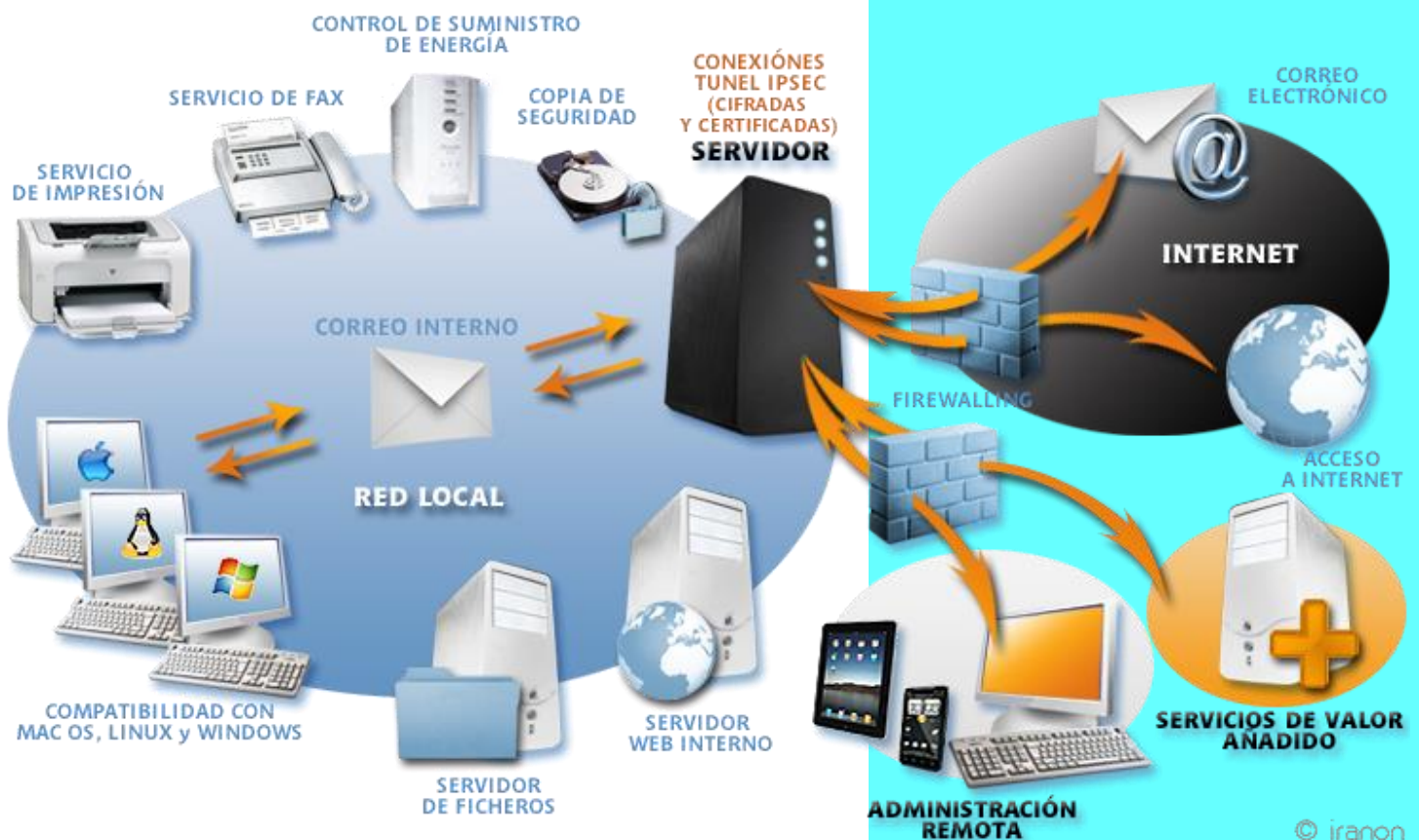


“Instalación de Sistema Operativo para Servidores”



© iranion

UNIDAD III

PROFESOR: Sergio Ávila M.

MATERIA:

ADMINISTRACION. Y
SEGURIDAD DE REDES

16-10-2015



**"INSTITUTO
TECNOLOGICO DE
GUSTAVO A. MADERO"**



PROFESOR: SERGIO AVILA M.

MATERIA: ADMINISTRACION Y SEGURIDAD DE REDES

INTEGRANTES: *Aguilar López Cristian David

***Galván León Víctor Manuel**

***Guevara Moreno Raymundo**

***Rodríguez Huerta Rubén**

***Suarez Hernández Cecilia**

CARRERA: TICS

UNIDAD III: SISTEMA OPERATIVO PARA SERVIDORES

VIERNES 16 DE OCTUBRE DEL 2015



Introducción:

En esta Práctica número 1 de Administración y seguridad de redes veremos cuales tipos de Sistemas Operativos para servidores que hay y conforme a las investigaciones recabadas nosotros como equipo elegimos el Sistema Operativo de Ubuntu Server 15.04.

Como se verá en esta práctica nosotros instalaremos el Sistema Operativo de Ubuntu Server 15.04 para nuestro servidor lo haremos de forma nativa, ya que tengamos instalado Ubuntu Server 15.04 haremos ciertas configuraciones para que nuestro servidor conceda permisos para que las terminales puedan tener conexión con él.

Nuestro Servidor será usado en una Farmacéutica ya que esta necesita un Servidor y cuatro terminales nosotros elegimos el Sistema Operativo de Ubuntu Server 15.04 ya que esta farmacia como es una empresa mediana no cuenta con el suficiente dinero para pagar licencias por lo tanto no le convendría que nosotros manejáramos otro donde sí se tengan que pagar licencias.

También nos dimos a la tarea de plantear las Políticas de la Empresa y las Políticas de Seguridad, para esto también requerimos del uso de un cronograma de actividades para que tengamos un registro de todos los procesos que llevemos a cabo y nuestra práctica sea un éxito.



Análisis de requerimientos de Mega Farmacia

- Ingresar Políticas de seguridad para el gestionamiento de la red
- Instalación de MySQL para el administración de la red
- Las VLAN basadas en 802.1Q permiten la segmentación de redes para mejorar el rendimiento y la seguridad.
- Private VLAN Edge (PVE) que simplifica el aislamiento de la red para conexiones de invitados o redes autónomas.
- Configuración automática de VLAN en varios switches mediante el protocolo genérico de registro de VLAN (GVRP) y el protocolo genérico de registro de atributos (GARP).
- Seguridad a nivel de puerto de usuario / red mediante autenticación 802.1X y filtrado basado en LINUX.
- Aumento del ancho de banda y redundancia de enlace con el protocolo de control de adición de enlace (LACP).
- Instalación de FarmaServicios para la administración de los medicamentos
- Conexión a internet para la actualización de precios con los proveedores
- Módulo SFP del paquete de protección estática de ventas promedio.

Políticas de la Empresa Mega Farmacia:

1. El coordinador en conjunto con el área de sistemas asigna a cada empleado un equipo de cómputo al cual debe ingresar con un usuario y contraseña.
2. El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe monitorear que se cumpla esta política. Además, todo el personal deberá informar a sistemas sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.
3. Todo el personal tendrán una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades. Estas cuentas de correo, sólo son para uso interno, no tienen la capacidad de enviar correos públicos.
4. El uso de internet queda reservado solo para las actividades de trabajo que así lo requieran. En general se restringe el acceso mediante el uso de contraseña en el administrador de contenidos de Internet Explorer.

