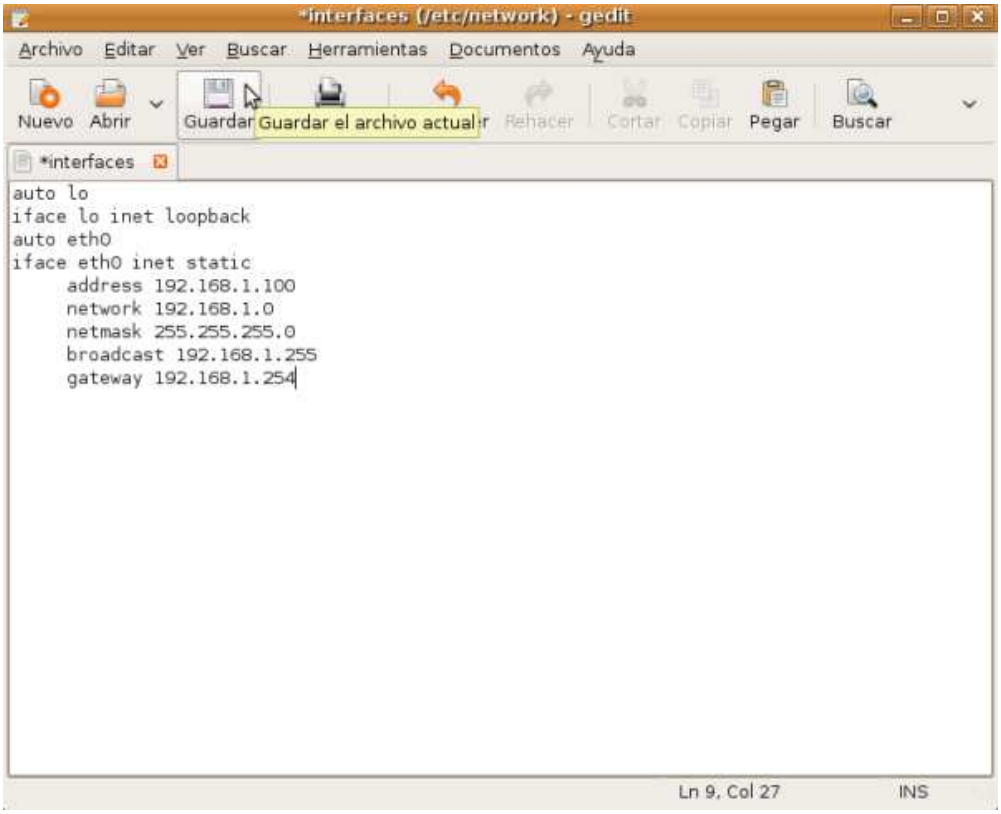
address 192.168.1.100

network 192.168.1.0

netmask 255.255.255.0

broadcast 192.168.1.255

gateway 192.168.1.254

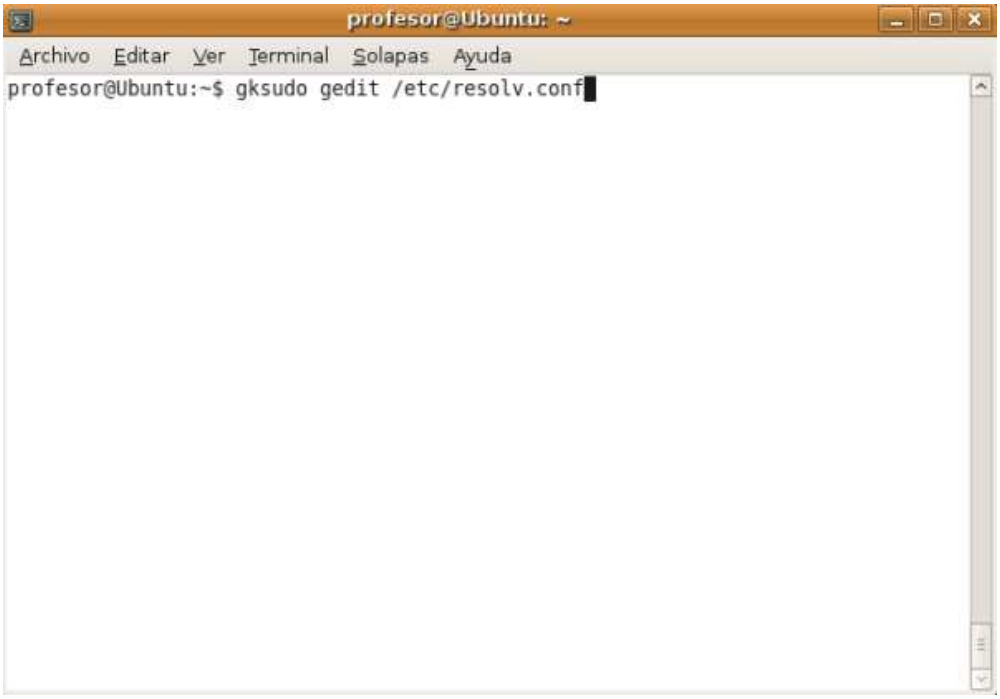


Si el esquema de direccionamiento de su red es diferente al que seguimos en este ejemplo utilice los valores propios de su red, es decir:

