DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE SERVICIOS TELEMÁTICOS Y PROTECCIÓN DE RED, BAJO PLATAFORMA LINUX, DENTRO DE LA EMPRESA LICORES CAPRI

CHRISTIAN DAVID NARANJO LÓPEZ
DAVID ESTEBAN GÓMEZ CORAL

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2017

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE SERVICIOS TELEMÁTICOS Y PROTECCIÓN DE RED, BAJO PLATAFORMA LINUX, DENTRO DE LA EMPRESA LICORES CAPRI

CHRISTIAN DAVID NARANJO LÓPEZ
DAVID ESTEBAN GÓMEZ CORAL

Trabajo de grado presentado como requisito parcial para optar al titulo de Ingeniero de Sistemas

ASESOR:
Ing. Esp. EDGAR DULCE VILLARREAL

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
2017

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Firma del jurado

_____
Firma del jurado

_____
Firma del asesor del proyecto

San Juan de Pasto, 5 de junio del 2017

AGRADECIMIENTOS

Agradecemos de manera especial al señor Juan Portilla, Gerente de la empresa Licores Capri, por brindarnos de manera cordial y acogedora, el acceso al espacio de trabajo de la organización, para la consecución de este proyecto.

Agradecemos al ingeniero, Edgar Dulce, por el apoyo, la asesoría y los ánimos dados desde el primer momento en que surgió la idea de trabajo de grado.

Los más sinceros agradecimientos a todo el personal que labora en la empresa Licores CAPRI, los cuales siempre mostraron la mejor disposición a la hora de brindarnos toda la ayuda que requerimos.

A nuestros padres, nuestras más profundas gratitudes por el apoyo incondicional para la culminación de nuestra carrera como ingenieros de sistemas.

A Dios unidad indivisible, por permitirme culminar esta etapa de mi vida, en la cual he aprendido muchas lecciones.

A mis padres: Elsa Ligia, Hugo René y a mi hermano René Gabriel, por su incondicional apoyo durante el transcurso de la carrera, los cuales me ayudaron y animaron a pasar todas las adversidades y obstáculos presentados.

A Abril Julieta y Carolina, la manifestación pura del amor.

A mis abuelos, Hilda y Benjamín, personas que han sido un pilar fundamental para mi vida, brindándome siempre su amor y las mejores enseñanzas que he recibido.

A familiares, amigos, compañeros de universidad, profesores, conocidos y allegados, que me ayudaron de múltiples formas en el transcurso de mi etapa universitaria.

David Gómez Coral

A Dios, por brindarme el regalo de la vida y guiarme en cada uno de los pasos que he dado en mi vida.

A mis padres, Ruby y Edwin, por todos sus esfuerzos y sacrificios para apoyarme en cada una de las decisiones que he tomado, su entrega y dedicación para hacer de mi un gran ser humano y por todo el amor que me brindan a diario, lo cual me llena de fuerza para afrontar los retos que me presenta la vida.

A mi hermana, María Alejandra, por ser el motor de mi vida y la más grande motivación de superarme cada día, para ser su ejemplo a seguir y llegar juntos al éxito que tanto hemos anhelado.

A mi familia, quienes han sido un gran apoyo a lo largo de la vida, ayudándome, motivándome e impulsándome a cumplir todos esos sueños y metas que me he trazado.

A todas y cada una de las personas que, de alguna manera, aportaron ese granito de arena para la consecución de este logro tan importante en mi vida.

Christian David Naranjo

“Las ideas y conclusiones aportadas en este trabajo de grado son responsabilidad exclusiva de sus autores”.

Artículo 1º del Acuerdo No. 324 de Octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo No. 005 de 2010 emanado del Honorable Consejo Académico”.

TABLA DE CONTENIDO

LISTA DE TABLAS

pág.

LISTAS DE FIGURAS

pág.

GLOSARIO

ANCHO DE BANDA: es la capacidad de transporte de datos, medido normalmente en megabytes por segundo (MB/s) o en gigabytes por segundo (GB/s). A mayor ancho de banda mayor velocidad de transmisión.

ANILLO: conexión de dos o más estaciones en una topología lógica en círculo. La información se transfiere de manera secuencial en las estaciones activas.

BIT: digito binario utilizado en el sistema de numeración binario. Puede ser 0 o 1.

BRIDGE: (puente). Dispositivo que permite conectar dos o más segmentos LAN para que funcionen como una sola red lógica, manteniendo separado el tráfico de cada segmento y comunicándolos cuando sea necesario, opera en un modo donde acepta todos los paquetes de la LAN (modo promiscuo).

BYTE: serie de dígitos binarios consecutivos que se manejan como una unidad.

CANAL: medio de transmisión por el que viajan las señales portadoras de información.

CABLE: medio físico de transmisión.

CABLE COAXIAL: cable que consta de un conductor cilíndrico exterior hueco, el cual rodea a un conductor de alambre solido en su interior.

CLIENTE: máquina que necesita de un recurso externo.

CÓDIGO: combinación de letras o de números que identifican un producto o a una persona, permiten realizar determinadas operaciones o manejar algunos aparatos. “los computadores funcionan con el código ascii; las tarjetas bancarias tienen un código personal secreto.”

CONCENTRADOR: termino que se utiliza para describir un dispositivo que sirve como el centro de una red con topología estrella.

DEMONIO: tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario, interactivo e infinito.

DHCP: acrónimo de *Dynamic Host Configuration Protocol*, es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

DNS: acronimo de *Domain Name System*, base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como internet.

DIRECCIÓN IP: acrónimo de Internet Protocol, dirección de 32 bits asignada a los anfitriones que utilizan TCP/IP.

ENLACE: término conformado por el canal y por el medio de transmisión para garantizar el tráfico de datos. Antes de establecer un enlace de datos es necesario determinar condiciones físicas, eléctricas y técnicas de tal manera que permitan adoptar el mejor sistema de enlace desde un usuario hasta una red de servicios.

ETHERNET: especificación LAN de banda base inventada por la corporación Xerox.

FTP: protocolo y utilidad estándar para la transferencia de ficheros en internet y en el sistema operativo LINUX.

GATEWAY: dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. Convierte códigos de datos y protocolos de transmisión que permiten interoperabilidad.

HIPERTEXTO: documento gráfico en que se permite la navegación.

HTML: siglas de Hypertext Markup Language. Permite la creación de hipertextos para internet.

INTERNET: interconexión de red informática, de carácter mundial y abierta al público, que conecta redes informáticas de organismos oficiales educativos y empresariales.

IPTABLES: nombre de la herramienta del espacio de usuario por medio de la cual el administrador crea reglas para filtrado de paquetes y para hacer NAT.

MODEM: dispositivo que transforma un flujo de bits digitales en una señal analógica moduladora y viceversa.

MEGAHERTZ: unidad de frecuencia igual a un millón de ciclos o periodos por segundo.

GIGAHERTZ: unidad de frecuencia igual a mil millones de ciclos o periodos por segundo.

NAVEGADOR: programa en un computador de un usuario que permite navegar por internet; es decir que permite visualizar las páginas web en un formato legible.

PAQUETE: bloque de información que se transmite como una unidad en la red de datos.

PHP: lenguaje de programación usado para la creación de contenido de sitios web, es un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios web.

PASSWORD: (contraseña). Palabra clave utilizada para evitar que cualquier extraño haga uso de nuestra cuenta de internet o tenga acceso a nuestro correo electrónico.

PROTOCOLO: conjunto de reglas y normas para el establecimiento de una conexión entre dos o más computadores.

PROXY: servidor encargado de centralizar el flujo entre internet y una red, para evitar que cada terminal conectada a esa red necesite tener su propia conexión.

PUERTO: (socket), forma genérica de denominar a una interfaz por la cual diferentes tipos de datos pueden ser enviados y recibidos. Dicha interfaz puede ser física, o a nivel de software.

PUNTO A PUNTO: método de comunicación en el cual se transmite desde una estación a otra.

RED: sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota para facilitar el intercambio de información entre usuarios con intereses comunes mediante la compartición de recursos.

RED DE ÁREA LOCAL (LAN): Red de comunicaciones que proporciona interconexión entre varios dispositivos de comunicación de datos en un área pequeña.

ROUTER: dispositivo de red que conecta dos redes de computadores. Usa protocolos de internet y asume que todos los dispositivos conectados a la red usan la misma arquitectura de red.

RUTA: es la trayectoria que el tráfico de red toma de su fuente a su destino.

SERVIDOR: programas de computador en ejecución que atienden peticiones de otros programas, los clientes. Realiza otras tareas para beneficio de los clientes, ofreciendo la posibilidad de compartir datos, información y recursos de hardware y software, su conexión es a través de una red y también se accede a través del computador donde funciona. Opera como oyente de un socket.

SERVIDOR DE APLICACIONES: servidor en una red de computadores que ejecuta ciertas aplicaciones de software. Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a los computadores clientes.

SERVIDOR WEB: programa que implementa el protocolo HTTP.

SERVICIO: aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes.

SISTEMA: conjunto de elementos que se interrelacionan eficazmente para lograr un objetivo común predeterminado. Un sistema está formado por: elementos de entrada, proceso que los modifica, salidas que genera el proceso y la retroalimentación que se obtiene.

SITIO WEB: documento publicado en internet compuesto por texto, gráficos, sonidos, video digital y vínculos.

SOFTWARE: programas de computadores que realizan instrucciones responsables para que el hardware realice una tarea. Se pueden dividir en varias categorías según el tipo de trabajo que realiza.

SOFTWARE LIBRE: conjunto de software que por elección manifiesta de su autor puede ser copiado, estudiado, modificado, utilizado libremente con cualquier fin y redistribuido con o sin cambios o mejoras.

SSH: es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a maquinas remotas a través de una red, permite maneja por completo el ordenador mediante un intérprete de comandos, y también puede redirigir el trafico

SWITCH: dispositivo que permite la interconexión de terminales, segmentan paquetes de datos transmitidos por las terminales debido a que afectan una manipulación inteligente de ellos.

TCP/IP: acrónimo de transmisión Control Protocol / Internet Protocol, usado para el control de la transmisión en redes LAN e Internet. Permite que diferentes tipos de computadores se comuniquen a través de redes heterogéneas.

UDP: acrónimo de User Datagram Protocol, Protocolo no orientado a conexión que hace parte del conjunto de protocolos TCP/IP, el cual provee muy pocos servicios de recuperación de errores ofreciendo a cambio una manera directa de enviar y recibir datagramas. Es útil cuando se asegura que el medio de transmisión es confiable para obtener velocidades altas que permitan aprovechar el ancho de banda de un canal.

WAN: acrónimo de Wide Área Network, Redes de cobertura amplia cuyos nodos se encuentran típicamente a distancias de 100 kilómetros de promedio.

RESUMEN

El presente documento describe las actividades desarrolladas en la empresa licores CAPRI, orientadas a administrar la red tecnológica de la organización, gracias a la adición de un dispositivo tipo servidor, en el cual se configuran distintos servicios de red para la conexión, comunicación y monitoreo permanente de los equipos clientes conectados de manera física y remota a la red local de la empresa.

Las funciones principales del servidor son, proveer de una base de datos que contengan los nombres de dominio que se utilizan en internet para la identificación del servidor y la red, el direccionamiento dinámico de un nuevo rango de direcciones IP para la creación de una subred en las estaciones de trabajo de la empresa, brindar acceso remoto seguro al servidor de la empresa para la gestión de los servicios, permitir el envío y recepción de archivos remotos al servidor, compartir carpetas para el envío de archivos por parte de los equipos dentro de la red local al servidor, monitorear y controlar el tráfico de datos entrante y saliente de la red, estableciendo unas reglas de seguridad, ejecutar aplicaciones que gestionen las funciones de la lógica del negocio, publicar a través de la red interna e internet archivos tipo HTML para proporcionar información a la comunidad en general de la empresa, permitir el intercambio de mensajes de manera instantánea entre los usuarios de la empresa, distribuir contenido multimedia continuo en tiempo real, proveer de internet a las estaciones de trabajo filtrando contenidos y estableciendo reglas de acceso, monitorear los recursos de hardware, equipos y servicios especificados en la red y crear una conexión privada de forma segura entre las sucursales de la compañía.

Se da importancia a la utilización de un sistema con licencias de código fuente libre, tipo GPL, como alternativa eficiente para la administración segura de la red. Se describe paso a paso la instalación del sistema operativo del servidor Linux Ubuntu Server, el cual tiene como opción, descargar desde internet de forma gratuita, todas las aplicaciones, utilidades y complementos necesarios para la puesta en marcha, de dispositivos tipo servidor. Todo esto impulsado al mejoramiento del proceso de negocio de la empresa, brindando nuevas herramientas que ayuden al crecimiento de la compañía.

ABSTRACT

This document describes the activities carried out in the company Licores Capri, aimed at managing the organization's technological network, thanks to the addition of a server type device, in which different network services configured for connection, communication and permanent monitoring of the client computers physically and remotely connected to the local network of the company.

The main functions of the server are to provide a database containing domain names used on the Internet for server and network identification, dynamic addressing of a new range of IP addresses for the creation of a subnet in the workstations of the company.