Políticas de Seguridad de la Empresa Mega Farmacia

5. Diariamente se realizan backups automáticos a la base de datos según los mecanismos establecidos y se realizan a cada hora.
6. Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados.
7. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.
8. Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.
9. Coordinación o sistemas designarán periódicamente nuevas contraseñas tanto para el acceso a las sesiones Windows como para el acceso a los programas.
10. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.
11. Todos los equipos asignados a los conectores/gestores tendrán deshabilitados los accesos a puertos USB, CD o Diskettes. Esta medida tiene 3 objetivos:

- Evitar ataques de virus en los equipos y el servidor.
- Evitar extracciones no autorizadas.
- Evitar la carga de archivos ajenos a la labor de gestión.

12. Los equipos autorizados para el uso de dispositivos de almacenamiento externos están supervisados por coordinación y por el área de sistemas, para la entrada y salida de información.

13. A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

- Actualizar su base de firmas de virus (actualización de la lista de amenazas)
- Búsqueda de virus (análisis del equipo)
- Eliminación de virus si fue detectado.

14. En caso autorizado de memorias USB y discos, es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Además los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

Sobre el mantenimiento y buen uso de la infraestructura

15. Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.

16. Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.

17. Si se presentara una suspensión de servicio eléctrico y el servidor solo se sostuviera con el no-break, se tendrán que apagar primero todos los equipos de la agencia y posteriormente el servidor.

18. El servidor y la máquina principal del área administrativa deberán conectarse a un equipo no-break para evitar la pérdida de información en los equipos por variaciones o fallas de energías.

19. Una vez al año se realizara una revisión en la red para detectar desperfectos y dar así mantenimiento a la agencia.

20. Periódicamente, por espacio de 4 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas.

21. Toda actividad elaborada por el equipo de sistemas deberá de estar debidamente documentada para darle seguimiento y que sirva como evidencia en los procesos de auditoría interna.

Proceso de Nuestra Instalación de Servidor

SISTEMA DE ARCHIVOS EN LINUX UBUNTU

Linux gestiona varios tipos de sistemas de ficheros ext3 es el sistema de archivos nativo de Ubuntu ext3 es una versión mejorada de ext2, versión utilizada en distribuciones anteriores a la 8.04. Linux también utiliza una zona de swap en el disco para realizar la paginación de los programas.

Es usado cuando la cantidad de memoria física (RAM) no es suficiente. Si el sistema necesita más memoria y la memoria física está llena, las páginas inactivas de la memoria se mueven al espacio swap.

El espacio swap se encuentra en discos duros o particiones, que evidentemente tienen un tiempo de acceso más elevado que la memoria física.

MEJORAS INTRODUCIDAS en la versión 15.04

EN EXT3

Disponibilidad. En ext2, tras un corte eléctrico, era necesario realizar una comprobación del disco mediante el comando E2FCK. La característica journaling de ext3 realiza sólo una comprobación de consistencia en determinados errores de hardware.

Fácil transición. La migración de ext2 a ext3 es muy sencilla. La propiedad Journaling se puede añadir sin tener que volver a dar formato al sistema.

Integridad de los datos. Ext proporciona una integridad superior de datos que otros sistemas de archivos ante cierres inesperados.

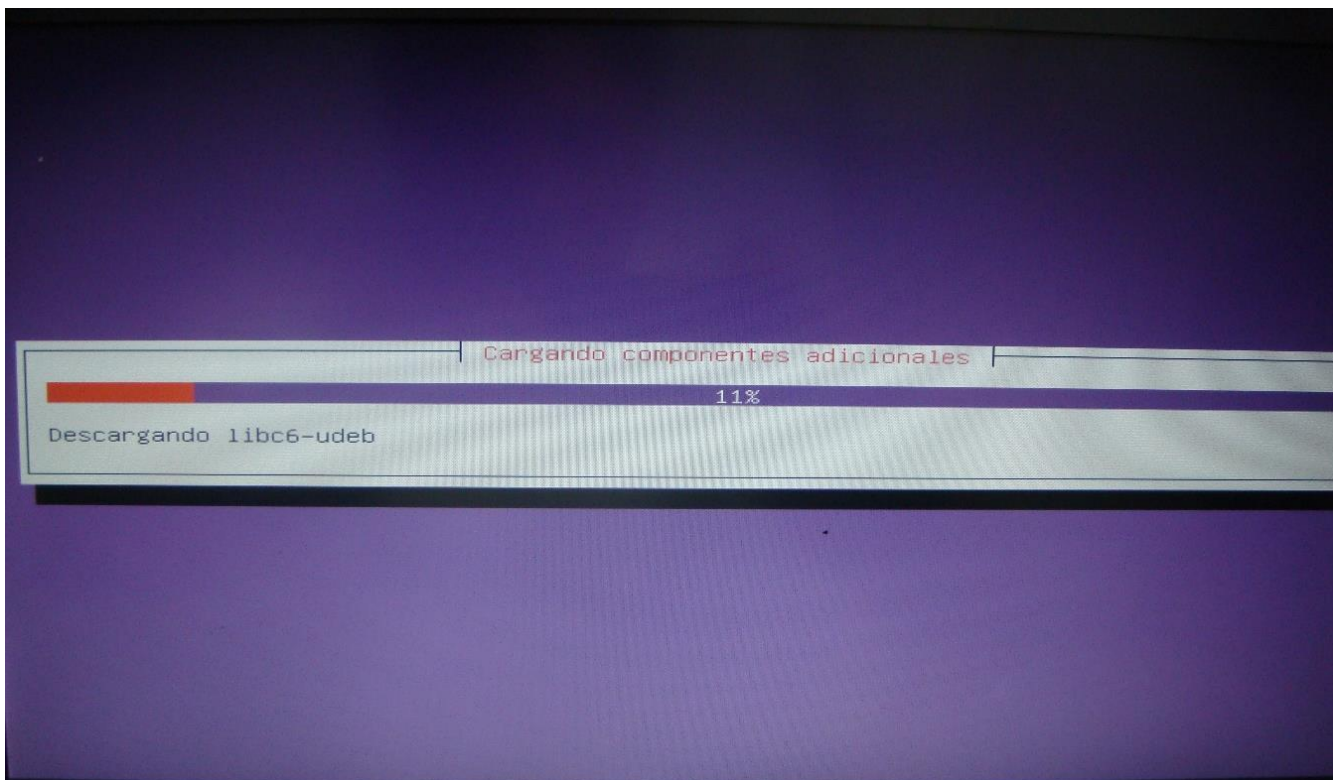
Velocidad. Ext3 permite escribir más datos de una vez porque los journals de ext3 optimizan el movimiento de los cabezales de los discos duros.