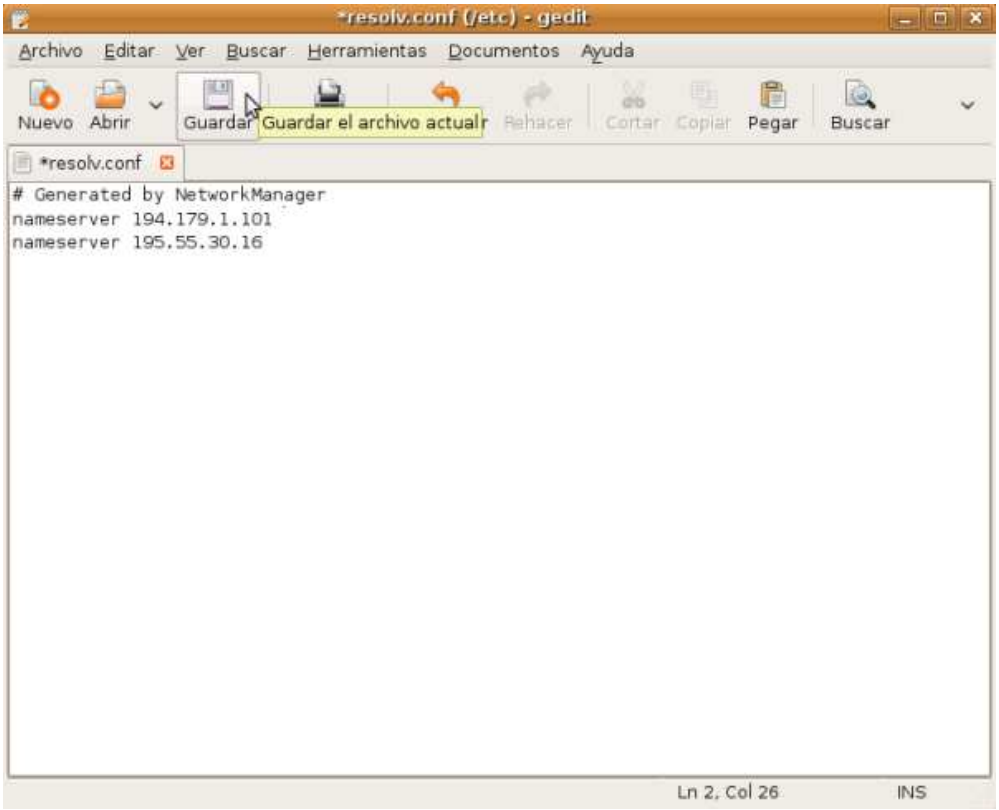
	Datos Configuración Ejemplo	Datos Configuración Particulares
address	192.168.1.100	IP EQUIPO EN SU RED
network	192.168.1.0	DIRECCIÓN DE RED DE SU RED
netmask	255.255.255.0	MÁSCARA DE RED EN SU RED
broadcast	192.168.1.255	DIRECCIÓN DE DIFUSIÓN EN SU RED
gateway	192.168.1.254	PUERTA DE ENLACE DE SU RED

Una vez hechos los cambios oportunos en el fichero, guárdelo. En el fichero anterior no se introduce información sobre los DNS. Esta información se debe de introducir en el fichero **/etc/resolv.conf**. Para ello deberemos editar dicho fichero. Abriremos una Terminal y en ella escribiremos el siguiente comando.

gksudo gedit /etc/resolv.conf



Aparecerá la ventana del editor que se muestra a continuación con el contenido actual del fichero **/etc/resolv.conf** cargado en la misma. Reemplace dicho contenido por el que se muestra en la siguiente figura.



Si los DNS de su red son distintos a los de este ejemplo utilice los valores propios de su red, es decir:

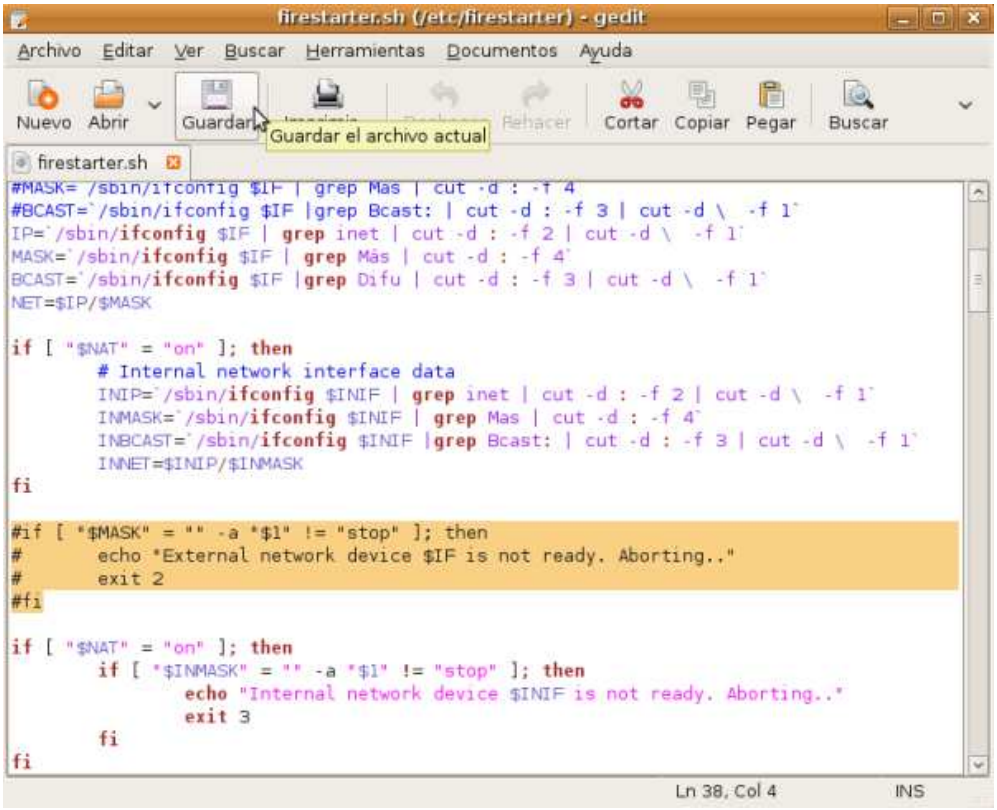
	Datos Configuración Ejemplo	Datos Configuración Particulares
nameserver	194.179.1.101	PRIMER DNS DE SU RED
nameserver	195.55.30.16	SEGUNDO DNS DE SU RED
…	…	…

Después de hacer los cambios en el fichero anterior, guárdelo.

A continuación edite el fichero **/etc/firestarter/firestarter.sh**. Desde una Terminal escribiremos el siguiente comando:

gksudo gedit /etc/firestarter/firestarter.sh

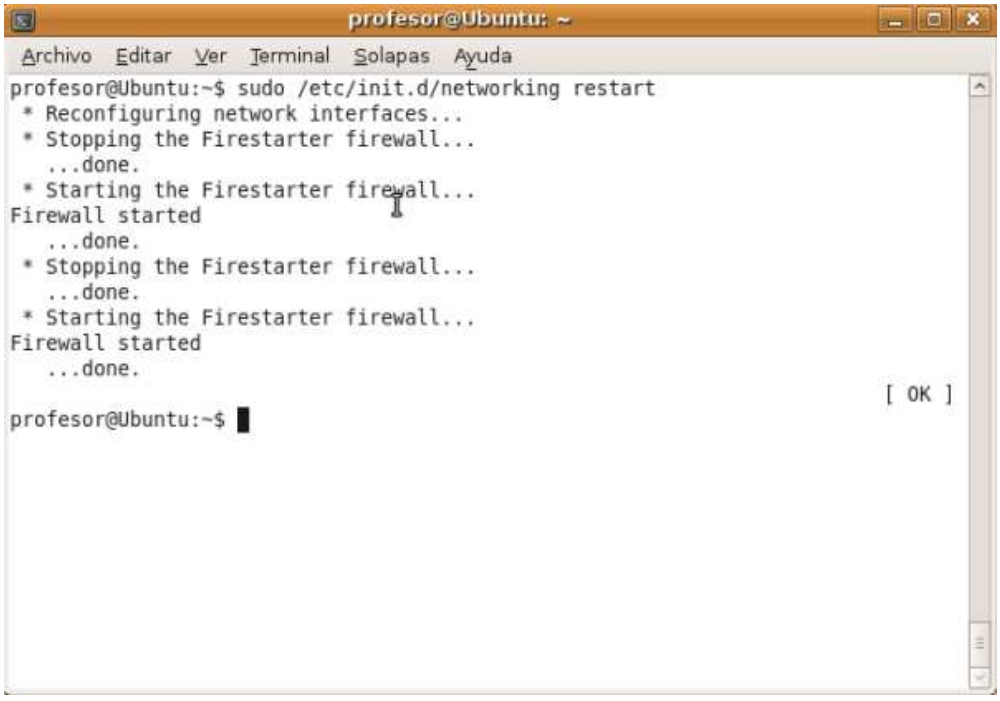
Aparecerá la ventana del editor que se muestra a continuación con el contenido actual del fichero **/etc/firestarter/firestarter.sh** cargado en la misma. Localice y comente (anteponiéndoles un carácter **#** al comienzo de la línea) las líneas que aparecen resaltadas en la siguiente figura.



Guarde el contenido del fichero después de hacer los cambios anteriores.