Provide secure remote access to the company's server for the management of the services, allow the sending and receiving of remote files to the server, share folders for the sending of files by the computers inside the local network to server.

Monitor and control incoming and outgoing data traffic, establish security rules, run applications that manage the functions of business logic, publish through the internal network and internet HTML files for provide information to the general community of the company.

Allow instantaneous exchange of messages between users of the company, distribute continuous multimedia content in real time, to provide workstations with the Internet by filtering content and establishing access rules, monitor hardware resources, equipment and services specified in the network and create a secure private connection between the branches of the company.

It is important to use a system with free source licenses, type GPL, as an efficient alternative for the safe management of the network. It describes step by step the installation of the operating system of the Linux server Ubuntu Server, which has, as an option, download from the internet for free, all the applications, utilities and add-ons required for the startup of server-type devices. Driven to improve the business process of the company, providing new tools to help the company grow.

INTRODUCCIÓN

Un servidor es un equipo o máquina que presta muchos servicios a otros computadores clientes, los cuales proveen grandes cantidades de información, a través de una arquitectura tipo cliente servidor, sirven para atender las peticiones de otros programas, compartir datos, recursos de hardware y software por medio de la conexión a una red interna o externa.

Con el auge de internet, en la actualidad se ha facilitado los procesos de negocios en las empresas sin importar la ubicación de sus clientes o proveedores, por lo cual es esencial proporcionar a las máquinas que actúen como servidores, una seguridad mediante software o hardware para evitar accesos indebidos de agentes externos ajenos a la empresa, con el fin de que sus aplicaciones, bases de datos, y procesos prestados, se ejecuten de manera completa y la información se envíe y se reciba de forma veraz y segura.

Las ventajas que prestan estos dispositivos son entre muchas otras, el control de los recursos de la red de una empresa, crear políticas de acceso y manejo de los dispositivos conectados, compartición de recursos entre dispositivos y usuarios, organizar la información, entre otros.

En el siguiente trabajo se presenta la propuesta para la implementación, aplicación, gestión y puesta en marcha de un servidor en la empresa Licores Capri, ubicada en la ciudad de San Juan de Pasto, en el cual se instala y configura un sistema operativo Linux Ubuntu server, software de libre distribución, sin costo, que ayude a la empresa al control, organización, y seguridad de su información.

El documento que se presenta a continuación se organiza de la siguiente manera: en los primeros capítulos se presenta una contextualización general de la empresa en la cual se desarrolla este proyecto, la descripción del problema que se trata de solucionar, los objetivos que se requieren alcanzar, la justificación expuesta y fundamentada de las ventajas que se obtienen al añadir nuevos servicios para la seguridad, conexión, comunicación y administración de dispositivos de la empresa. Se describen los referentes teóricos, los cuales se necesitan para el diagnóstico y propuesta de mejoramiento de la red de la empresa, como redes, topologías, componentes, dispositivos, modelos de referencia, protocolos, y servicios de red. Después se presenta un informe el cual presenta un diagnóstico inicial de la situación en la que se encontró la red tecnológica de la compañía, se definen unos requerimientos, así como el análisis de todo el hardware y software instalado en la red. Posteriormente en la propuesta de mejoramiento de la red, se incluye el desarrollo de toda la configuración e instalación del servidor que es capaz de administrar todos los servicios de seguridad y comunicación en la red de la organización. Por último, se describen las conclusiones y recomendaciones, que

se tienen en cuenta, una vez, se ha realizado, la instalación, configuración, pruebas y puesta en marcha del servidor dentro de la red local de la organización.

1. CONTEXTUALIZACIÓN DE LA COMUNIDAD

La empresa en la cual se requiere realizar una propuesta para el mejoramiento de su red, se dedica a la venta y distribución de licores en la ciudad de Pasto, y está conformada por un grupo de trabajo el cual participa de manera activa en los procesos de negocio en el área de ventas, contabilidad, sistemas y gerencia.

En cada área se llevan tareas comerciales y administrativas, con el fin de la elaboración de reportes como estados de cuenta, facturas, inventarios, compras y ventas, que ayudan a llevar un mejor control de las actividades realizadas.

La información es ingresada por los empleados de cada área mediante una aplicación instalada en un equipo físico de la red, estos datos se guardan en archivos ubicados en un servidor principal. También, se evidencia la existencia de gran cantidad de material impreso, resultante del proceso de facturación, mediante el cual se lleva un control de ventas, y créditos realizados por la empresa.

Se evidencia la importancia de optimizar la red de cableado estructurado y conexión inalámbrica, con el fin de permitir la comunicación y conexión de nuevos servicios de red, los cuales ayuden a ofrecer un mejor desempeño y seguridad dentro de la organización.

DESCRIPCIÓN E IDENTIFICACIÓN DEL PROBLEMA O NECESIDAD

En la empresa Licores Capri se cuenta con un sistema básico para el manejo de su información y procesos como son la facturación, inventarios, contabilidad, etc. Actualmente la empresa tiene dos puntos de venta en los cuales se maneja de forma independiente esta información y no hay ningún tipo de conexión entre las sucursales lo cual ha generado una serie de problemas al momento de consolidar la información proveniente de cada uno de los puntos de venta. Entre los problemas encontrados están:

a. La información se maneja desde un computador el cual actúa como servidor y al cual acceden los demás equipos mediante la herramienta conexión a escritorio remoto haciendo ineficientes los procesos de la empresa.

b. El almacenamiento de la información de la empresa se realiza en dispositivos de almacenamiento externos los cuales son susceptibles a daños y pérdidas

c. La red y los equipos conectados a ella, no presentan ningún tipo de control ni seguridad, lo cual hace que la información de la empresa sea vulnerable frente a ataques informáticos externos.

d. Dificultad al consolidar la información proveniente de los puntos de venta

e. No existe un nombre de dominios para la identificación de los equipos de la red dentro y fuera de ella.

f. No existe un direccionamiento IP organizado de las estaciones de trabajo.

g. No se puede acceder a los equipos de la red de manera remota por lo cual se dificulta la administración de los servicios de red que existen en la empresa.

h. La empresa carece de un sitio web el cual brinde información general a la comunidad virtual de los servicios y productos ofrecidos en la compañía.

i. No es posible el envió y recepción de archivos de forma remota a la red de la empresa.

j. No existen carpetas ni ficheros, donde los equipos de la red puedan compartir archivos que puedan ser respaldados y guardados.

k. No hay reglas de seguridad para el tráfico de datos en la red.
l. No hay un contenedor donde se puedan alojar nuevas aplicaciones para la lógica de negocio de la compañía.

m. Los equipos de la red no pueden intercambiar mensajes de manera instantánea, para el control del proceso de negocio y del personal.

n. No existe un mecanismo para distribuir a través de la red contenido multimedia en tiempo real.

o. No hay control, filtrado de contenido, ni gestión de los equipos de la red que acceden a internet.

p. No hay un control ni monitorización permanente de los equipos, recursos, dispositivos y servicios especificados en la red.

Estos problemas han entorpecido el funcionamiento normal de los procesos de negocio de la organización, el cual genera un descontento entre los funcionarios de la empresa ya que hay un aumento significativo de trabajo para el personal.

FORMULACIÓN DEL PROBLEMA

¿Cómo ayudará la implementación de un servidor de servicios telemáticos a la empresa Licores Capri a mejorar la eficiencia y eficacia en la seguridad y los procesos para el manejo de la información?

SISTEMATIZACIÓN

- ¿Qué tipo de seguridad maneja actualmente la empresa para la protección de la información?

- ¿De qué manera se consolida la información que proviene de cada uno de los puntos de venta?

- ¿Cuenta la empresa con una infraestructura adecuada para la implementación de redes y servicios telemáticos?

- ¿Cómo establecer planes de mejoramiento a los servicios que actualmente se realizan en la empresa para brindar un mejor servicio a sus clientes?

OBJETIVOS Y ALCANCE

OBJETIVO GENERAL

Mejorar la conexión y la seguridad de la red de la empresa Licores Capri, poniendo en funcionamiento un servidor que facilite una comunicación segura entre las sucursales de la empresa, el cual permita prestar servicios de red a sus usuarios, para beneficio interno de la organización, minimizando gastos de licenciamiento.

OBJETIVOS ESPECÍFICOS

- Recolectar la información inicial acerca del estado de la red computacional de la empresa y las aplicaciones que utiliza.

- Poner en funcionamiento un servidor Linux, el cual añada los nuevos servicios DHCP, DNS, FTP, SSH, web, de aplicaciones, ficheros compartidos, streaming, chat, PROXY, para la comunicación y conexión segura de toda la red de la empresa

- Vigilar mediante un servicio de monitorización de red, las conexiones de equipos dentro de la red local y la conexión de otros dispositivos permitidos que requieran acceder a la red a través de internet.

- Mejorar la seguridad de la información de la empresa, durante el envío y recepción de los datos que estén contenidos en los servidores de la organización a través de un firewall.

- Respaldar los archivos de las aplicaciones utilizadas en la red, así como los archivos de configuración de los servicios instalados en el servidor, creando copias de seguridad periódicas.

ALCANCE DEL PROYECTO

Integrar a la red de la empresa, un servidor Linux que facilite y mejore de manera segura, los servicios de intercambio de información y comunicación, conexión de dispositivos, y respaldo de datos contenidos en el equipo que guarda la base de datos de las aplicaciones con las cuales se trabaja en la empresa.
Mediante una matriz DOFA, se evalúa las diferentes debilidades y amenazas, que se detectan dentro de la red computacional de la empresa, con el propósito de establecer políticas de seguridad en la red.

Se hacen recomendaciones y tutoriales que ayuden a la instalación, configuración y administración del servidor, con el fin de proteger el equipo y asegurar la continuidad de los servicios.

Se implementan servicios bajo licencias GNU Open Source, por cuestión económica, para tener en cuenta el ahorro en la adquisición de software y hardware.

El servidor cuenta con diferentes servicios de red y seguridad listados a continuación:

- Un servidor **DHCP** (Protocolo de configuración de host dinámico) mediante la aplicación **isc-dhcp-server**, para la asignación automática de direcciones IP dinámicas a los equipos clientes de la red local.

- Un servidor **DNS** (sistema de nombre de dominio) mediante la aplicación **bind9**, para la asignación de un nombre al servidor principal dentro de la red local y también para internet, ayudando a crear una conexión del servidor de la empresa con las maquinas que necesiten conectarse a este.

- Un servicio de FIREWALL a través de la herramienta **iptables**, para controlar el tráfico de información de entrada y salida bajo reglas de seguridad configuradas según los requerimientos de la organización.

- Un servidor SSH (Interprete de ordenes seguro) con la aplicación del mismo nombre, la cual permite que los usuarios, accedan de forma local y remota al terminal de configuración y administración del servidor principal, permitiendo gestionar y añadir nuevos servicios de red disponibles para este tipo de sistemas.

- Un servidor de aplicaciones, con la ayuda de la aplicación **tomcat**, que proporcione servicios de conexión a los equipos clientes con el fin de gestionar las funciones de la lógica de negocio y de acceso a los datos de las aplicaciones.
- Un servicio de archivos compartidos multiplataforma mediante la aplicación **samba**, con el fin de que el servidor Linux pueda trabajar dentro de la red con clientes que tengan instalados diferentes sistemas operativos.

- Servicio de copias de seguridad periódicas para el respaldo de la información de las aplicaciones que se utilizan en la red con la herramienta **cron**, así como copias de seguridad de la configuración del servidor.

- Servicio para la transferencia de archivos FTP (Protocolo de transferencia de archivos), mediante la aplicación **vsftpd**, entre sistemas conectados a la red basados en la arquitectura cliente servidor.

- Servidor web **apache2** el cual aloja páginas de la empresa con el fin de dar a conocer sus servicios y que usuarios de la red internet puedan obtener información de la organización a través de un hosting

- Servicio de chat con la aplicación **openfire** y plugin **meetings** para *streaming*, que permita la comunicación entre los trabajadores de la empresa para el control del personal.

- Servidor proxy a través de la aplicación **squid**, que gestione los servicios de acceso a internet a los equipos clientes de la red.

- Servicio de monitorización de la red gracias a la aplicación **nagios**, con el fin de vigilar los dispositivos y servicios especificados.

- Servicio de red virtual privada para la conectividad punto a punto con validación de usuarios y dispositivos conectados remotamente de forma cifrada, con la herramienta **openvpn**.

2. JUSTIFICACIÓN

"Las organizaciones actuales se enfrentan sin precedentes a los desafíos de exigencia y seguridad informática cada vez más complejos, donde la sofisticación y el volumen de ataques están aumentando exponencialmente causando daños a los equipos y la perdida de datos personales y de clientes"[1].

Mediante el uso de tecnologías de la información las organizaciones en la actualidad impulsan su desarrollo empresarial, ampliando el uso de nuevas tecnologías, las cuales se encargan de prestar servicios, en toda una organización.

La implementación de un servidor ayuda al funcionamiento de algunos servicios de red y seguridad, permitiendo que las aplicaciones, datos, y procesos tecnológicos requeridos en la organización estén salvaguardados, así como la creación de políticas de seguridad para la protección de la información.