Pasos para la Instalación de Ubuntu Server

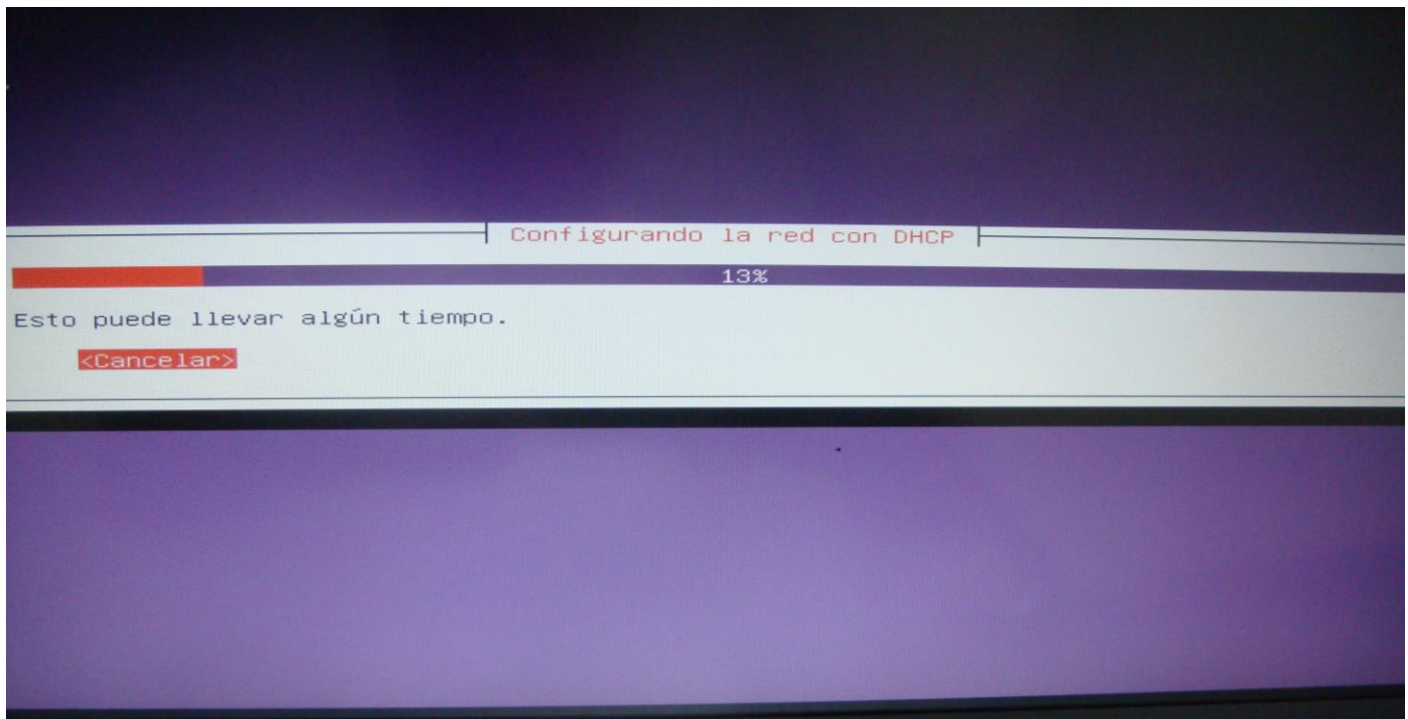
Inicio de instalación de Ubuntu server y sus configuraciones de conexión con el cliente



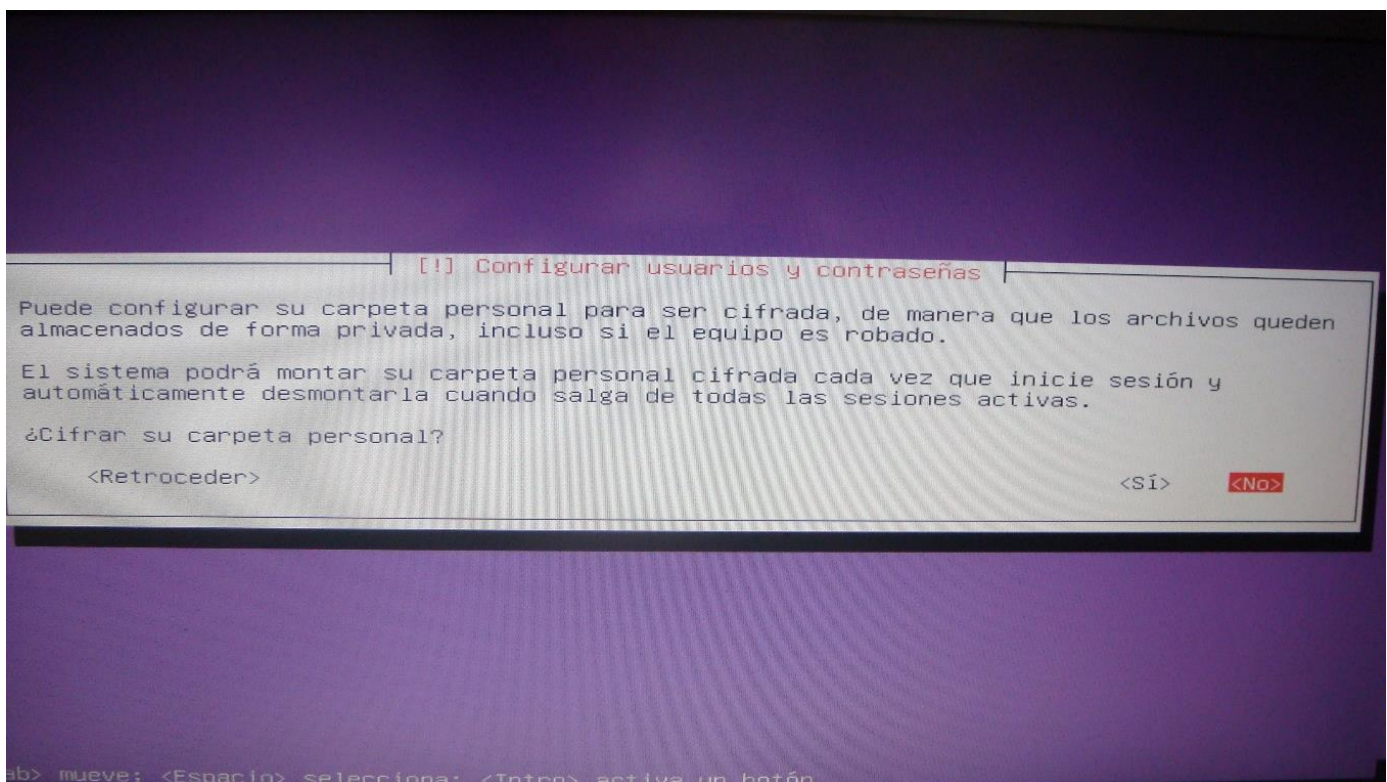
Pantalla principal de instalación que se muestra durante el arranque del disco de instalación esta nos muestra el lenguaje que tendrá nuestra interfaz de instalación.