Desde una Terminal lance el siguiente comando para que se reinicien los interfaces de red con la nueva configuración.

sudo /etc/init.d/networking restart

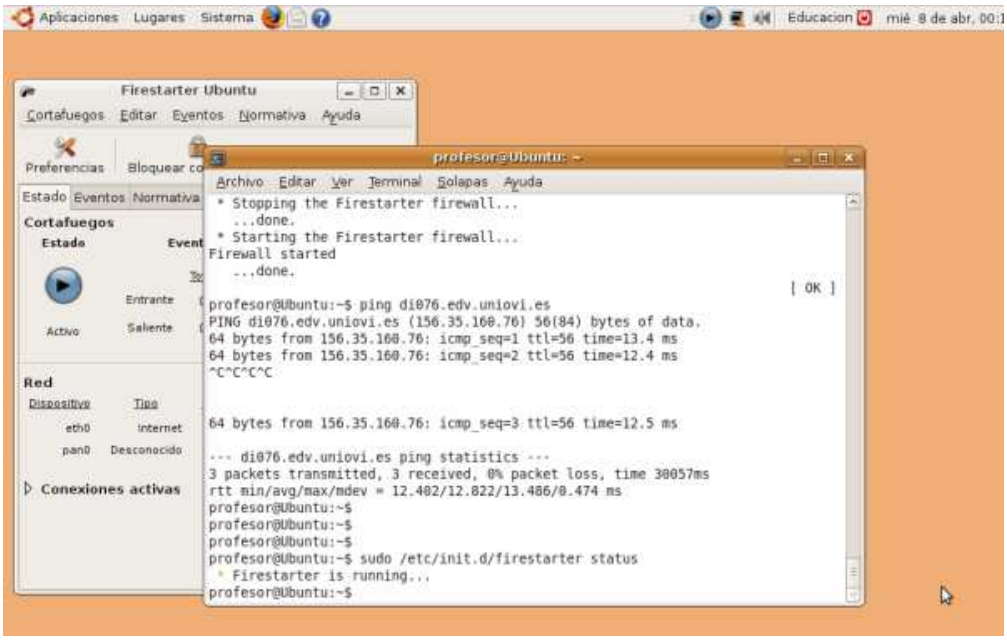


Después de ello, lance la consola de administración de Firestarter desde **Aplicaciones->Internet->Firestarter**. Podrá observar como el estado de funcionamiento indicado por la

consola de administración del cortafuegos es **Activo**. Desde una línea de comandos lance el comando:

sudo /etc/init.d/firestarter status

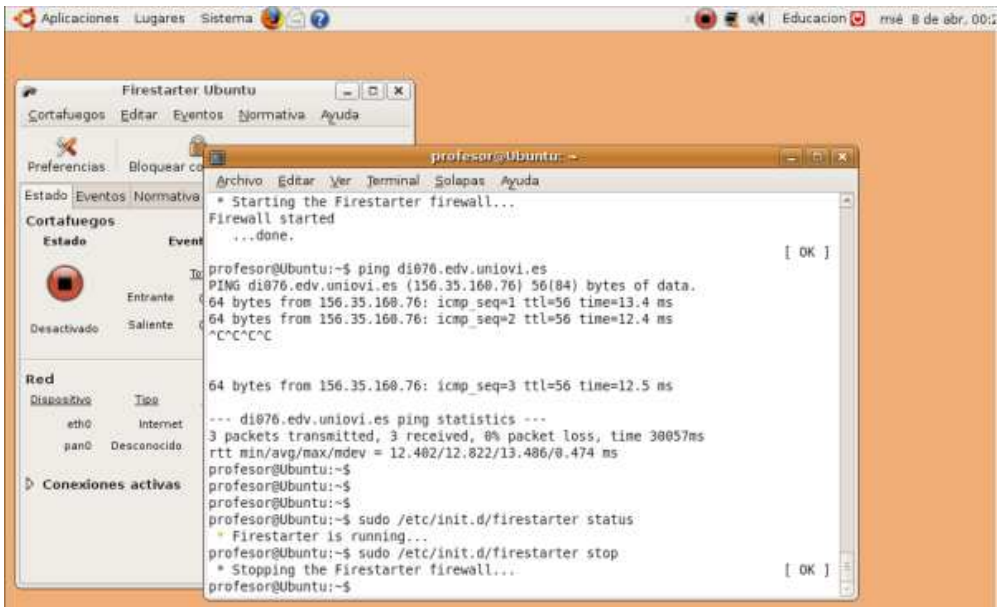
El sistema le mostrará un mensaje indicándole que el cortafuegos se está ejecutando (**Firestarter is running...**) tal y como se muestra en la siguiente figura.



Detenga a continuación el cortafuegos desde la línea de comandos mediante el siguiente comando:

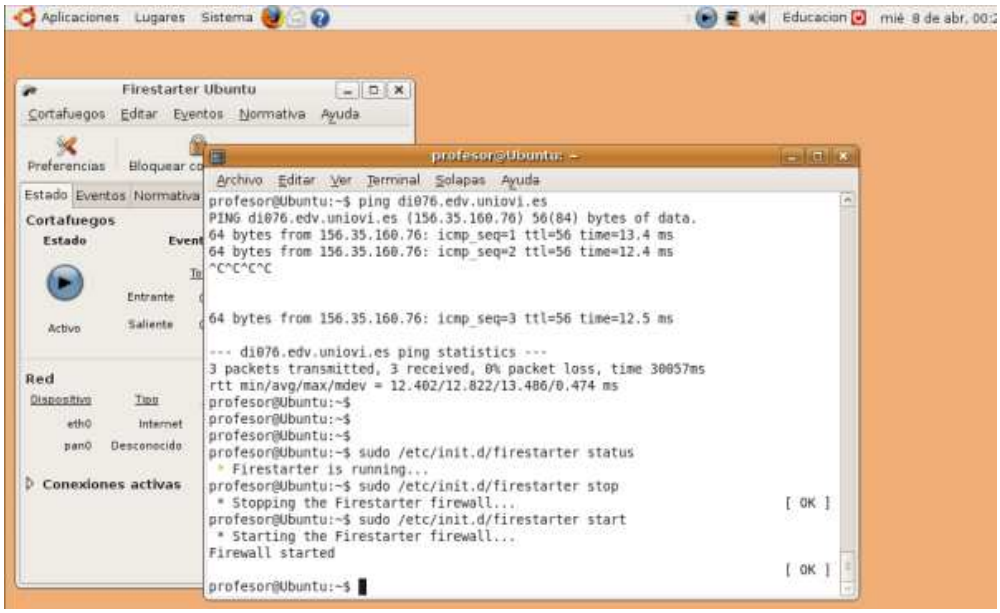
sudo /etc/init.d/firestarter stop

El sistema le mostrará un mensaje indicándole que ha detenido el cortafuegos e inmediatamente verá como el estado del cortafuegos pasa de **Activo** a **Desactivado** en la ventana de la consola de administración del cortafuegos.

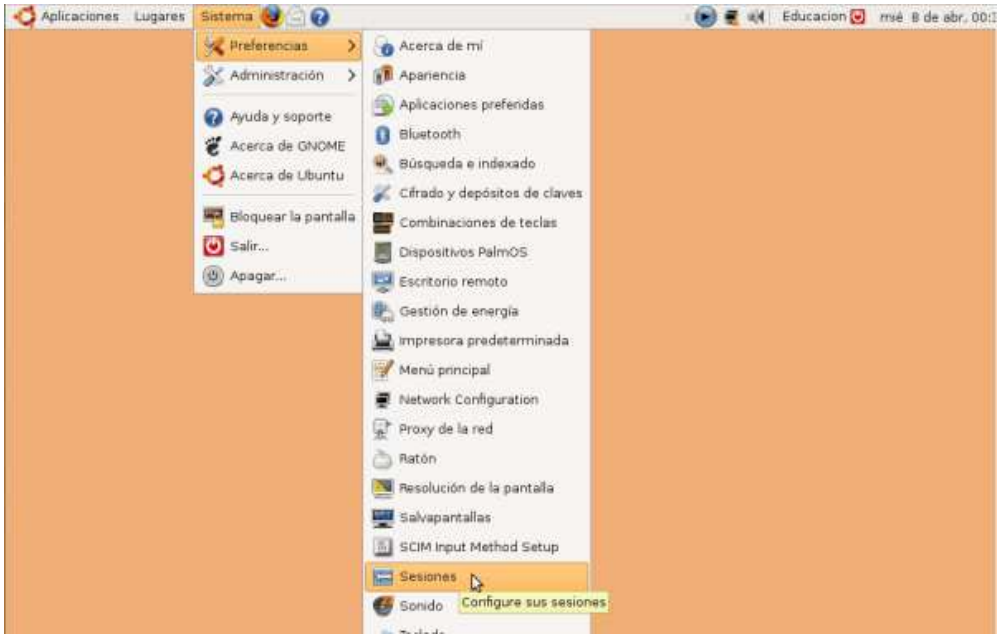


Esto indica que cualquier acción que hagamos sobre el cortafuegos desde la línea de comandos tendrá reflejo en el estado del cortafuegos reportado por la consola de administración del mismo y viceversa. Finalmente volveremos a lanzar de nuevo el cortafuegos para que continúe protegiendo a nuestro sistema con la orden:

sudo /etc/init.d/firestarter start



Por último, haremos desaparecer de barra de eventos la aplicación de **Conexiones de red** que se carga al iniciar sesión en el sistema, ya que no la necesitaremos, pues hemos desviado la configuración de red de usuario a los ficheros **/etc/network/interfaces** y **/etc/resolv.conf** que se procesan por el comando **ifup** al inicio del sistema. Para hacer que un programa no se inicie al iniciar sesión el usuario tendremos que ir al menú **Sistema->Preferencias->Sesiones**.

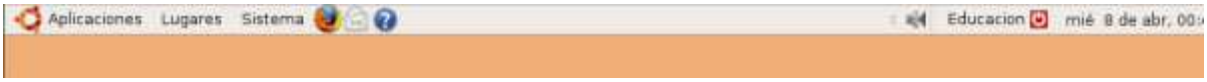


En la pestaña **Programas de inicio** del programa **Preferencias de la sesión** desmarcamos la casilla de **Configuraciones de red (Network Manager)**. Con esto no se cargará más dicha aplicación al iniciar sesión el usuario y tampoco veremos su icono en la barra de eventos.