Uno de los objetivos para cumplir la misión y visión de la empresa Licores Capri es el de mejorar los servicios de administración que operan en la compañía, con el fin de cumplir con el plan estratégico, y motivados por la implementación de nuevas tecnologías informáticas que sirvan de apoyo a la consecución de mejores resultados, dando gran importancia a las facilidades que proporcionan las aplicaciones de software en el control de procesos de negocio que requieran de tiempo, costos e información.

La implementación de un servidor con mayor capacidad y velocidad de procesamiento, el cual trabaja bajo un sistema operativo Linux, utilizado a escala mundial en gran cantidad de empresas, por su costo, seguridad, confiabilidad, migración y escalabilidad; mejora y amplia los servicios de red que corren en el servidor, ya que cuenta con una serie de servicios como el servicio DHCP, para el direccionamiento IP de la red interna y externa, el servicio DNS, para la asignación de un dominio disponible, a acordar con los directivos de la empresa, la resolución de las IP, los nombres del servidor y de la red, el servidor SSH para el acceso remoto a la consola de gestión del servidor de manera segura, el servicio FTP para la trasferencia de archivos remotos al servidor de la red, un firewall para controlar el tráfico de red y acceso de los equipos de la red interna y redes externas, la configuración de copias de seguridad periódicas, para respaldar la información que se obtiene de los procesos de negocio, un servidor de aplicaciones para el acceso a programas que maneja la organización en su parte

[1] CÁMARA DE COMERCIO DE PASTO. Desarrollo de tics y comunicaciones. Disponible en: www.ccpasto.org.co/index.php/desarrollo-de-tics-y-comunicaciones

administrativa, un servidor web en la que se pueda publicitar a través de internet la marca de la empresa ayudando a aumentar la cobertura de mercado; servicios de chat y streaming para el control del personal, un servidor proxy que gestione las políticas de acceso a la red interna e Internet, un sistema de monitorización de los equipos conectados a la red, y una red virtual privada para la conexión de las redes locales de las sucursales de manera remota y segura al servidor.

3. REFERENTES TEÓRICOS, CONCEPTUALES Y LEGALES

En este capítulo se realiza una descripción de la teoría básica que se necesita para el desarrollo del proyecto, brindando a la red de la empresa las herramientas y aplicaciones adecuadas que sirvan de solución a posibles riesgos y problemas encontrados, dando la mayor importancia a la instalación de un servidor capaz de proveer los servicios necesarios a los clientes de la empresa.

3.1 SISTEMA OPERATIVO

Conjunto de programas interconectados que permiten la gestión y administración de los recursos hardware de un equipo. Provee la interacción con los usuarios mediante una interfaz o consola de entrada. Comparte recursos de un equipo entre diferentes usuarios, establece mecanismos para recuperación de posibles fallos y errores de hardware, programas y de sistemas de archivos.

Entre los recursos gestionados por los sistemas operativos están las unidades de procesamiento, las unidades de almacenamiento, los dispositivos de entrada y de salida, así como los datos guardados en el equipo o los que estén compartidos en red. Entre sus objetivos principales están:

- Proveer un ambiente beneficioso de trabajo.
- Aprovechar de manera eficiente los recursos hardware.
- Asignar los recursos de un equipo de la mejor forma de acuerdo a las necesidades.
- Administrar y controlar la ejecución de los programas instalados.

En la Tabla 1, se describe los principales sistemas operativos y sus características:

Tabla 1. Tipos de sistemas operativos más conocidos

Sistema	Características	Ventajas	Desventajas
Mac OS	▪ Multi-usuario ▪ Multi-tarea ▪ Software propietario ▪ Micro-kernel ▪ Arquitectura de 64 bits. ▪ Compatible con hardware de otros fabricantes.	▪ Habilitada la línea de comandos de Unix ▪ Alto desempeño ▪ Confiabilidad ▪ Respaldo y soporte técnico	▪ *Alto Precio de hardware* ▪ *Alto precio de software*
Unix	▪ Multi-usuario. ▪ Software libre, de prueba y propietario. ▪ Multi-tarea ▪ Sistema operativo para redes ▪ Compatibilidad de hardware ▪ Diferentes distribuciones con un mismo kernel ▪ Sistema de archivos ufs ▪ Soporta arquitecturas de 32 o 64 bits.	▪ Ideal para servidores.	▪ Información limitada ▪ Capacitación limitada ▪ Altos costos
Microsoft Windows	▪ Software propietario ▪ Multi-usuario ▪ Multi-tarea ▪ Compatible con varios tipos de hardware ▪ Kernel hibrido ▪ Sistema de archivos NTFS ▪ Soporta arquitecturas de 32 o 64 bits	▪ Actualización permanente ▪ Fácil de usar ▪ Fácil de instalar ▪ Los controladores son fáciles de instalar ▪ Hay una gran cantidad de aplicaciones pagas y gratuitas disponibles para instalar.	▪ Costo de licencias ▪ Portabilidad ▪ No permite la modificación de su sistema operativo
Linux	▪ Multi-usuario ▪ Software libre ▪ Multi-tarea ▪ Compatibilidad con hardware de otros fabricantes ▪ Sus distribuciones tienen en común un mismo Kernel ▪ Sistemas de archivos ext4. ▪ Arquitectura para equipos de 32 o 64 bits	▪ Software de distribución libre ▪ Actualización permanente ▪ Portabilidad ▪ Múltiples entornos gráficos ▪ Permite modificar su kernel ▪ Requerimientos de hardware bajos para instalación ▪ No tiene costo, es gratis ▪ Gran estabilidad ▪ Seguridad ▪ Compatibilidad entre servidores ▪ Gran velocidad ▪ Gran apoyo de la comunidad. ▪ Sistema de crecimiento rápido	▪ Complejidad ▪ No existe un respaldo. ▪ No hay soporte técnico

3.2 ¿POR QUÉ UN SERVIDOR UBUNTU LINUX?

Los sistemas operativos GNU/Linux tienen como principal característica que sus licencias son basadas en software libre, el usuario manipula libremente el código del software lo cual conlleva ventajas como la mejora y personalización, de su código fuente.

Al haber una gran comunidad de usuarios trabajando por mejorar cada vez más las funcionalidades del sistema operativo, se obtiene un sistema con características de funcionalidad como:

I. Escalabilidad
II. Disponibilidad
III. Rendimiento
IV. Seguridad
V. Administración dedicada a configuraciones centralizadas y automatizadas.
VI. Facilidad de uso.
VII. Adaptabilidad.
VIII. Accesibilidad.

Ubuntu server hace parte de las distribuciones de Linux basada en Debian, sistema operativo de código abierto, el cual aumenta exponencialmente día a día su demanda, gracias a que cada vez es más amigable e intuitivo para usuarios medios, y gradualmente cada vez es utilizado en mayor número en servidores llegando en la actualidad a estar en los primeros lugares.

"Entre los aspectos más relevantes por los cuales conviene elegir un servidor Ubuntu[2] están: Ubuntu tiene una dedicación fuerte de desarrollo detrás de él y una comunidad mundial de colaboradores que trabajan juntos para actualizar y mantener sus actualizaciones de código y seguridad.

Ubuntu cuenta con soporte en línea en caso de fallas o errores que requieren su ayuda gracias a la empresa Canonical Ltda, que se encarga de estos procesos. Se puede confiar en la experiencia y respuesta rápida para aquellas cargas de trabajo de impacto critico cuando más se lo necesita

Ubuntu es fácil de instalar, mantener y actualizar. Puede completar la instalación en 25 minutos o menos en el hardware de clase servidor. Linux es estable y requiere poco mantenimiento o mantenimiento diario. Reiniciar el sistema rara vez es necesario, por lo que es la plataforma perfecta para aquellas aplicaciones y servicios de tiempo de inactividad cero. Ubuntu actualiza fácilmente desde la línea de comandos a través de un comando de los paquetes instalados.

El sistema operativo es en realidad un conjunto de programas, incluido su núcleo, conocido como Kernel. Consta de varias capas, en la capa más interna esta la

[2] HESS KENETH. (2010). Ubuntu Server: The Linux Server Operating Systems Dark Horse.

interfaz con el hardware, una capa más arriba están las funciones de administración, que asigna distintos recursos a determinado proceso.

ASPECTOS GENERALES Y LEGALES DE LA DISTRIBUCIÓN DE UBUNTU SERVER. Es un sistema operativo basado en el sistema operativo Debian, y corre especialmente en equipos para la administración tanto, de redes locales, como redes conectadas a Internet

Este sistema operativo usa un formato de paquetes de tipo deb, los cuales son operados por unas herramientas de manejo de paquetes tipo APT. Ubuntu es el sistema operativo más popular para gestionar ambientes tipo anfitrión, soportando arquitecturas para procesadores tipo Intel, AMD y ARM.

Linux hace parte de software con licencias GPL “Licencia General Publica”. Software libre, el cual brinda accesibilidad copia y uso de su código fuente para los usuarios que requieran modificarlo.

El padre de distribución Linux de Ubuntu es Debian. También conocido como Debian GNU/Linux, tiene un público fiel gracias a su estabilidad, con un sistema de instalación de apt-get y el compromiso con el software libre según la definición de la Free Software Foundation.

INTERNET. Conjunto de tecnologías que se interconectan por medio de redes distintas entre sí, no depende del computador o del sistema operativo en que se utiliza, se transmite información entre iguales o distintas plataformas, de las cuales entre ellas existirán distintos tipos de redes, como ethernet, Token ring o enlaces vía satélite. No se utilizan protocolos dependientes de una arquitectura de red específica, creando un estándar valido para cualquier tipo de red y dispositivo conectado.

REDES DE DATOS. Infraestructura que a través de ella se transporta información. Teniendo características diferentes requiriendo de varios computadores y otros dispositivos de interconexión para el envío y recepción de datos, así como para la gestión de recursos.

3.3 TOPOLOGÍAS

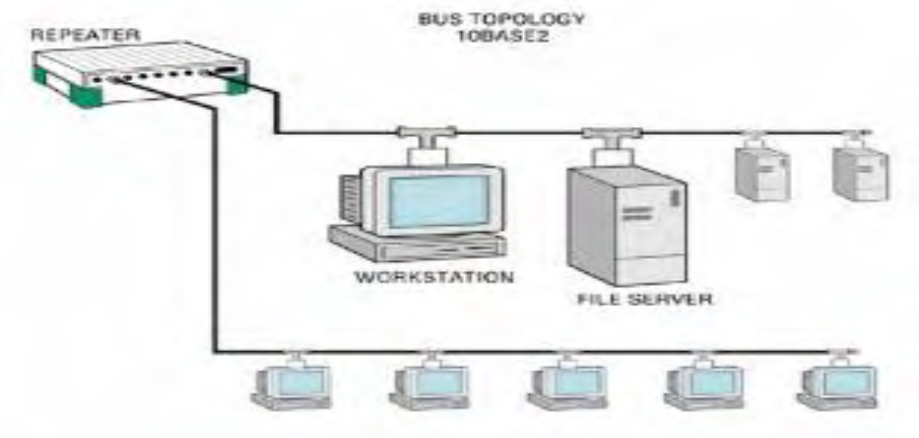
Las topologías de red hacen referencia a los tipos de conexión entre distintos dispositivos de una red, su forma de conexión es cableada. Entre las cosas que es deben tener en cuenta en el momento de elección de un sistema cableado son sus costos conjuntamente con el rendimiento e integridad de la red.

Su objetivo principal es describir la distribución física de una red. Entre el diseño de topologías más comunes se encuentran la red de área local LAN y la red de área extensa WAN.

Las formas de organizar las redes están envueltas en un constante desarrollo y transmisión, una red centralizada es la que tiene un computador que realiza todas las tareas de procesamiento de datos desde uno o más lugares distantes, una red distribuida es en la que se encuentran clientes de red procesando trabajos para usuarios finales, así como un computador ubicado en un sitio central. Los principales tipos son:

Bus. Los nodos están conectados a un medio denominado bus. En la Figura 1 se aprecia una jerarquía extendida desde un sistema central. En el momento de pasar una señal que puede ser conducida por ejemplo con cable coaxial o fibra óptica, a través del bus, todas las conexiones activas detectan señales que llevan una designación de dirección.

Figura 1. Topología de red tipo bus

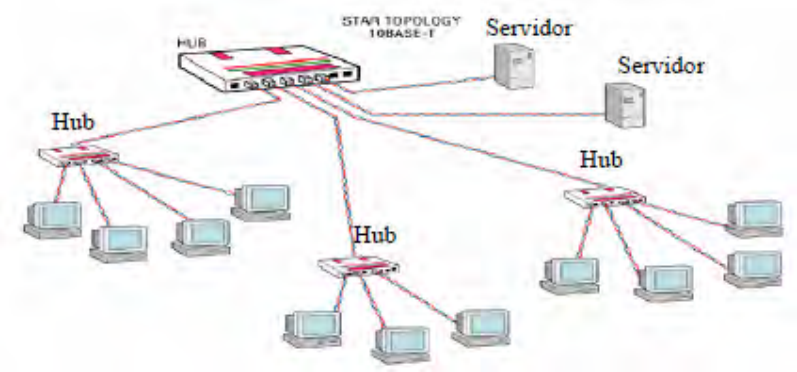


Fuente: Administración del ancho de banda en una WLAN

Uno de los sistemas más comunes en este tipo de redes es Ethernet, también los servicios de sistemas de banda ancha, los cuales tienen un cable bidireccional, y su trayectoria al mismo medio es de avance y regreso, también pueden tener dos cables para lograr direccionalidad. Su sistema se basa en los servicios de televisión por cable, los cuales tienen un procesador de señales que toma una señal de entrada de un dispositivo que se encuentre en la red y lo convierte para la retransmisión en un canal de frecuencia mayor.