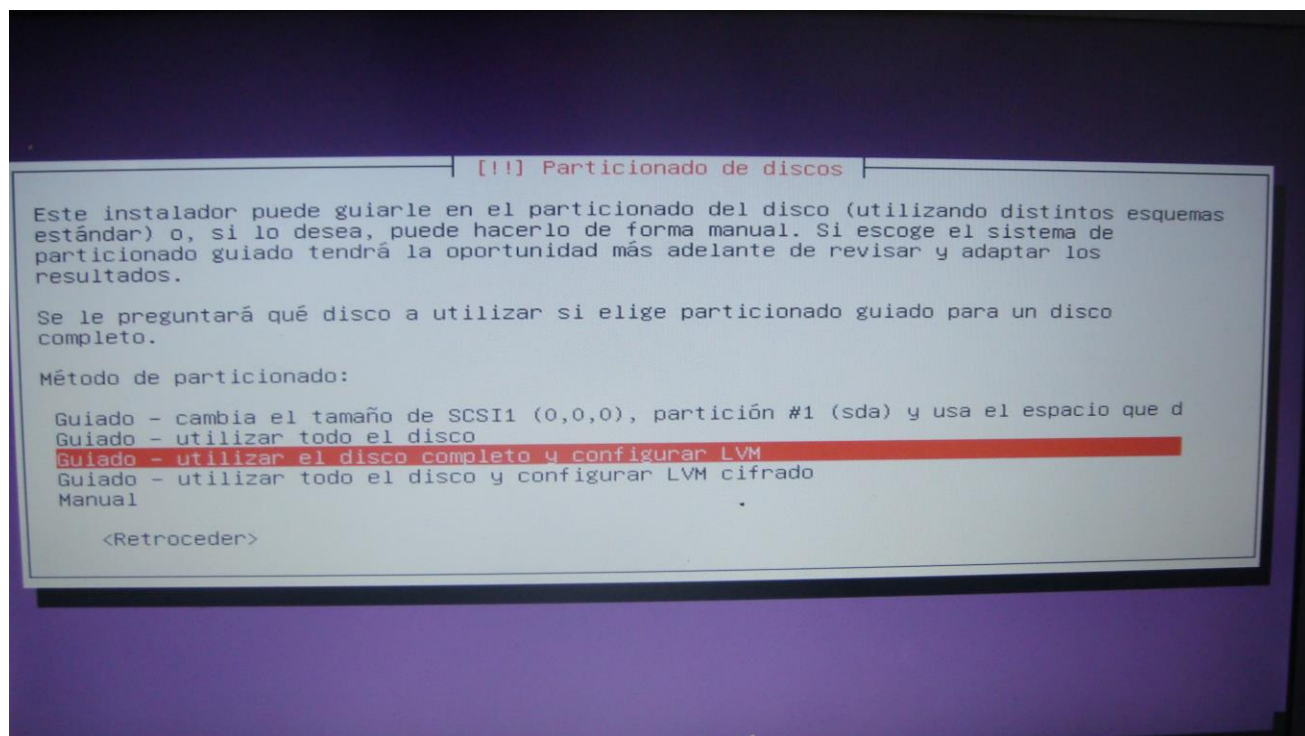
Pantalla que muestra la carga de componentes.



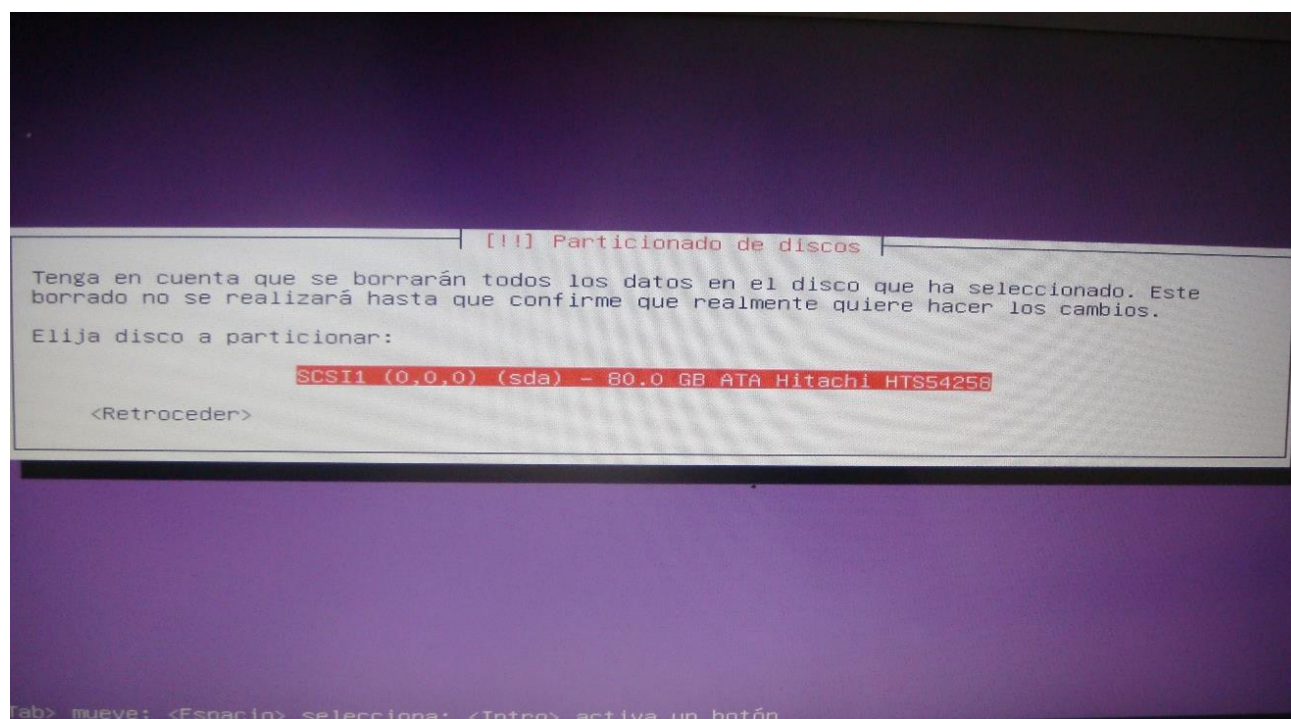
Muestra la línea de configuración de los componentes de red dhcp que se utilizara para conexión.



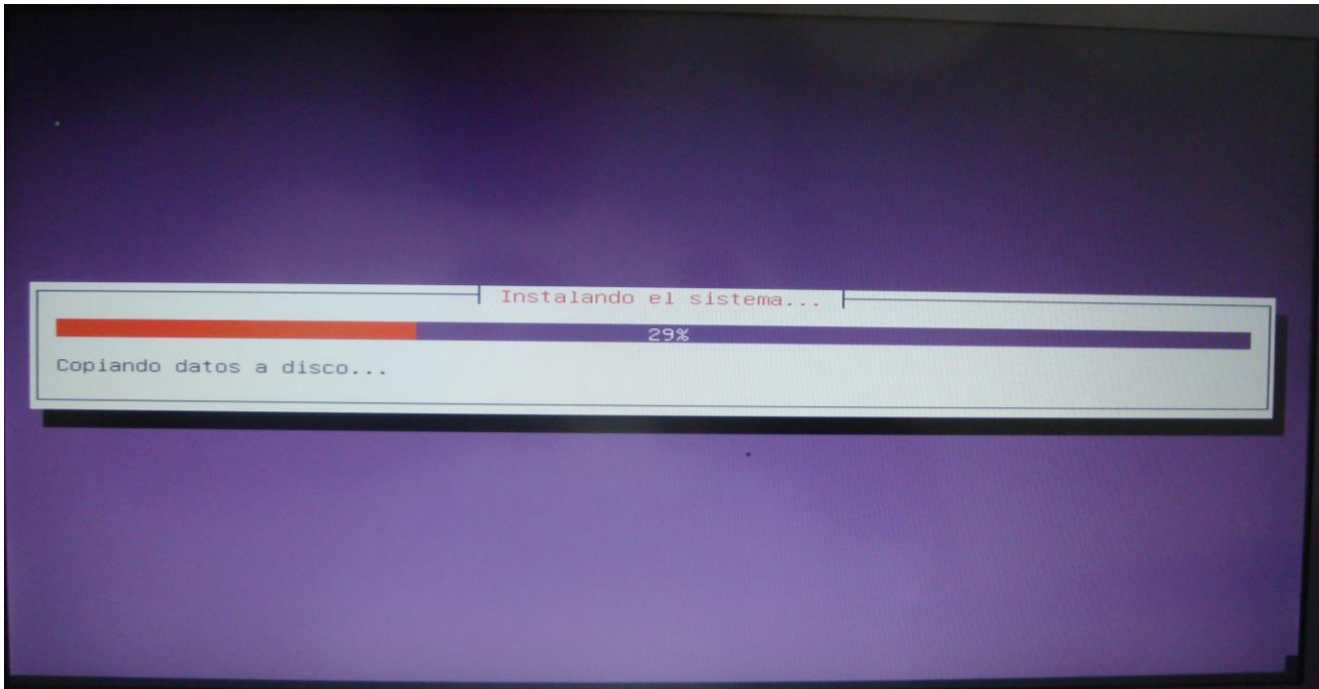
Nos muestra que se iniciara la configuración del nombre de usuario y contraseña.