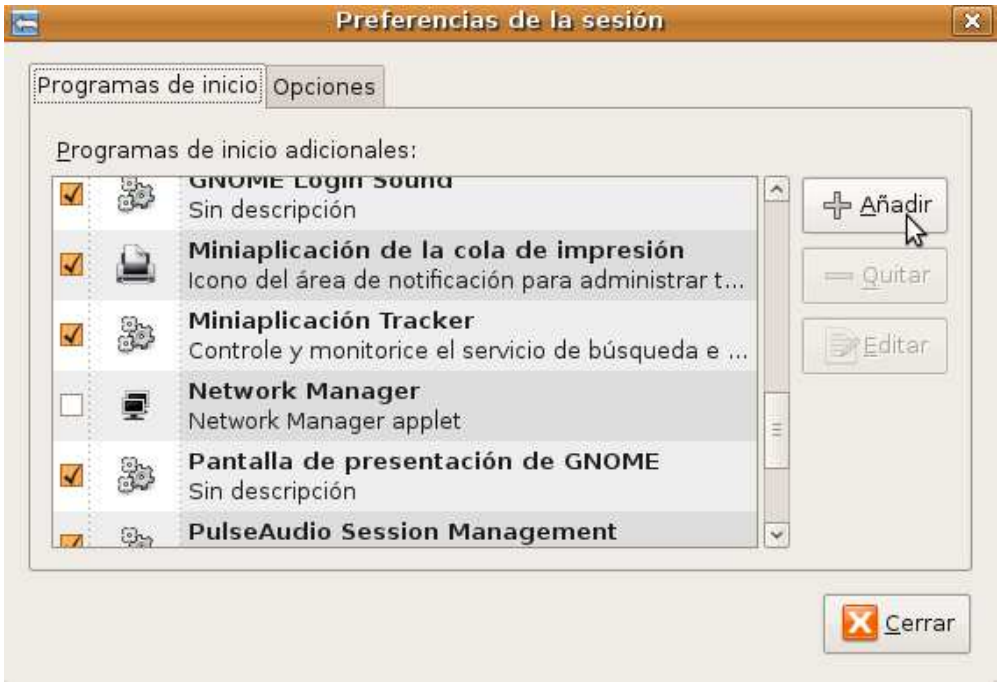
Luego pulsaremos el botón **Cerrar** para cerrar la aplicación.

Para comprobar que el programa de **Configuración de red** (**Network Manager**) no se arranca al iniciar sesión en el sistema, saldremos primero de sesión para posteriormente volver a iniciar sesión en el sistema como usuario **profesor**.

Vemos como al iniciar sesión ya no aparece más el icono del programa de **Configuración de red** (**Network Manager**) en la barra de notificación de eventos.



Iniciaremos de nuevo el programa de **Preferencias de la sesión** desde **Sistema->Preferencias->Sesiones**.



En la pestaña **Programas de inicio** del programa **Preferencias de la sesión** pulsaremos el botón **Añadir** para añadir una nueva aplicación al inicio de sesión para el usuario **profesor**. En la casilla orden escribiremos la siguiente orden:

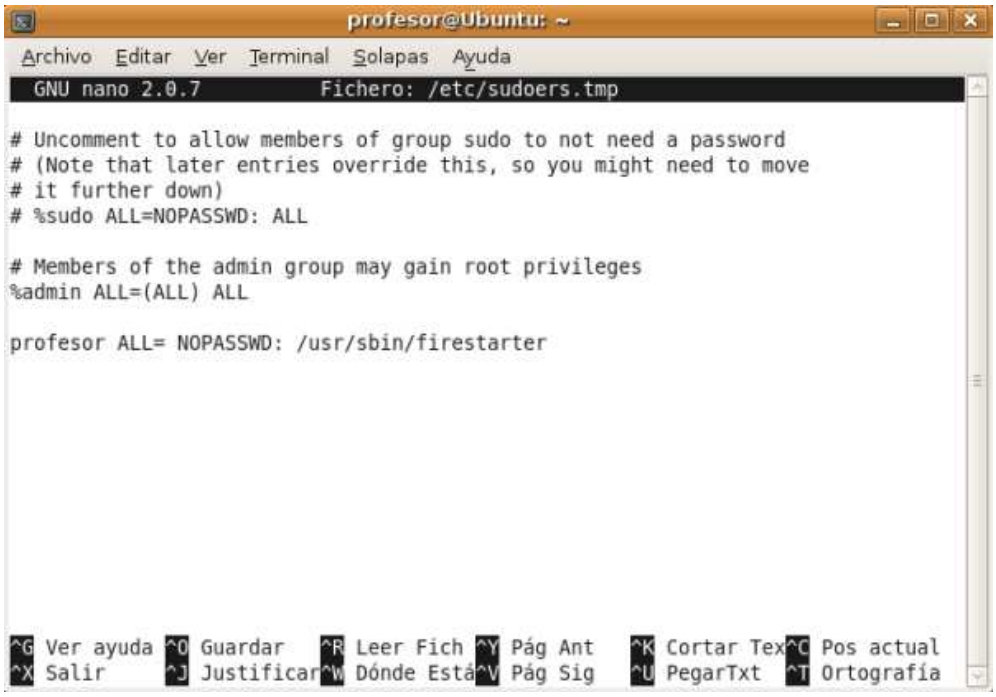
sudo /usr/sbin/firestarter --start-hidden