Estrella. Los nodos están conectados a un medio central con conexiones punto a punto, el tamaño de la red depende de la capacidad de conexiones que soporte el medio central, en el caso de que falle este medio, todo el sistema deja de funcionar. Las operaciones de la red se hacen en un lugar determinado, el cual es alimentado por información de los clientes contiguos ingresando a un sistema central a través de líneas de comunicación como se aprecia en la Figura 2.

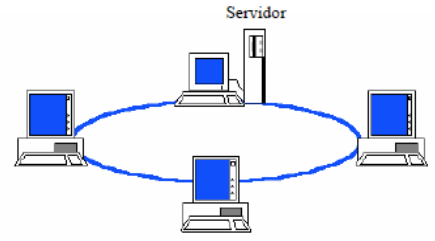
Figura 2. Topología de red en estrella



Fuente: Administración del ancho de banda en una WLAN

Anillo. La organización de este tipo de red uniendo diferentes nodos a una red de forma circular dejando una cadena que conecte a cada nodo enlazándose continuamente de izquierda a derecha, cada nodo está conectado a un nodo adyacente, esta tecnología conocida como Token-Ring forma de manera lógica un anillo, en este caso cuando un nodo falle toda la red se ve interrumpida. Entre su principal ventaja es su esquema de transmisión de señales que determinan si un nodo puede acceder a este sistema de comunicación. Ver el esquema de red en la Figura 3.

Figura 3. Topología de red en anillo

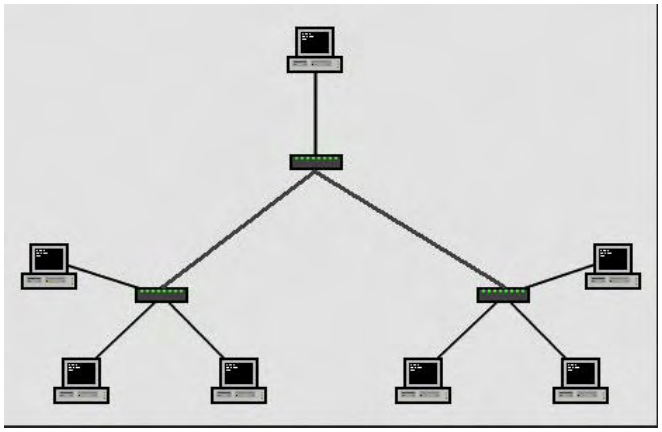


Fuente: Administración del ancho de banda en una WLAN

Árbol. Topología de red la cual sus nodos están organizados en forma de un árbol, similar a la topología estrella con la diferencia que esta no cuenta con un solo dispositivo central, cuenta además con otros dispositivos que añaden más segmentos de red. Tiene un nodo de enlace troncal, en el cual normalmente está ubicado un hub o switch, desde el cual se ramifican otros nodos. El fallo de un nodo no interrumpe la comunicación de la red y se comparte un canal de comunicaciones igual para toda la red. Se puede ver también como una combinación de varias topologías de estrella, extendidas a partir de un punto denominado la raíz.

Una de sus desventajas es el envio de datos a todos los clientes de la red sin importar su destinatario. También suelen generar interferencia entre señales cuando hay transmisión simultánea entre dos o más clientes. En la Figura 4, se muestra de forma detallada el diseño de red de este tipo de topología.

Figura 4. Topología de red en árbol



Fuente: Baum-netzwerktopologie

Malla. Todos los equipos se conectan entre sí, los nodos deben tener una capacidad para conectar muchos puertos, tiene una conectividad grande, si un nodo falla, la información puede seguirse enviando por distintas rutas. Los mensajes enviados de un nodo a otro pueden ser llevado por caminos diferentes, si una red de malla está conectada totalmente, no hay interrupción de comunicaciones, y cada servidor tiene una conexión propia con los demás equipos. Tampoco necesita tener un nodo central lo cual beneficia a la reducción de fallos, así como su mantenimiento, ya que si un nodo cae la red sigue funcionando normalmente. Como se muestra en la Figura 5, se identifica el diseño de una red en malla básica.

Figura 5. Topología de red en malla

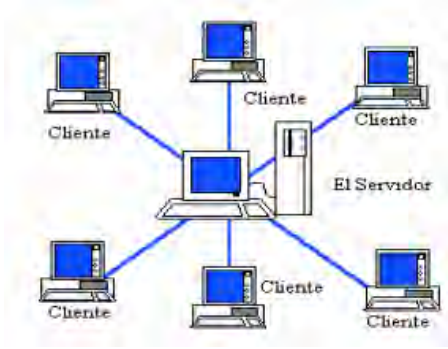
Fuente: Mesh network topology, own work

Entre sus desventajas está el alto costo que se puede incurrir implementando este tipo de red de forma cableada, exigiendo un uso más riguroso de recursos.

3.4 CLASIFICACIÓN DE LAS REDES DE ACUERDO A SU TAMAÑO

Redes LAN. Es una red pequeña que alberga de 3 a 50 clientes en una red, que se encuentra normalmente en un solo sitio y la cual le pertenece a una empresa, todos los nodos tienen una tarjeta de red, la cual les sirve para conectar a un sistema cableado en una red. Como se muestra en la Figura 6, las maquinas se conectan a través protocolos de comunicación iguales entre ellas se intercambia datos y pueden ser habilitados el compartimiento de recursos de dispositivos conectados en la red, como archivos o impresoras.

Figura 6. Muestra modelo de red LAN

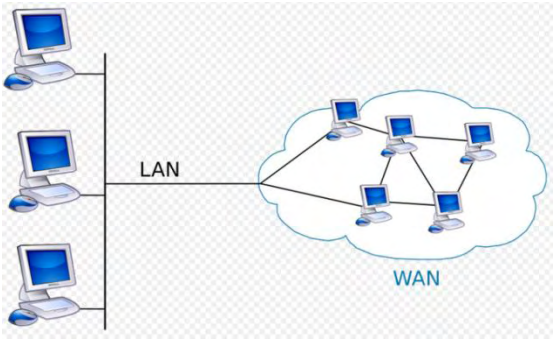


Fuente: Administración del ancho de banda en una WLAN.

Redes WAN. Este tipo de redes permite una conexión nacional o internacional mediante líneas telefónicas o de forma satelital. Esta une a varias redes locales, pero no necesariamente todos los nodos deben estar ubicado en un mismo lugar físico. Estas redes son construidas por empresas para uso privado, y otras son construidos por los proveedores de internet para dar conexión al cliente. Internet

brinda una conexión de alta velocidad por lo cual varias redes de este tipo se basan a través de esta red, sin la necesidad de tener redes privadas, mientras que una red privada virtual que tienen una seguridad en el medio de comunicación con cifrado y encriptación aumenta día a día. En la Figura 7, se muestra una interconexión entre una red local y una red de área amplia.

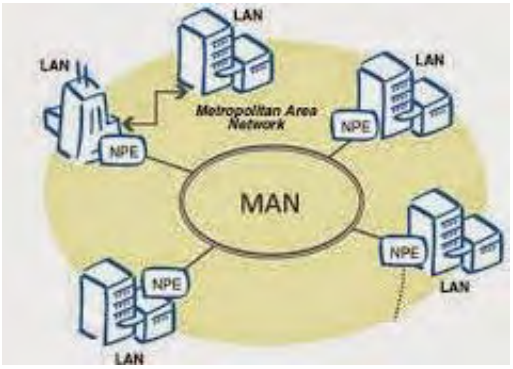
Figura 7. Interconexión entre una red LAN y una red WAN



Fuente: LAN and WAN scheme

Redes MAN. Acrónimo en inglés de Metropolitan Area Network, red de área metropolitana. Redes de fibra óptica que tienen una alta velocidad, conectado segmentos de red local de un área específica, como por ejemplo en un campus o una ciudad. Su área de cobertura geográficamente es extensa, dando la capacidad distintos tipos de servicios, sobre medios de transmisión como fibra óptica o par trenzado, su latencia es baja, tiene una gran estabilidad y no evidencia interferencias radioeléctricas. en la Figura 8 se identifica un diseño de una red tipo MAN.

Figura 8. Interconexión entre una red LAN y una red MAN



Fuente: Redes de area local. Edwin Grueso

3.5 MEDIOS DE TRANSMISIÓN

Son medios físicos que interconectan dispositivos y computadores, pueden ser tanto terrestres como aéreos, conectan entre si servidores y estaciones de trabajo.

Cable coaxial. Cuenta con un hilo conductor de cobre envuelto por una capa trenzada que funciona como polo a tierra. Entre las dos capas hay una capa gruesa de material aislante, todo en conjunto es protegido por un cable externo. Se utiliza en largas distancias, con velocidades de transmisión superior, poca interferencia, permitiendo conectar múltiples nodos. Se utiliza para televisión, telefonía, redes de área local, conexión de dispositivos a corta distancia, entre otros. Puede transmitir señales análogas o digitales. Es fácil de instalar, se puede conectar nodos lejanos, resiste interferencias mayores que el cable de par trenzado, soporta anchos de banda mayores que los del cable de par trenzado, robusto y resistente al mal trato, utilizado en internet tipo delgado para distancias cortas, y tipo grueso para distancias largas Sus desventajas son la atenuación, el ruido técnico y ruido de intermodulación, perdida de datos, algunos cables son pesados y costosos.

Cable UTP. Acrónimo en inglés de Unshielded Twisted Pair, traducido como cable de par trenzado. Cable de cobre recubierto de una capa plástica como se muestra en la Figura 9, este se conforma de ocho hilos trenzados en pares, con el fin de la reducción de ruido durante la transmisión de información. Últimamente ha crecido la conexión de una red local con este tipo de cableado, el cual transporta datos con una velocidad de 10Mbps o más rápido.

Figura 9. Cable UTP categoría 5

Fuente: Network & ethernet cables, cableorganizer

Entre las ventajas que presenta este tipo de cable son su bajo costo, es fácil de instalar, la distancia más grande para la conexión entre un nodo y un repetidor de señal es de 100 metros, soporta velocidad de transmisión de más de 100 Mbps, más grandes que un cable coaxial, es una tecnología conocida compatible con tipos de redes Ethernet o anillo, resistente a interferencias de señales, ofrece un gran rendimiento relacionado con su costo económico. Sus principales desventajas son que no soporta a condiciones extremas de interferencia, rayos, corrosión, cruce de señales, por lo cual se recomienda instalarlo en lugares con poca interferencia electromagnética.

Fibra óptica. Medio dúctil y muy refinado conductor de energía tipo óptica. La forma de un cable de este tipo es cilíndrica y por dentro se identifican tres secciones, núcleo, revestimiento y cubierta. El núcleo formado por fibras de cristal o de plástico alrededor protegido por su cubierta hecha de material platico, aísla lo que lleva adentro de, humedad, aplastamiento, entre otros. Sirve mucho para grandes distancias como conexiones LAN. Los beneficios principales frente a los otros tipos de cables son que permiten mayor ancho de banda, su peso y su tamaño son menores, hay menor atenuaciones de señales, tiene un aislante electromagnético, y puede abarcar mayores distancias entre repetidores. Es un medio seguro, puede transmitir voz, video y datos por un mismo canal. Ver Figura 10.

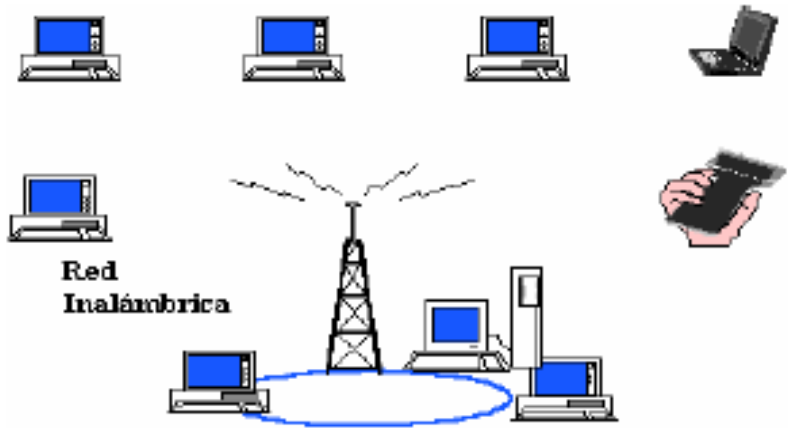
Figura 10. Cable de fibra óptica

Fuente: Fibra óptica, alambre y cable, www.coatindustrial.com

Este tipo de cables e interfaces de red son de costos elevados, teniendo un cuidado riguroso en su manejo, ya que son difíciles de configurar, y necesitan más destreza para conectar e instalar estos tipos de cable.