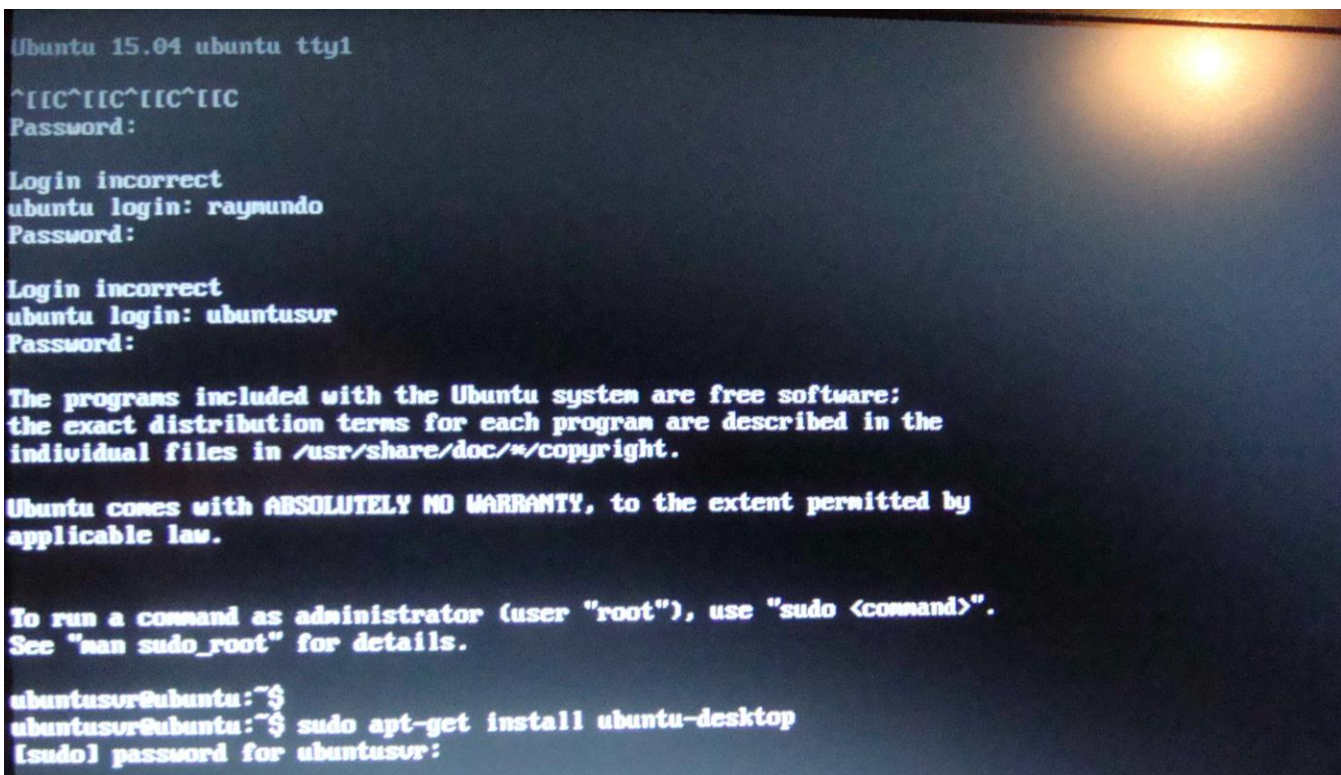
Nos informa la siguiente pantalla de que se iniciara la forma en que peticionaremos nuestro disco para la posterior instalación ya sea ocupando todo el disco duro o peticionándolo manualmente.



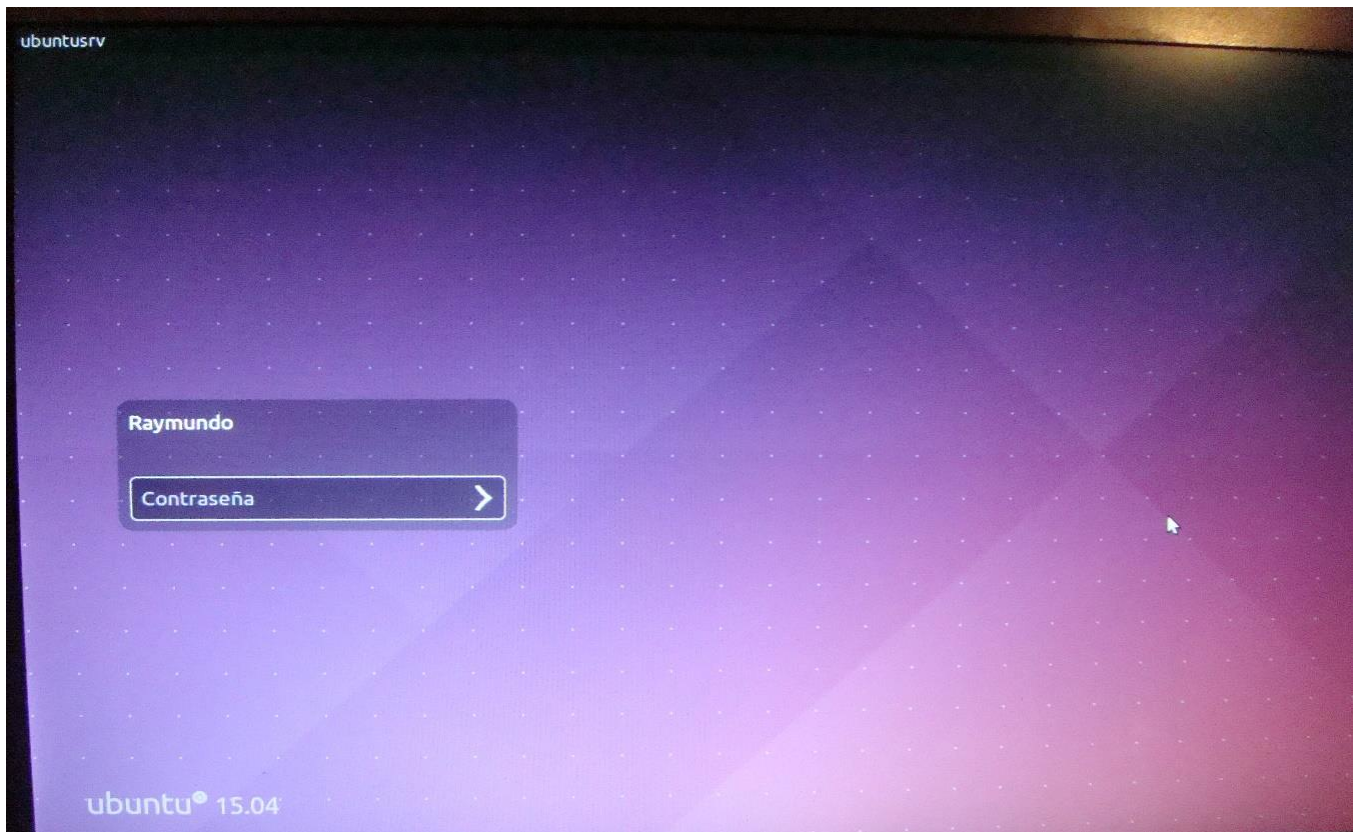
Nos muestra la forma en cómo se seleccione la partición de nuestro disco, el cual se ocupó por completo.