Tras pulsar sobre el botón "Añadir" en la ventana anterior, a continuación pulsaremos sobre el botón **Cerrar** para cerrar la ventana de Preferencias de la sesión. Aún no hemos terminado, pues modificaremos el fichero **/etc/sudoers** para que al intentar arrancar el programa de monitorización del cortafuegos al iniciar sesión, no nos pida la contraseña al tratarse de un programa que necesita de privilegios de administración. Para ello lanzaremos una Terminal y en ella escribiremos el siguiente comando:

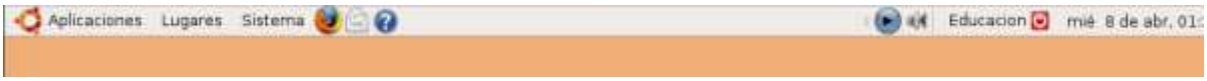
export EDITOR=gedit && sudo visudo

Aparecerá la ventana del editor que se muestra a continuación con el contenido actual del fichero **/etc/sudoers** cargado en la misma. Añada al final del fichero la siguiente línea:

profesor ALL= NOPASSWD: /usr/sbin/firestarter



Para guardar el archivo pulse CTRL+O, a continuación pulse ENTER y finalmente, para salir del editor, pulse CTRL+X. Se cerrará la ventana del editor. Salga de sesión y vuelva a iniciar sesión con el usuario profesor. Podrá ver ahora en la barra de eventos como aparece el icono de monitorización del cortafuegos mostrándonos que se encuentra activo, como podemos ver en la siguiente figura.



Aumento de privilegios

En ambientes donde varios usuarios usan uno o más sistemas GNU/Linux, es necesario otorgar distintos permisos o privilegios para que estos puedan hacer uso de comandos propios del usuario administrador **root**. Por motivos de seguridad no se debe 'entregar' la contraseña de **root** para que los usuarios puedan hacer uso de los programas propios de sus funciones pero que son propiedad de **root**. Por otro lado, hacer uso del comando **su** tampoco es práctico porque es lo mismo, necesitan la contraseña de **root**, así que la mejor alternativa es hacer uso de **sudo**.

Pero, ¿qué es y qué hace sudo?. **sudo** permite implementar un control de acceso altamente granulado sobre qué usuarios ejecutan qué comandos. Si un usuario normal desea ejecutar un comando de **root** (o de cualquier otro usuario), **sudo** verifica en su lista de permisos y si está permitido la ejecución de ese comando para ese usuario, entonces **sudo** se encarga de ejecutarlo. Es decir, **sudo** es un programa que basado en una lista de control (**/etc/sudoers**) permite (o no), al usuario que lo invocó, la ejecución de un determinado programa propiedad de otro usuario, generalmente del administrador del sistema o **root**.

sudo, para fines prácticos se puede dividir en tres partes:

- **sudo**, el comando con permisos de SUID, que los usuarios usan para ejecutar otros comandos de otros usuarios.
- **visudo**, el comando que permite al administrador modificar **/etc/sudoers**.
- **/etc/sudoers**, el archivo de permisos que le indica a **sudo** que usuarios ejecutan qué comandos.

sudo (**SU**peruser **DO**) lo ejecuta un usuario normal, que se supone tiene permisos para ejecutar cierto comando. Entonces, **sudo** requiere que los usuarios se autentifiquen a sí mismos a través de su contraseña para permitirles la ejecución del comando. Veamos un ejemplo:

```
$ sudo /sbin/ifconfig

Password:*******

eth0      Link encap:Ethernet  HWaddr 4C:00:10:60:5F:21

          inet addr:200.13.110.62  Bcast:200.13.110.255  Mask:255.255.255.0

          inet6 addr: fe80::4e00:10ff:fe60:5f21/64 Scope:Link

...
```

Como se podrá observar se usa el comando sudo seguido del comando a ejecutar (con toda su ruta si es que este no está en el PATH del usuario) al que se tiene permiso. **sudo** pregunta por la contraseña del usuario que ejecuta el comando y si éste tiene permisos, el comando se ejecutará.

Por defecto, después de hacer lo anterior tendrás 5 minutos para volver a usar el mismo comando u otros a los que tuviera derecho, sin necesidad de ingresar la contraseña de nuevo.

Si se quiere extender el tiempo por otros 5 minutos usa la opción **sudo -v** (validate).

Por el contario, si ya terminó lo que tenía que hacer, puede usar **sudo -k** (kill) para terminar con el tiempo de gracia de validación.

Ahora bien, ¿qué comandos son los que puedo utilizar?. La opción **-l** es la indicada para eso:

$ sudo -l

User marco may run the following commands on this host:

(root) /sbin/ifconfig

(root) /sbin/lspci

En el caso anterior se ejecutó un comando de **root**, pero no tiene que ser así, también es posible ejecutar comandos de otros usuarios del sistema indicando la opción **-u**:

$ sudo -u ana /comando/de/ana

Una de las opciones más interesantes es la que permite editar archivos de texto de **root** (claro, con el permiso otorgado en **/etc/sudoers** como se verá más adelante), y esto se logra con la opción **-e**, esta opción está ligada a otro comando de **sudo** llamado **sudoedit** que invoca al editor por defecto del usuario, que generalmente es **vi**.