Transmisión inalámbrica. El medio de transmisión inalámbrico es principalmente a través del aire, mediante una antena se genera energía electromagnética, la cual es recibida por otros dispositivos que tienen una antena también, su configuración puede ser direccional u omnidireccional, en la primera, la señal se potencia en un punto emitida a cierta dirección, el receptor debe estar alineado con el emisor, la segunda configuración, la energía se dispersa en todas las direcciones, por lo cual varias antenas pueden captar esta señal, en enlaces punto a punto se usan microondas, para conexiones con varios nodos receptores se utilizan las ondas de radio, las señales infrarrojas se usan para transmisión a corta distancia. En la Figura 11, se muestra un diagrama de transmisión inalámbrica.

Figura 11. Modelo de red de transmisión inalámbrica



Fuente: Administración del ancho de banda en una WLAN

3.6 COMPONENTES DE UNA RED

Servidor. Existen variedad de conceptos para definir este importante miembro de la red, entre los más importantes están:

- Es un computador en el cual se ejecuta una aplicación el cual realiza una tarea específica en servicio de otros computadores denominados clientes.

- No necesariamente es una maquina con altas especificaciones y características, puede ser desde un computador antiguo, hasta un equipo potente, la escogencia del equipo depende del uso que se le quiera dar al servidor.

- Es un computador, que se encarga de brindar un servicio a otros computadores que se conectan con él.

Su finalidad es atender a múltiples usuarios, demandando gran carga de trabajo, capacidad de respuesta rápida, y la recuperación de interrupciones de manera inmediata, es por eso que un servidor, para responder a muchas peticiones de una red, debe contar con características mínimas como:

- Dos procesadores de 2.66 Ghz
- 4 Gigabytes de memoria RAM
- Disco duro de 200 Giga Bytes.

Un servidor siempre debe estar activo, a la orden de cualquier usuario sin importar ni fechas ni horas.

Estaciones de trabajo. Son los equipos clientes asignados para tareas específicas o varias simultáneamente, como referencia de este trabajo se necesitan máquinas para captura, administración y consulta de información, se recomienda cumplir con los requisitos mínimos que las aplicaciones requieran, no necesariamente equipos sofisticados, capaces de cumplir con las funciones encomendadas.

Tarjetas de interfaz de red. Todos los equipos que requieran conectarse a la red necesitan de una tarjeta de interfaz de red, la cual debe ser conectada a un cable o mediante conexión inalámbrica, que admitan diversos medios, hace la configuración de red mucho más fácil tomando en cuenta sus costos, la distancia del cableado y la topología que se requiere implementar.

3.7 DISPOSITIVOS DE UNA RED

En la Tabla 2, se presentan las definiciones e imágenes de los dispositivos que se necesitan, para hacer una conexión básica de la red con los servicios prestados de un servidor, para que gestione y administre las estaciones de trabajo y equipos de una organización, tanto de forma local como remota, así como garantizar su acceso seguro a internet.

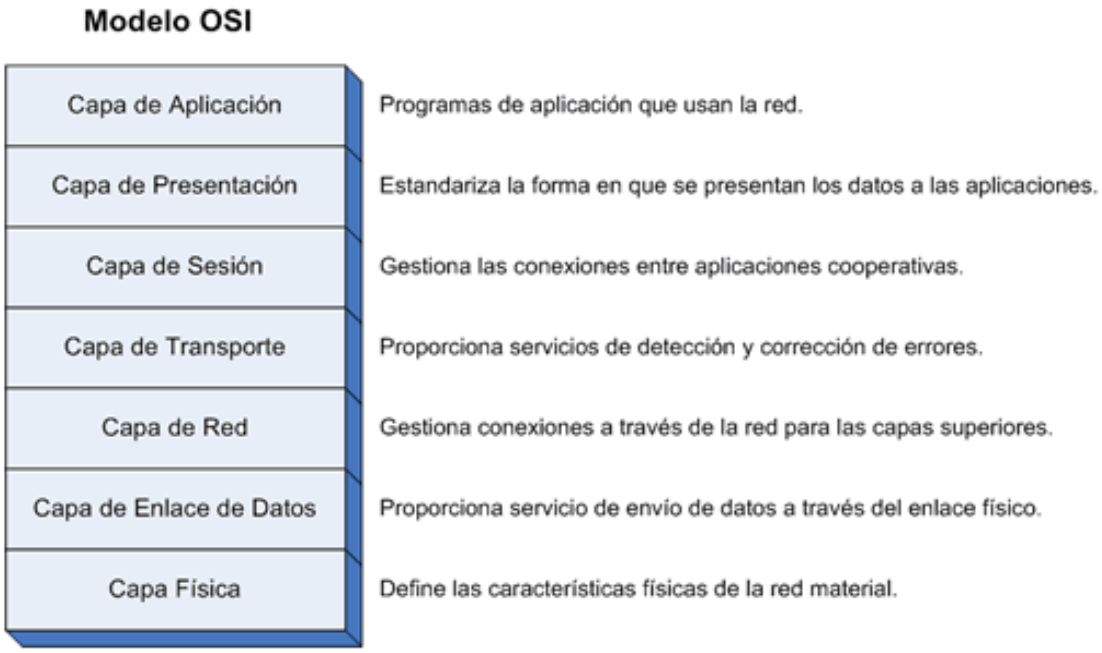
Tabla 2. Dispositivos de red

Dispositivo	Descripción	Imagen
SWITCH	Tiene como función principal la recepción de paquetes, revisa de donde procede y lo envía a su destinatario, distribuye el ancho de banda de manera igual entre los equipos conectados.	
ACCESS POINT	Punto de acceso inalámbrico que conecta dispositivos de comunicación inalámbrica para conectarlos dentro de una red.	
ROUTER	Determina la unión de redes, provee seguridad a una red, se compone de una interfaz, con la cual se puede conectar a varias redes.	

3.8 MODELO DE REFERENCIA OSI

Acrónimo en ingles de Open Systems Interconnect, modelo desarrollado por la ISO (International Standards Organization). Tiene como objetivo principal solucionar la compatibilidad entre redes conformadas por varios componentes y dispositivos, y los servicios ofrecidos por los diferentes proveedores de internet, formado por 7 capas que especifican la función de los protocolos de comunicación. Cada capa del modelo representa una tarea realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia. En la Figura 12, se muestra cada capa de la arquitectura del modelo, y una comparación entre ellas.

Figura 12. Modelo OSI



Fuente: Comparación modelo OSI. Textos científicos

Entre sus funciones principales se encuentran:

Capa física

- Transmitir el flujo de bits a través de un medio.
- Manejar voltajes y pulsos eléctricos.
- Describir cables, conectores, componentes y dispositivos de interfaz con el medio de transmisión.

Capa enlace de datos

- Ordenar el flujo de bits bajo una trama con un formato definido.
- Para formar una trama, esta capa debe agregar secuencias de bits al principio y al final del flujo inicial de bits.
- Transferir tramas de forma segura libre de errores, utilizando reconocimientos y retransmisión de tramas.

Capa de red

- Se encarga de dividir mensajes de la capa de transportes en paquetes y de su ensamble al llegar los paquetes.
- Utiliza la capa de enlace para él envió de paquetes encapsulados en una trama.
- Enrutamiento de paquetes.
- Envía los paquetes de nodo a nodo usando un circuito virtual o en forma de datagramas.
- Controla la congestión de red.

Capa de transporte

- Realizar conexiones punto a punto sin errores para el envío y recepción de paquetes.
- Multiplexación de la conexión entre diferentes procesos del usuario.
- Difundir mensajes (broadcast) a múltiples destinos.

Capa de sesión

- Permitir establecer una sesión a los usuarios en diferentes equipos.
- Controlar el dialogo entre nodos, quien habla, cuanto tiempo, half dúplex o full dúplex.
- Permitir la sincronización de equipos en las redes.

Capa de presentación

- Establecer una sintaxis de los datos transmitidos.
- Definir de los campos de un registro como nombres, dirección, teléfono.
- Definir el código a usar para representar cadenas de caracteres como ASCII
- Compresión de datos.
- Criptografía.

Capa de aplicación

- Transferencia de archivos (ftp).
- Login remoto (ssh).
- Compartimiento de archivos (samba).

La instalación de los servicios de red en un servidor, se definen en la capa de aplicaciones, permitiendo una función de comunicación, la cual puede ser realizada por varios protocolos.

Entre las ventajas que se encuentra en este modelo de referencia, son la reducción de cambios de hardware, es decir, que se pueden añadir nuevas aplicaciones sin cambios en la red física, también se puede añadir nuevo hardware sin necesidad de configurar el software de aplicación.

3.9 PROTOCOLOS DE COMUNICACIÓN

Reglas y procedimientos para establecer una comunicación, cuando una red de computadores se interconecta, todas las reglas y procedimientos que gestionan la conexión se llaman protocolos, los cuales tienen propósitos distintos, y efectúan distintas tareas. El modelo OSI distingue a estos protocolos en varias capas, trabajando juntos algunos, conocidos como pila de protocolos.

3.10 TCP/IP

Acrónimo de Transmition Control Protocol / Internet Protocol, traducido como Protocolo de control de transmisión, protocolo de internet, reglas que permiten que internet sea una red global, y transmiten datos entre distintos computadores de diferentes redes remotas, la cual se usa de manera transparente en las redes que estén conectadas a estas, también trabajan a un nivel inferior en algunas aplicaciones conectadas a la red de cada sistema operativo.

Como se evidencia en la Tabla 3, se identifican las capas del modelo de referencia TCP/IP, así como ejemplos de protocolos disponibles por cada capa.

Tabla 3. Capa modelo de referencia TCP/IP

Capa de aplicación (HTTP, FTP, TELNET, SSH,DNS,RIP,SNMP)
Capa de transporte (UDP, TCP, DCCP, UTP,ICMP,FCP)
Capa de red (IP,ICMP,IPSEC,IGMP)
Capa de acceso a la red (Ethernet, Token Ring,ARP,L2TP,NDP)
Capa física (Cable coaxial, par trenzado)

Su capa más baja es la física, la cual hace referencia al medio físico por el cual la información pasa, un ejemplo sería un cable de red, ondas o enlaces vía satélite. La siguiente capa de acceso a la red determina la manera en que los equipos envían y reciben los datos a través de la capa física. Estas dos capas no forman parte de este, la siguiente capa de red define como se transmiten los mensajes a través de distintos tipos de redes, el protocolo más conocido e importante es el IP, donde proporciona su direccionamiento determinando caminos eficientes a través de los routers que siguen los paquetes desde el origen al destino. Una vez establecida la comunicación entre las anteriores capas, la capa de transporte utiliza la comunicación enviando y recibiendo los paquetes que la capa de red fragmenta en paquetes, considerando la comunicación entre redes establecidas, la capa de aplicaciones nos proporciona los distintos servicios de Internet: FTP, SSH, SSH, HTTP.

3.11 IP

Este protocolo se ocupa de establecer una conexión y una comunicación entre diferentes sistemas, enviando mensajes sin garantizar su entrega, fragmenta los mensajes en pedazos permitiendo unirlos una vez llegan a su destino, reconstruyendo los paquetes en su secuencia correcta conforme van llegando.

3.12 DIRECCIONES IP

Dirección asignada a cada dispositivo de una red, organizada en una serie de números con cuatro octetos, cada uno de estos define una dirección única, en una parte representa una red con su respectiva subred si es necesario, y la otra parte representa un nodo especifico, identificando cada host, en internet no puede haber dos computadores con 2 direcciones IP idénticas, aunque se puede tener varios ordenadores con una misma dirección IP, siempre y cuando pertenezcan a redes independientes entre sí, siempre y cuando ninguna ruta las conecte.

Su representación general es de la forma a.b.c.d, cada una de las letras le corresponde un número entre 0 y 255, sus formas de representación pueden ser de forma hexadecimal o en forma binaria.

De acuerdo con las necesidades, se definen varias clases de redes, fijando diferentes lugares donde se dividen las direcciones, las clases son:

- CLASE A: red comprendida entre 1.0.0.0 hasta 127.0.0.0. El número de la red está contenido en el primer octeto, en las restantes se define la identificación de los hosts dentro de esa red. Estas usan 7 bits para el numero de red lo cual

permite 126 redes, los 24 bits restantes se asignan para el numero de hosts, los cuales pueden ser hasta 16,777,214 hosts.

- CLASE B: red comprendida entre 128.0.0.0 hasta 191.255.0.0. El número de la red está definido entre los dos primeros octetos. Estas direcciones usan 14 bits para el número de red, y los restantes 16 bits para la asignación de hosts, de modo que se pueden usar 16382 redes de 65534 host cada una.

- CLASE C: red comprendida entre 192.0.0.0 hasta 223.255.255.0. El número de la red está contenido en los 4 primeros octetos. Usan 14 bits para el numero de red, y 8 para los hosts, por lo cual se pueden usar 2,097,150 redes y hasta 254 host por cada red.

- CLASE D: reservadas para multicasting (multidifusión), se usan para direccionar grupos de hosts.

3.13 CLASIFICACIÓN DIRECCIONES IP

De acuerdo a su función las IP pueden ser:

IP pública. Direcciones visibles en todo internet, un equipo conectado con una IP publica es visible desde cualquier otro punto conectado a internet, para la conexión a la red internet es necesario contar con una dirección IP pública.