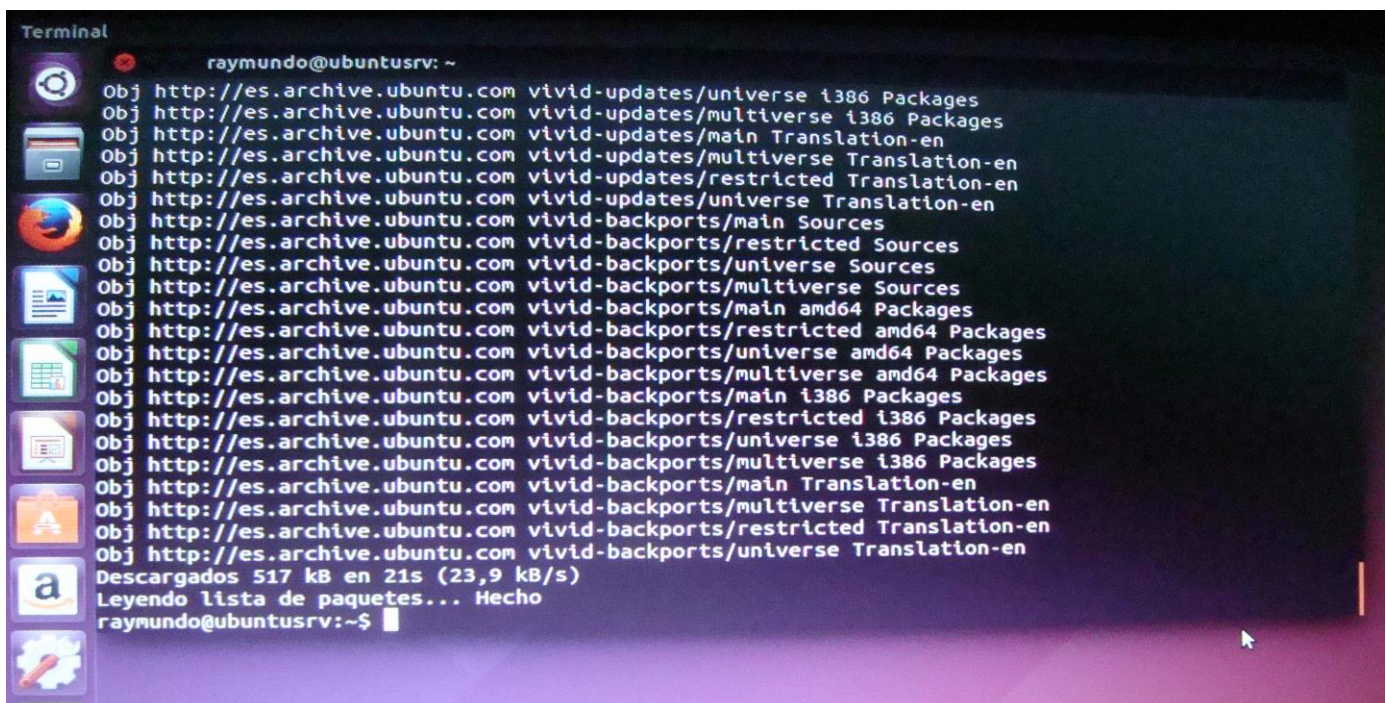
Pantalla que muestra la instalación del sistema lo cual en promedio de acuerdo con el hardware se tardara aprox. 20 minutos.



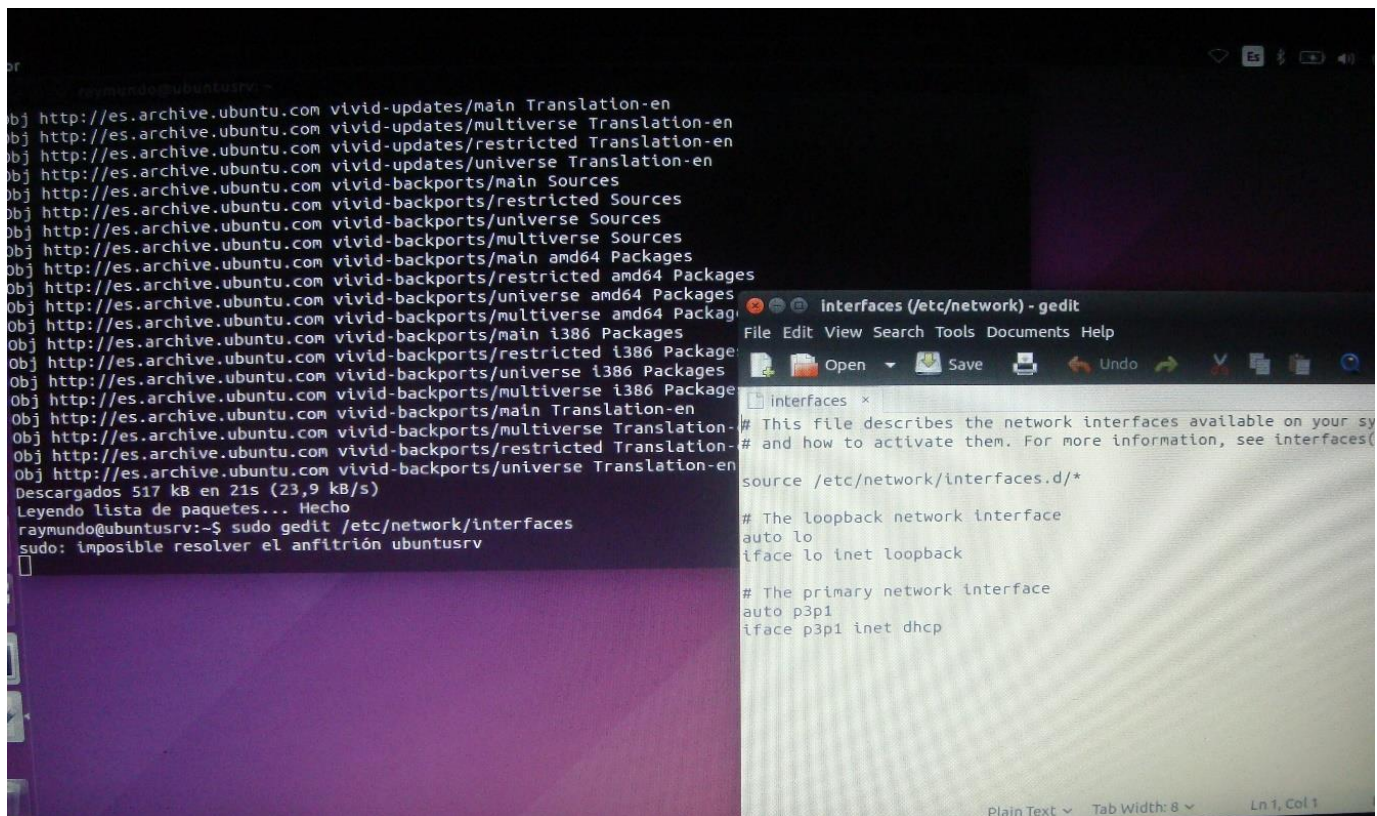
Pantalla principal después de la instalación la cual solo nos muestra una pantalla de login, por lo cual para hacerlo más cómodo nuestra configuración se le instalara mediante un comando la interfaz gráfica como lo muestra la pantalla.