$ sudo -e /etc/inittab

(Permitira modificar el archivo indicado como si se fuera root)

Cuando se configura **sudo** se tienen múltiples opciones que se pueden establecer, estás se consultan a través de la opción **-L**

$> sudo -L

Available options in a sudoers ``Defaults'' line:

syslog: Syslog facility if syslog is being used for logging

syslog_goodpri: Syslog priority to use when user authenticates successfully

syslog_badpri: Syslog priority to use when user authenticates unsuccessfully

long_otp_prompt: Put OTP prompt on its own line

ignore_dot: Ignore '.' in $PATH

mail_always: Always send mail when sudo is run

mail_badpass: Send mail if user authentication fails

mail_no_user: Send mail if the user is not in sudoers

mail_no_host: Send mail if the user is not in sudoers for this host

mail_no_perms: Send mail if the user is not allowed to run a command

tty_tickets: Use a separate timestamp for each user/tty combo

lecture: Lecture user the first time they run sudo

lecture_file: File containing the sudo lecture

authenticate: Require users to authenticate by default

root_sudo: Root may run sudo

...

varias opciones más

Esto es bastante útil, ya que nos muestra las opciones y una pequeña descripción; estás opciones se establecen en el archivo de configuración **/etc/sudoers**.

Una de las opciones más importantes de consulta es **-V**, que permite listar las opciones de sudo establecidas por defecto (defaults) para todos los usuarios, comandos, equipos, etc.

sudo -V

Sudo version 1.6.9p5

Sudoers path: /etc/sudoers

Authentication methods: 'pam'

Syslog facility if syslog is being used for logging: local2

Syslog priority to use when user authenticates successfully: notice

Syslog priority to use when user authenticates unsuccessfully: alert

Send mail if the user is not in sudoers

Lecture user the first time they run sudo

Require users to authenticate by default

Root may run sudo

Log the hostname in the (non-syslog) log file

Allow some information gathering to give useful error messages

Visudo will honor the EDITOR environment variable

Set the LOGNAME and USER environment variables

Reset the environment to a default set of variables

Length at which to wrap log file lines (0 for no wrap): 80

Authentication timestamp timeout: 5 minutes

Password prompt timeout: 5 minutes

Number of tries to enter a password: 3

Umask to use or 0777 to use user's: 022

Path to log file: /var/log/sudo.log

...

varias opciones más listadas

El archivo **/var/log/sudo.log** es el archivo 'log' o de bitácora por defecto de **sudo**. En este archivo se loguea absolutamente todo lo que se haga con **sudo**, qué usuarios ejecutaron qué, intentos de uso, etc.

Otro comando que podemos utilizar es "visudo", el cual permite la edición del archivo de configuración de sudo **/etc/sudoers**. Invoca al editor que se tenga por defecto que generalmente es vi. **visudo** cuando es usado, bloquea el archivo **/etc/sudoers** de tal manera que nadie más lo puede utilizar, esto por razones obvias de seguridad que evitarán que dos o más usuarios administradores modifiquen accidentalmente los cambios que el otro realizó.

Otra característica importante de **visudo** es que al cerrar el archivo, verifica que el archivo esté bien configurado, es decir, detectará si hay errores de sintaxis principalmente en sus múltiples opciones o reglas de acceso que se tengan. Por esta razón no debe editarse **/etc/sudoers** directamente (perfectamente posible ya que es un archivo de texto como cualquier otro) sino siempre usar visudo.

Si al cerrar visudo detecta un error nos mostrará la línea donde se encuentra, y la pregunta "What now?":

>>> sudoers file: syntax error, line 15 <<<

What now?

Se tienen tres opciones para esta pregunta:

- **e** - edita de nuevo el archivo, colocando el cursor en la línea del error (si el editor soporta esta función.)
- **x** - salir sin guardar los cambios.
- **Q** - salir y guarda los cambios.

Por defecto el archivo de configuración es **/etc/sudoers** pero se pueden editar otros archivos que no sean ese y que se aplique la sintaxis de sudo, y esto se logra con la opción **-f** (**visudo -f /otro/archivo**).

Si tan solo se desea comprobar que **/etc/sudoers** está bien configurado se usa la opción **-c**.

#> visudo -c

/etc/sudoers file parsed OK

La opción **-s** activa el modo **estricto** del uso de **visudo**, es decir no solo se comprobará lo sintáctico sino también el orden correcto de las reglas, por ejemplo si se define el alias para un grupo de comandos y éste se usa antes de su definición, con esta opción se detectará este tipo

de errores.

También podemos utilizar "sudoers" como archivo de configuración de **sudo**, generalmente ubicado bajo **/etc** y se modifica a través del uso de **visudo**. En este archivo se establece quién (usuarios) puede ejecutar qué (comandos) y de qué modo (opciones), generando efectivamente una lista de control de acceso que puede ser tan detallada como se desee.

En el momento de elaborar este material podía obtenerse más información sobre sudo en el siguiente enlace: http://www.linuxtotal.com.mx/index.php?cont=info_admon_014