IP privada. Son direcciones reservadas, visibles por otros hosts de una red en particular o de otras redes privadas interconectadas por medio de routers, utilizados en una empresa para las estaciones de trabajo, los computadores conectados con una IP privada salen a internet por medio de un router o de un proxy el cual tenga una IP publica, estos equipos dentro de una red no pueden ser accedidos desde internet con estas direcciones.

3.14 SUBREDES

Es una subdivisión lógica de una red IP, y la práctica de dividir una red en dos o más subredes es conocida como subnetting. Los equipos que hacen parte de una subred son asignados con un grupo de bits idénticos en su dirección IP, esto hace posible la división lógica de direcciones IP en dos campos, uno con el prefijo de la red y el otro con un identificador de host, el resto de los campos contiene un identificador para un host especifico de la red. El prefijo de la ruta expresado en notación CIDR (Acrónimo en inglés de Classless Inter-Domain Routing), método

por el cual se puede localizar una dirección IP y su ruta, se escribe primero con la primera dirección IP de la red, seguido por el carácter slash (/) , terminando con el tamaño en forma de bit del prefijo, por ejemplo, 192.168.1.0/24 es el prefijo de una red que empieza por la dirección dada, teniendo 24 bits localizados para el prefijo de la red y los 8 restantes reservados para la dirección de host.

3.15 SERVICIOS DE RED

Es un servicio el cual se lo presta con software y hardware con el objetivo de proveer a los usuarios de una red de equipos herramientas que faciliten un trabajo. Estos servicios son implementos, gestionados y administrados desde uno o varios servidores.

3.16 TIPOS DE SERVICIOS EN RED

Una red se conforma de distintos dispositivos, los cuales pueden ser equipos de computación, periféricos, dispositivos de red, y una infraestructura de conectividad cableada o inalámbrica, con el fin de establecer una comunicación en la red, esta comunicación puede ser mejorada con una serie de servicios, que ayuden a mejorar la productividad de los equipos clientes.

Los servicios de red a implementar, son:

Servidor DHCP. Acrónimo en inglés de Dynamic Host Configuration Protocol, traducido como protocolo de configuración de host dinámico. Protocolo de tipo cliente servidor que ofrece servicio de direccionamiento dinámico a equipos conectados a una misma red, asignando una dirección exclusiva a un equipo que lo solicite para establecer comunicación con la red.

Existen 3 mecanismos para la asignación de direcciones IP, asignación automática, dinámica y manual. Según el autor Droms, R. “En la asignación automática, el servidor DHCP asigna una dirección IP permanente a un cliente. En la asignación dinámica, el servidor DHCP asigna una dirección a un equipo cliente por un periodo limitado de tiempo, o hasta que el cliente libera la dirección. En la asignación manual, una dirección IP es asignada por el administrador de red, y el servidor es usado únicamente para asignar la dirección al cliente. Una red particular usa uno o más de estos mecanismos, dependiendo de las políticas del administrador de la red”[3].

[3] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, Marzo 1997, <http://www.rfc-editor.org/info/rfc2131>.

Servidor DNS. Acrónimo en inglés Domain Name System, traducido al español es sistema de nombres de dominio. Sistema que organiza de manera jerárquica a equipos, servicios o recurso conectado a internet o una red privada. Atiende peticiones de búsqueda de equipos en una red. Utiliza una base de datos donde guarda los nombres y las direcciones de los equipos para localizarlos de manera más rápida.

Los servidores de nombre de dominio manejan dos tipos de datos, “El primer tipo de datos se agrupa en conjuntos denominados zonas; cada zona es la base de datos completa de un subárbol particular del espacio de dominios. Estos datos se los conoce como autoritativos”. “El segundo tipo son datos en cache los cuales han sido adquiridos por resolución local. Estos datos pueden estar incompletos, pero mejoran el rendimiento del proceso de recuperación cuando datos no locales son accesados repetidamente”[4].

Servidor SSH. Acrónimo en inglés de Secure Shell, traducido al español como intérprete de órdenes seguro. Protocolo que sirve para el acceso a equipos remotos a través de una red.

Se maneja mediante un intérprete de comandos, permitiendo establecer una comunicación segura con otros equipos para él envió y copia de datos enviando toda la información mediante un canal de comunicación seguro.

Se lleva a cabo un handshake (traducido como apretón de manos) encriptado, para que el cliente pueda verificar que se está conectando con el servidor correcto. La capa de transporte de la conexión entre el cliente y la maquina remota es encriptada mediante un código simétrico, el cliente se autentica ante el servidor y finalmente el cliente remoto actúa sobre la maquina remota sobre la comunicación encriptada.

El protocolo permite configurar parámetros de seguridad, se utiliza un método de autenticación de claves públicas, permitiendo varios tipos de configuración, como “El método de intercambio de claves, algoritmo de clave pública, algoritmo de encriptación simétrica, algoritmo de autenticación de mensajes y el algoritmo de hash”[5].

[4] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, noviembre 1987, <http://www.rfc-editor.org/info/rfc1035>.
[5] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, Enero 2006, <http://www.rfc-editor.org/info/rfc4253>.

Servidor FTP. Acrónimo en inglés de File transfer Protocol, traducido al español como protocolo de transferencia de archivos. Protocolo usado para la transferencia de archivos, ofrece ficheros a clientes que utilicen programas FTP o navegadores que soporten el protocolo, el equipo servidor escucha de la red las conexiones que piden archivos desde otros equipos de la red.

Sus características principales son "promover el intercambio de archivos (programas de computación y/o datos, fomentar indirecta o implícitamente (mediante programas), el uso remoto de computadores", blindar al usuario de variaciones en los sistemas de almacenamiento de archivos entre host, y transferir datos de forma segura y eficiente"[6].

Servidor de archivos. Protocolo el cual configura directorios los cuales están disponibles para compartir a través de una red, tal como documentos, archivos de sonido, fotografías, videos, imágenes, bases de datos entre otros, las cuales se acceden a través de los equipos clientes conectados a una misma red.

Una aplicación la cual brinda este servicio, es samba, la cual provee servicios de archivos e impresoras configurados en clientes con sistema operativo Windows, Unix, Linux, entre otros, desarrollado bajo términos de aplicaciones GNU (Licencias publicas generales).

Firewall. Traducido al español como cortafuegos, es un sistema de seguridad que monitorea y controla el tráfico de datos que entra y sale dentro de una red, basado en unas reglas de seguridad preestablecidas.

Los firewalls están presentes en dispositivos de red, los cuales se encargan de las políticas de seguridad en las organizaciones, varios métodos han sido usados para implementar firewall, estos filtran el tráfico de red en una o más de siete capas del modelo OSI, principalmente en las capas de aplicación, transporte y red.

La configuración de estos dispositivos involucra unos conjuntos de reglas de filtro conocido como políticas, estas reglas pueden ser bastante complejas y propensas a errores. Una vez las políticas han sido especificadas, el firewall necesita ser probado para determinar si se ha implementado la política correcta.

La misión del firewall es la de aceptar o denegar el tráfico de información configurado, funcionando generalmente denegando cualquier trafico producido, cerrando todos los puertos de un servidor.

[6] Postel, J., "File Transfer Protocol specification", RFC 765, DOI 10.17487/RFC0765, Junio 1980, <http://www.rfc-editor.org/info/rfc765>.

Iptables es una aplicación que administra el firewall del sistema operativo, y puede definir tablas que contengan cadenas o reglas para la manipulación de paquetes, las reglas y cadenas pueden ser de estos tipos

- Cadenas INPUT: los paquetes destinados al servidor atraviesan esta cadena.
- Cadenas OUTPUT: los paquetes creados desde el servidor atraviesan la cadena.
- Cadenas FORWARD: los paquetes que pasan por el servidor deben ser encaminados al destino recorren la cadena

Servidor de aplicaciones. Servicio que ejecuta aplicaciones ocupando gran cantidad de espacio entre servidores de bases de datos, y equipos clientes, estableciendo comunicaciones entre sí, gestiona las funciones de lógica de negocio y acceso de los datos de las aplicaciones, permitiendo tener una alta disponibilidad de los datos, gran escalabilidad, fácil mantenimiento, gran seguridad, así como integridad de la información.

"Un servidor de aplicaciones es un Framework que provee facilidades para crear tanto aplicaciones web como un ambiente para que se ejecuten. Contienen un modelo de capas comprensible, actúa como un conjunto de componentes accesibles por el desarrollador de software a través de una API definida por su misma plataforma"[7].

Servidor web. Servicio que generalmente proporciona información estática a un navegador, cargando un archivo y publicándolo a través de la red, al navegador de los equipos clientes. El lenguaje con que hablan el servidor y los equipos clientes es HTML.

El servidor Apache desarrollado a principios de 1995, es uno de los servidores web más populares en el mundo, ayudando de manera eficiente al crecimiento de la World wide web, en el 2009 se convierte en el primer software que gestionaba más de 100 millones de sitios web. Desarrollado y actualizado por una comunidad de desarrolladores bajo el auspicio de su fundación, más comúnmente usado en sistemas basados en Linux, aunque está disponible para la mayoría de sistemas operativos.

Soporta una gran variedad de herramientas, implementadas como módulos, los cuales extienden su funcionalidad, por ejemplo, el soporte de lenguajes de programación como Perl, Python y PHP, módulos de autenticación, como mod-

[7] "Application server". www.jsonpedia.org. Publicado 2015-10-16.

auth, Capas de puertos seguros y soporte para capas de transporte segura, un módulo para proxy, y un módulo de reescritura de la URL, métodos de compresión de archivos, módulos de detección de intrusos y un motor de prevención para aplicaciones web. Una de sus características más importantes es que usa host virtuales con el fin de gestionar diferentes sitios web de manera simultánea.

Servidor de Chat. Permiten el intercambio de mensajes de manera instantánea entre múltiples usuarios conectados a una red generalmente Internet a través de un software el cual administra y controla la información de los usuarios y los servicios que se les brindaran.

También se pueden crear diferentes grupos de usuarios entre los cuales se podrán intercambiar mensajes los cuales pueden contener además del texto, elementos de multimedia como música, fotos, videos o enlaces a diferentes páginas web o incluso realizar un video chat siempre y cuando el equipo cuente con los dispositivos requeridos para esto.

En general, se usa el protocolo XMPP (traducido como Extensible Messaging and Presence Portocol), el cual se define como "Un protocolo abierto de XML (Extensible Markup Language) para mensajería en tiempo real, presencia y servicios de petición-respuesta"[8].

Openfire es una aplicación que implementa el protoco XMPP, el cual permite dar servicio de mensajería instantánea y servicio de chat en grupo escrito en java, desarrollado bajo un modelo comunitario, como parte del proyecto Ignite RealTime, La administración de esta aplicaciones es hecha a través de su interface web, la cual corre en los puertos 9090 y 9091 por defecto, los administradores pueden conectarse desde cualquier lugar y editar el servidor y sus configuraciones, su instalación es amigable y guiada, con la opción de crear una base de datos propia de la aplicación o conectarla con un controlador de bases de datos para guardas los mensajes y los detalles de usuario, puede soportar más de 50.000 usuarios al mismo tiempo.

Hay variedad de herramientas que se las puede instalar como plugins disponibles de forma gratuita para su descarga las cuales pueden ser instaladas mediante la consola de administración, también permite instancias multiples del servicio para que trabajen de manera conjunta en ambientes tipo cluster.

[8] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, DOI 10.17487/RFC3920, Octubre 2004, <http://www.rfc-editor.org/info/rfc3920>.

Servidor de streaming. Distribución de contenido multimedia continúa en tiempo real. El contenido distribuido puede ser tanto radio como video. Se caracteriza por ser una conexión rápida sin pérdidas excesivas de paquetes.

Para su funcionamiento esta tecnología utiliza un buffer de datos el cual va almacenando el contenido de la descarga y luego casi de manera inmediata lo muestra al usuario. En la utilización del streaming se hace necesario tener una conexión de por lo menos el mismo ancho de banda con la que se recibe la transmisión del servicio.

Este servicio es ofrecido como un plugin dominado Meetings el cual se puede descargar en la aplicación Openfire y se lo gestiona desde la consola de administración de este programa.

Servidor Proxy. Este servidor es un intermediario entre las peticiones que realiza una maquina cliente al servidor a través de un navegador web y una red como Internet. Cuando se navega mediante este servidor, las solicitudes realizadas por el navegador llegarán al proxy y este a su vez realizara la petición al servidor que provee el servicio al que se quiere tener acceso, de esta misma forma, las respuestas enviadas por el servidor deberán atravesar primero el proxy antes de llegar a nuestro navegador.

Además de recibir peticiones del usuario, el servidor proxy almacena paginas e información en un espacio de la memoria denominado cache de tal manera que cuando se recibe una nueva petición el proxy verifica si esta ya se ha realizado con anterioridad y de ser así se muestra una copia de la página, siempre y cuando esta no haya sido actualizada. Este mecanismo mejora el rendimiento y velocidad de la conexión a internet de los equipos que están detrás del proxy.