Pantalla principal de nuestro servido después de instalarle interfaz gráfica. Listo para logearnos



Después de instalarle la interfaz gráfica a nuestro servidor Ubuntu, hemos de actualizar todos los repositorios para que cuando instalemos la herramienta dhcp no falten archivos y la configuración de red sea adecuada.



The screenshot shows a terminal window with the following output:

```
Obj http://es.archive.ubuntu.com vivid-updates/main Translation-en
Obj http://es.archive.ubuntu.com vivid-updates/multiverse Translation-en
Obj http://es.archive.ubuntu.com vivid-updates/restricted Translation-en
Obj http://es.archive.ubuntu.com vivid-updates/universe Translation-en
Obj http://es.archive.ubuntu.com vivid-backports/main Sources
Obj http://es.archive.ubuntu.com vivid-backports/restricted Sources
Obj http://es.archive.ubuntu.com vivid-backports/universe Sources
Obj http://es.archive.ubuntu.com vivid-backports/multiverse Sources
Obj http://es.archive.ubuntu.com vivid-backports/main amd64 Packages
Obj http://es.archive.ubuntu.com vivid-backports/restricted amd64 Packages
Obj http://es.archive.ubuntu.com vivid-backports/universe amd64 Packages
Obj http://es.archive.ubuntu.com vivid-backports/multiverse amd64 Packages
Obj http://es.archive.ubuntu.com vivid-backports/main i386 Packages
Obj http://es.archive.ubuntu.com vivid-backports/restricted i386 Packages
Obj http://es.archive.ubuntu.com vivid-backports/universe i386 Packages
Obj http://es.archive.ubuntu.com vivid-backports/multiverse i386 Packages
Obj http://es.archive.ubuntu.com vivid-backports/main Translation-en
Obj http://es.archive.ubuntu.com vivid-backports/restricted Translation-en
Obj http://es.archive.ubuntu.com vivid-backports/universe Translation-en
Descargados 517 kB en 21s (23,9 kB/s)
Leyendo lista de paquetes... Hecho
raymundo@ubuntu:~$ sudo gedit /etc/network/interfaces
sudo: imposible resolver el anfitrión ubuntu:~$
```

Overlaid on the terminal is a window titled "Interfaces (/etc/network) - gedit". It shows the content of the `/etc/network/interfaces` file:

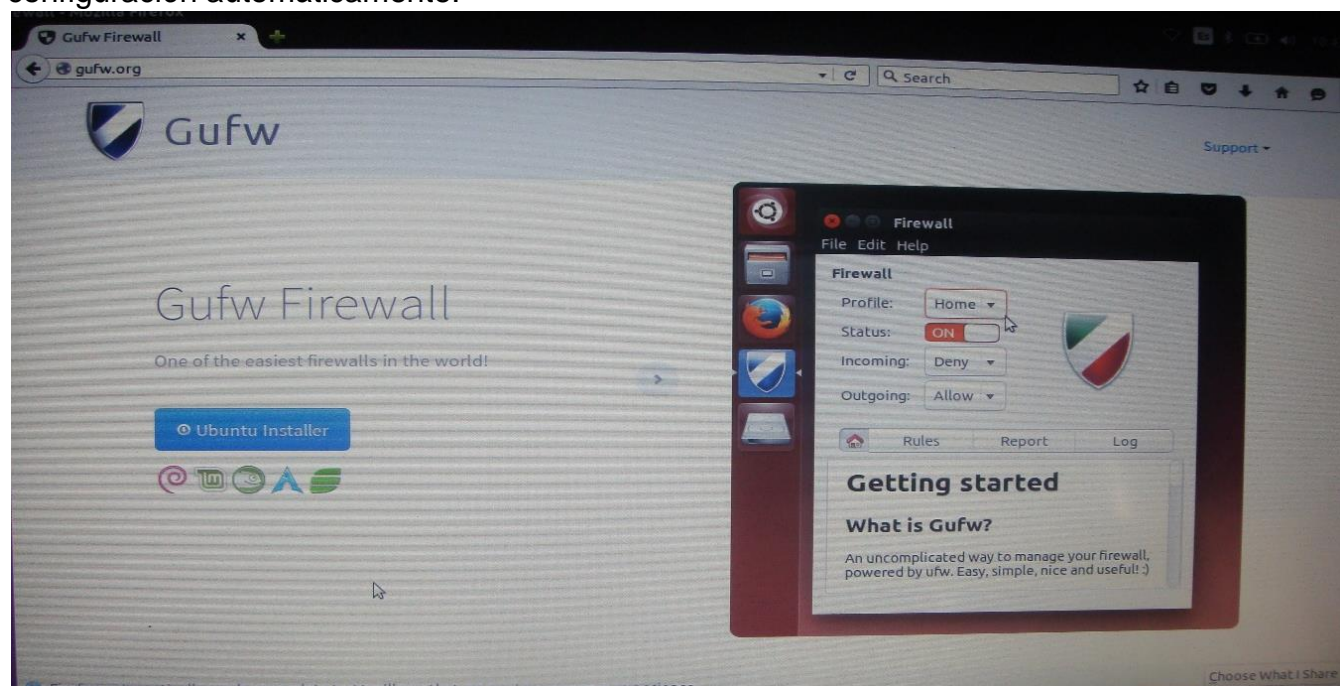
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