Como lo indica la RFC 2616 existen dos tipos de proxy: “Un ‘proxy transparente’ es un proxy que no modifica la petición o respuesta más allá de la que es requerida para su autenticación e identificación. Un ‘proxy no transparente’ es un proxy que modifica la petición o respuesta a fin de proporcionar algún servicio añadido al agente de usuario, tales como un grupo de servicios de anotación, transformación de multimedia, reducción de protocolos, o filtración de anonimato”[9].

Una de las aplicaciones más conocidas que implementa este protocolo es Squid, la cual se la puede descargar de forma gratuita en los repositorios oficiales de Ubuntu, después que el servidor proxy es instalado, los exploradores web pueden ser configurados para usar este como un servidor HTTP proxy, permitiendo que el

[9] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", DOI 10.17487/RFC2616, Junio 1999, <http://www.rfc-editor.org/info/rfc2616>.

programa retenga copias de documentos que han retornado los cuales, en repetidas ocasiones para los mismos documentos pueden reducir el tiempo de acceso, así como una disminución del consumo de ancho de banda, es supremamente útil para gestionar la velocidad de internet de los equipos clientes, y poder compartir a una red LAN conexión a internet.

Entre las funcionalidades más importantes están:

- Reducción del tráfico de red
- Mejora de velocidad
- Filtrado de contenidos
- Esconder la identidad de un servidor web
- Dar servicio web a otros usuarios
- Modificar contenidos de servidores web
- Cambios de formatos de páginas web
- Mejorar la privacidad del tráfico web

Servicio de monitoreo de red. Sistema de monitorización de redes, su función es la de identificar los equipos y servicios especificados en una red. Informando de posibles cambios y comportamientos de los dispositivos configurados. Vigila los recursos de hardware. Así como la asistencia remota mediante servicios SSH.

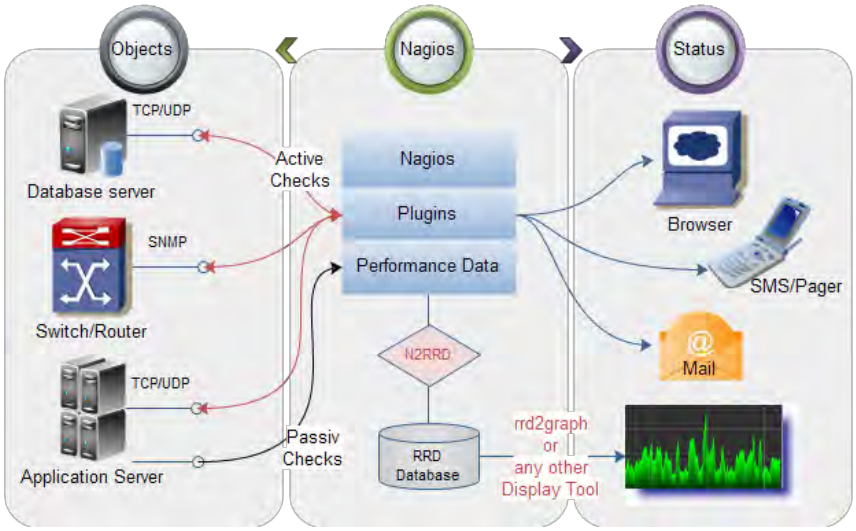
Mediante este sistema se evalúa generalmente, el tiempo de respuesta y la disponibilidad entre el cliente y servidor, aunque han empezado a tomar fuerza otras características importantes para ser evaluadas como son la consistencia y la fiabilidad.

Cuando se presenta algún problema en el sistema como fallas de peticiones de estado tales como el tiempo de espera agotado, la conexión no puede ser establecida, entre otros, el sistema genera notificaciones al administrador de la red mediante el uso de correos electrónicos, alarmas o ventanas emergentes para que se ejecuten las correcciones pertinentes y evitar así un posible daño aun mayor del que ya se ha notificado.

Un programa que permite hacer el monitoreo de la red es Nagios, el cual puede alertar sobre aplicaciones, servicios y dispositivos de red, diseñado originalmente para correr bajo Linux y su licencia es gratuita.

En la Figura 13, se muestra como Nagios opera y gestiona distintas características en una red:

Figura 13. Principios operativos de Nagios



Fuente: Operating principle of nagios. Badri Pillai

Servicio VPN. Servicio que provee una forma de conexión privada en una red que se conecta a través de Internet. Permite a los usuarios enviar y recibir información en redes públicas o compartidas, permitiendo que dispositivos especificados que se encuentren fuera de una red privada se conecten de forma segura y eficaz dentro de esta. Provee gran funcionalidad, seguridad y gran beneficio en la gestión de la red para los usuarios.

Este tipo de servicios simulan una conexión punto a punto creando un túnel a través del cual viaja la información encriptada y solo puede ser recibida si el usuario de destino tiene las llaves de acceso para des encriptar esa información como se explica a continuación: “Para emular un enlace punto a punto, los datos son encapsulados o empaquetados, con un encabezado que proporciona información de enrutamiento que le permite atravesar la interconexión de redes de transporte públicas o compartidas para alcanzar a su destino. Para emular un enlace privado, los datos enviados son encriptados para su confidencialidad. Los paquetes que son interceptados en las redes públicas o privadas son indescifrables sin las claves de encriptación. La parte de la conexión en la cual los

datos privados son encapsulados es conocida como Túnel. La parte de la conexión en la cual los datos son encriptados es conocida como la conexión de red virtual privada (VPN)"[10].

OpenVPN es una aplicación que implementa una red virtual privada para la creación segura de conexiones punto a punto o sitio a sitio de forma enrutada o modo puente para el acceso remoto, usa un protocolo de seguridad tipo SSL/TLS para intercambio de llaves, entre sus características principales se encuentra la encriptación de datos y el control de los canales de comunicación, autenticación, servicio de red, gran seguridad y extensibilidad disponible para la mayoría de plataformas incluidos sistemas móviles.

La configuración ethernet bridging, combina una interface ethernet con una o más interfaces tipo TAP, las cuales forman un puente juntas bajo el nombre de una interface de red simple tipo puente, sirve para conectar múltiples interfaces virtuales o físicas, en una máquina común mientras esta esté compartiendo una subred.

[10] Microsoft TechNet, https://technet.microsoft.com/en-us/library/bb742566.aspx

4. INFORME DE RESULTADOS

4.1 DEFINICIÓN DE LA SITUACIÓN ACTUAL DE LA RED DE LA EMPRESA

La empresa cuenta con dos sucursales, la sede principal se encuentra ubicada en el barrio las cuadras, y la otra en el centro de la ciudad, su infraestructura de red permite establecer comunicación con un servidor que guarda toda la información administrativa y contable de la organización proveniente de los equipos ubicados en cada sede.

El servidor actual tiene instalado el sistema operativo Windows 7 Ultímate en su versión de 64 bits. También cuenta con la aplicación Manager en su versión 6.1.M29, la cual es un software de gestión contable y tributaria, mediante el cual se administran las operaciones diarias de la empresa, como registros de compras, ventas, proveedores, tarifas, estados de cuenta, entre otros.

El servidor es dedicado exclusivamente a la conexión de la aplicación con la base de datos. Para poder añadir más servicios de red que mejoren la calidad y seguridad dentro de los procesos internos de la empresa se requiere de otro servidor capaz de llevar un control efectivo y seguro de la red internet e intranet. En la Figura 14, se identifica las características del servidor actual instalado en la empresa.

Figura 14. Servidor actual licores Capri

La información del servidor puede ser manipulada por diferentes usuarios tanto locales como remotos, exponiéndolo a posibles ataques de red, el sistema operativo del servidor es vulnerable a ataques de virus y software malicioso, no se cuentan con algunas licencias de software originales, lo cual dificulta el trabajo de reinstalar el servidor, su software y las bases de datos.

Hay un uso limitado del software contable, y las bases de datos, aunque en algunas ocasiones han ocurrido retrasos en la conexión del servidor con las maquinas clientes en la generación de informes, presentando inconsistencias al momento de actualizar la información. Los fallos se han tratado de corregir sobre la marcha con base en las necesidades presentadas.

Para realizar respaldos de los archivos de la empresa, es necesario que una persona encargada, haga una copia de cada uno de los equipos, esta información se encuentra almacenada en el disco duro, por lo cual se deben utilizar varios CD y unidades de disco extraíbles para salvaguardar los datos.

Por otra parte, la cantidad de documentos que se imprimen es abundante, debido a que en los puestos de trabajo existen impresoras conectadas de manera local a los equipos mediante cable USB, para la entrega de facturas a los clientes, y también para los reportes de cuentas.

4.2 ANÁLISIS DE LOS SERVICIOS ADQUIRIDOS EN LA EMPRESA

La empresa cuenta con el servicio de internet, contratados por medio de dos empresas que lo proveen, Claro y Movistar Colombia, con una velocidad respectiva de 10Mbps y 5Mbps.

Actualmente se ha optado por la utilización de la arquitectura cliente-servidor. Esto, con el fin de establecer la conexión entre los equipos que se conectan al servidor tanto de manera local como remota.

4.3 DEFINICIÓN DE LOS REQUERIMIENTOS

Se requiere hacer copias de seguridad de los archivos generados por las bases de datos de las aplicaciones instaladas en la empresa, desde el servidor actual, a otro manejador, que permita la fácil gestión y recuperación de la información en caso de ser necesaria, además, cabe resaltar la necesidad de un respaldo periódico programado de toda la información contenida en el servidor principal.

Los servicios a implementar se harán con aplicaciones bajo licencias de software libre, dado que son una alternativa de bajo costo para la empresa, aprovechando

la calidad de los programas, la seguridad, y la permanente actualización y corrección de errores en el software.

4.4 ANÁLISIS DE HARDWARE Y SOFTWARE

Los equipos y dispositivos de la empresa tienen un uso aproximado de 3 años de funcionamiento, durante este tiempo han ocurrido cortes de energía, gran tráfico de datos y pérdida de información, por lo cual, el servidor se ha visto afectado, poniendo en riesgo la integridad de la información almacenada.

La mayoría de equipos clientes cuentan con tecnología de procesamiento Intel Core I 3 e Intel Core I 7, la memoria RAM de cada equipo es de 4 GB, y tienen una capacidad de almacenamiento de 900 GB, además de puertos de comunicación básicos.

Se requiere un espacio más amplio, para la adquisición e instalación de nuevos equipos, así como para la implementación del nuevo servidor.

La topología de la red de la primera sucursal ubicada en las cuadras es de tipo estrella, en la Figura 15, se muestra que los computadores clientes están conectados por medio de un switch de 8 puertos a otro switch que conecta al servidor y al modem de internet, y un punto de acceso para la conexión inalámbrica de dispositivos móviles.

La topología de red de tipo estrella de la segunda sucursal ubicada en el centro de la ciudad, cuenta como se muestra en la figura 16, con computadores clientes conectados a un anrutador, el cual también tiene conectado un modem con acceso a internet para la conectividad remota de los equipos clientes al servidor que se encuentra en la otra sucursal.

A continuación, se presenta las figuras 15 y 16, donde se muestra la topología de las dos sucursales.