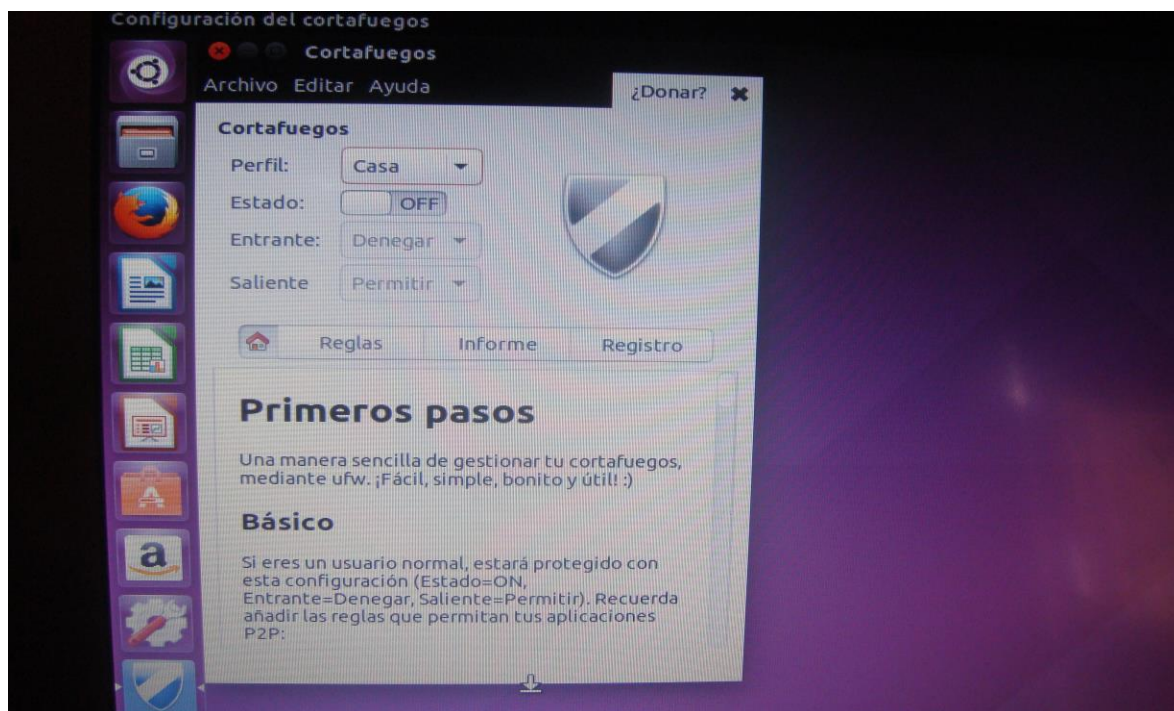
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto p3p1
iface p3p1 inet dhcp
```

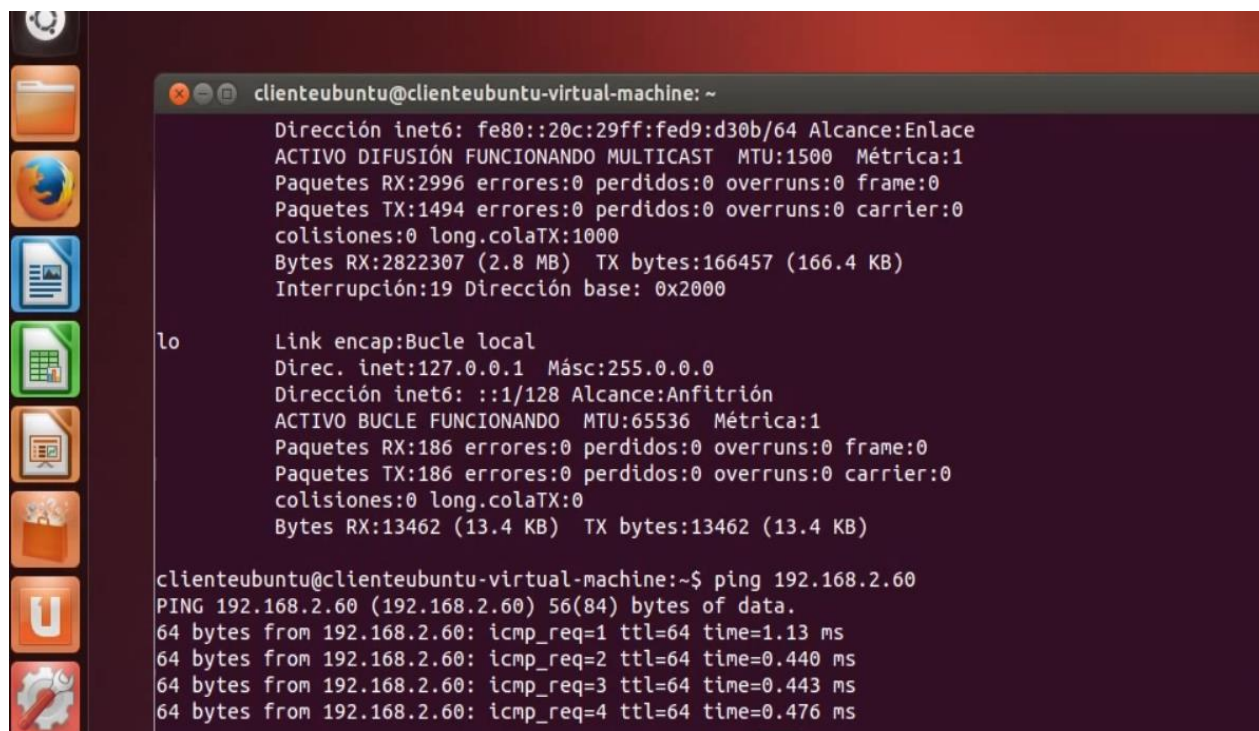
Después de actualizar nuestros repositorios y nuestro sistema operativo nos disponemos a actualizar el archivo de configuración de las interfaces para colocar nuestra configuración de la ip, y máscaras, y red que se manejaran de manera estática esto para no permitir que el servidor no cambie su configuración automáticamente.



La herramienta de configuración del cortafuego por defecto para Ubuntu es UFW. Desarrollado para facilitar ip estables configuración del cortafuego, UFW proporciona una manera fácil de usar para crear un firewall basado en host IPv4 o IPv6.



Pantalla de nuestro software SWF listo para configurar y bloquear entradas y establecer reglas de conexión.



Pantalla muestra la conexión de nuestro cliente con el servidor mediante un ping la cual nos demostrara que la comunicación con el servidor es correcta y viceversa.

Comandos utilizados en esta práctica:

(sudo apt-get install Ubuntu-desktop)

Comando utilizado para llevar Ubuntu server a modo grafico

(sudo apt-get update && upgrade)

Comando se utilizó para actualizar repositorios de Ubuntu

(sudo apt-get install isc-dhcp-server)

Comando para instalar herramienta dhcp que se utilizara para conexión.

(sudo gedit /etc/network/interfaces)

Comando que se utiliza para editar archivo de las interfaces editar y guardar.

(sudo /etc/init.d/network restart)

Comando para reiniciar la red y actualizar los cambios hechos en en el archivo que se editó de interfaces.

(sudo gedit /etc/dhcp/dhcp.conf.)

Comando para configurar el archivo del servidor

(sudo apt-get install dhcp3-client)

Comando para instalar herramienta del cliente dhcp y permita comunicarse con el servidor.

(sudo gedit /etc/dhcp/dhclient)

Comando para editar archivo de configuración del cliente.

(ping "dirección de red")

Comando utilizado para comprobar comunicación cliente servidor.

"CRONOGRAMA DE ACTIVIDADES"



Conclusión Raymundo:

Los S.O en red tienen unas características que los definen y que los representan. Por lo que los sistemas operativos en red se utilizan con el objetivo de optimizar la utilización de recursos de una pequeña o gran red y sobre todo para realizar una gestión centralizada del software y de todos los recursos de hardware que se pueden gestionar en una red. Por lo que un S.O en red se instala en un equipo que tendrá un rango superior al resto de los equipos de una red. En nuestro caso instalamos y configuramos un S.O de código abierto que nos permite la libre instalación y evitar la compra de licencias.

Conclusión de Rubén:

El administrador es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad de la compañía, dependerá de que los empleados aprendan las reglas a través de sesiones de capacitación y de concientización. Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente
- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

Conclusión Cecilia:

Como vimos en esta práctica se recabaron conocimientos en cuanto a la instalación de un servidor en nuestro caso fue Ubuntu en nuestra empresa Mega farmacias ya que para poder hacer la instalación se necesitó información sobre un análisis de requerimientos, además de políticas de la empresa y políticas de seguridad.

Se hizo el proceso de la instalación y se hizo la configuración debida en el servidor además nuestra políticas de seguridad nos sirven para garantizar lo que es la integridad, disponibilidad y confidencialidad de la información que maneja nuestra empresa.

Como vemos el administrador asegura que los recursos y los derechos de acceso a estos recursos coincidan con la política de seguridad de nuestra empresa.

Conclusión Cristian:

En este trabajo observamos lo que es un servidor en Ubuntu el cual nos pareció perfecto para nuestra empresa porque es un software libre además de ser seguro para los usuarios, se vio que no solo es instalarlos se necesita de información para que no solo sea una instalación vacía. El servidor debe de facilitar las acciones para con nuestra empresa.

Conclusión Víctor:

Como se vio generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores.

Bibliografía:

<http://www.ubuntu.com/download/server>

https://www.ifex.org/campaigns/risk_assessment/es/

http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

<http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap5.html>