Figura 15. Diseño actual red LAN Las Cuadras

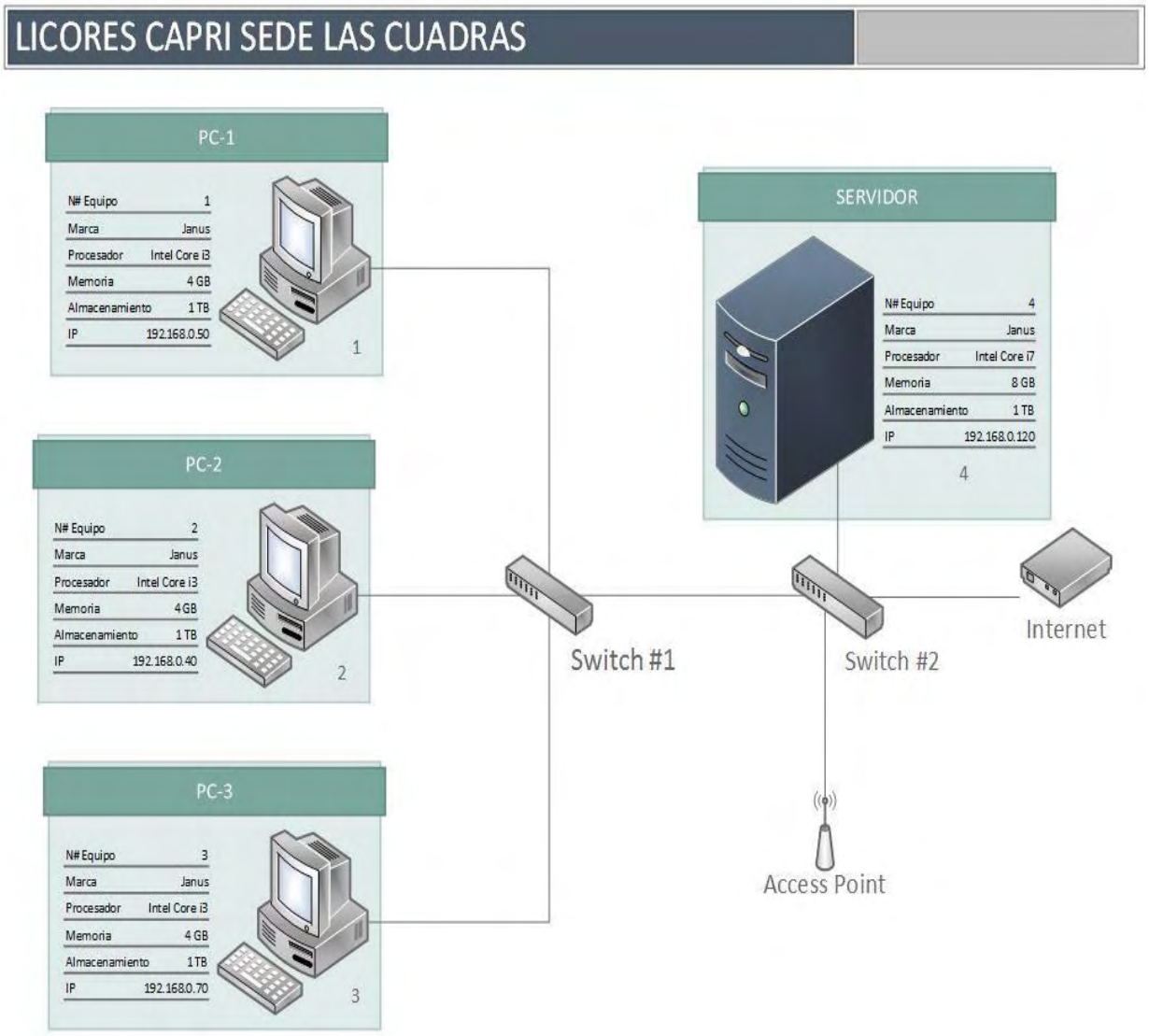
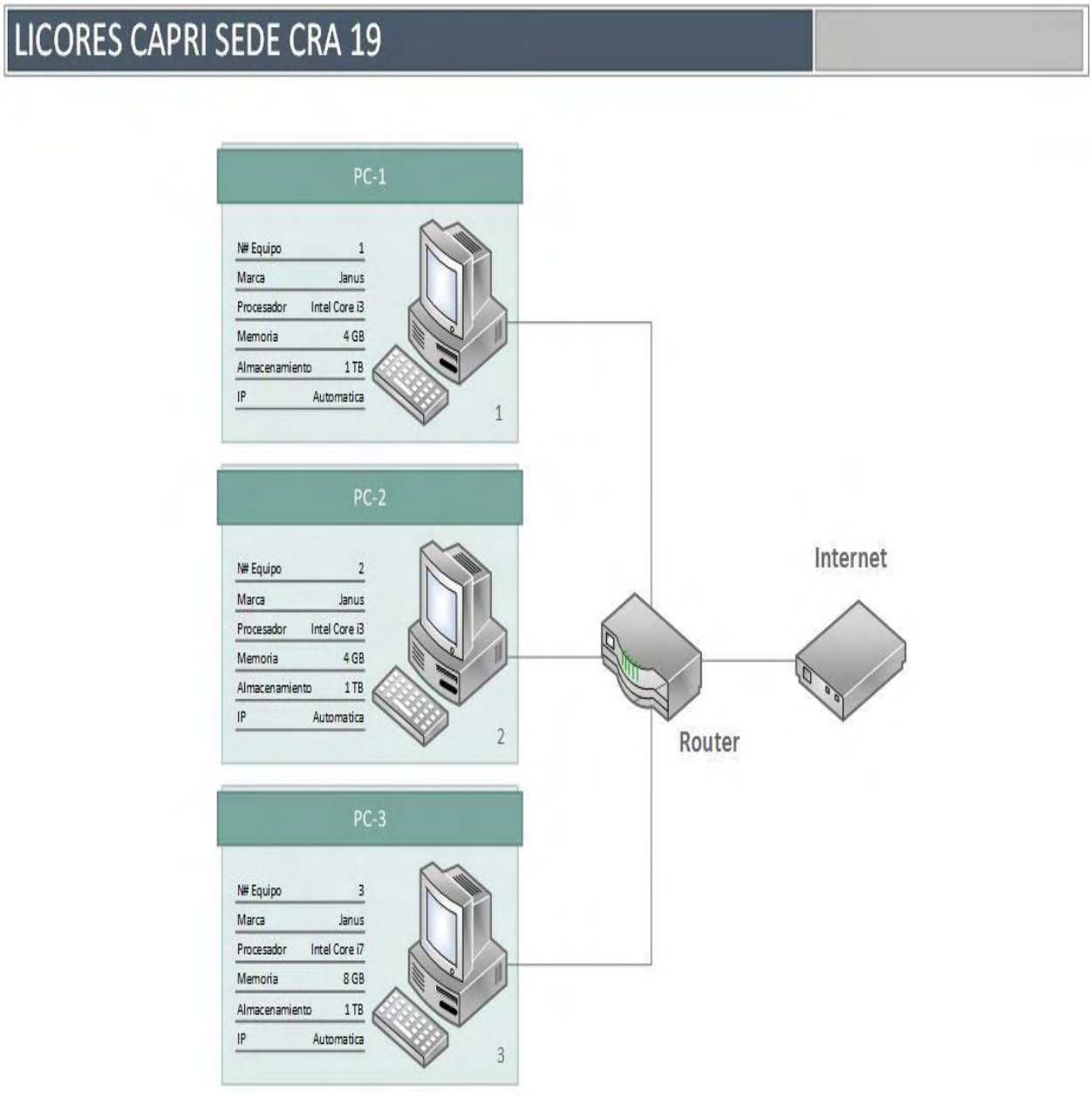


Figura 16. Diseño actual red LAN sede centro



A continuación, se especifica en la Tabla 4, las características de la red local de las sucursales de la empresa.

Tabla 4. Descripción detallada red LAN Licores Capri

ESPECIFICACIONES DE LAS REDES		
TAMAÑO	Small LAN	7 usuarios conectados
TIPO		Centralizada
TECNOLOGIA		Ethernet
TOPOLOGIA		Estrella
PROTOCOLO		TCP/IP IPv4
DISPOSITIVOS DE RED	**MARCA**	**VELOCIDAD**
Switch #1 8 puertos. Tipo RJ45	TP-LINK	10/100 Mbps
Switch #2 8 puertos. Tipo RJ45	TP-LINK	10/100 Mbps
Punto de acceso	TP-LINK	Inalámbrico
Enrutador	TP-LINK	
SERVICIO		
INTERNET DSL (CLARO)	10 Mbps	Cable
INTERNET DSL (MOVISTAR)	5 Mbps	Cable
SERVIDOR		
Windows 7 Ultímate		Grupo de trabajo

4.5 ANÁLISIS DE SOFTWARE

En la empresa se utiliza un programa especializado en la gestión administrativa y contable de compañías productoras y/o comercializadoras de bienes o servicios públicos o privados llamado Manager el cual maneja la versión 6.1.M29. También se utiliza software de ofimática básica, programa para visualización de archivos de formato PDF, navegadores de internet como Google Chrome, Firefox, e Internet Explorer, Teamviewer para asistencia remota, Avast Software Antivirus para la protección de software malicioso y el sistema operativo Windows 7 ultímate en su versión de 32 y 64 bits.

4.6 MATRIZ DOFA SITUACIÓN ACTUAL RED LICORES CAPRI

Con el fin de establecer estrategias y soluciones a los problemas encontrados en la fase de diagnóstico inicial se realiza una matriz DOFA, la cual evalúa los aspectos internos y externos que ayuden o perjudiquen al buen funcionamiento de la empresa. Como lo indican sus siglas, esta matriz debe contener las debilidades (D) las cuales se refieren a los aspectos internos que de alguna manera interfieren o detienen el crecimiento de la empresa y el cumplimiento de sus objetivos,

oportunidades (O) en las cuales se evalúa las características o acontecimientos externos que pueden contribuir al desarrollo de la empresa, fortalezas (F) las cuales indican las características internas que tiene la empresa para el cumplimiento de objetivos y metas, por ultimo las amenazas (A) en las cuales se evalúan los acontecimientos o factores externos, que pueden poner en riesgo el funcionamiento normal de la empresa.

A continuación, se presenta la Tabla 5 donde se evalúan las debilidades, oportunidades, amenazas y fortalezas que se encontraron una vez hecho el diagnóstico de la red de la empresa Licores Capri.

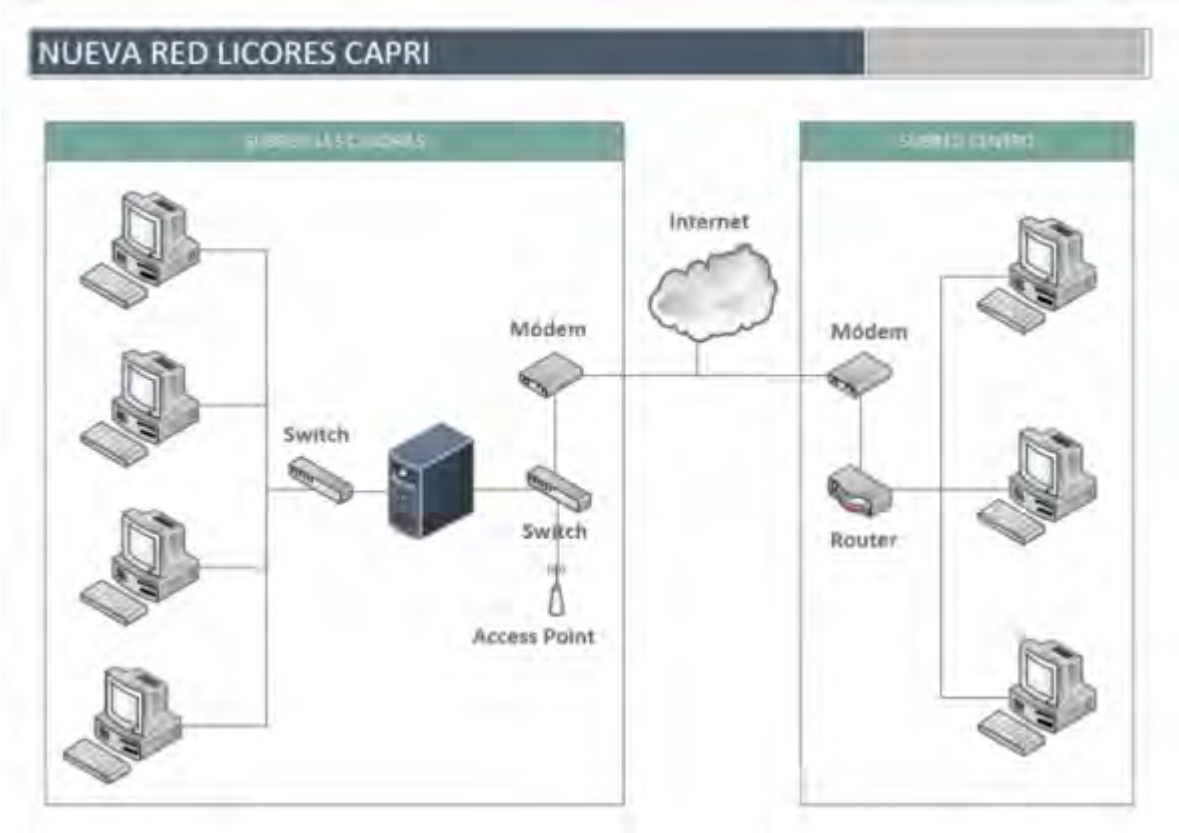
Tabla 5. Matriz DOFA red empresa Licores Capri

Matriz DOFA	**FORTALEZAS** ▪ La empresa cuenta con una infraestructura tecnológica la cual se conecta a internet. ▪ Buen conocimiento del personal acerca de las aplicaciones instaladas en los equipos de la red. ▪ Personal que vigila constantemente los equipos en la red. ▪ Buena velocidad de conexión de internet. ▪ Las redes locales de la empresa cuentan con cableado nuevo.	**DEBILIDADES** ▪ Redes locales con poca seguridad. ▪ Uso indebido del internet. ▪ Algunas aplicaciones sin licencias. ▪ No existe una revisión programada para la administración de red. ▪ Bajo presupuesto para la compra de nuevos equipos. ▪ Tiempos de respuesta altos en la atención de nuevos requerimientos. ▪ Ausencia de nuevas herramientas de red. ▪ Deficiencias en las aplicaciones de administración, contabilidad y facturación.
OPORTUNIDADES ▪ Creación de políticas de seguridad eficientes. ▪ Mejora de la comunicación de las redes. ▪ Red escalable. ▪ Disponibilidad de servidores para la administración redes. ▪ Nuevos servicios de red. ▪ Desarrollo de autogestión. ▪ Desarrollo de alianzas.	**ESTRATEGIAS (FO)** ▪ Crear una red virtual privada para la conexión de las redes de las sucursales de la empresa. ▪ Permitir el acceso remoto al servidor para la administración de los servicios de red. ▪ Transferencia remota de archivos de manera segura. ▪ Implementar nuevo canales de comunicación para los usuarios locales y remotos de la red.	**ESTRATEGIAS (DO)** ▪ Creación de un nombre de dominio para la identificación de los equipos de la red interna e internet. ▪ Organización de los equipos conectados a la red de la empresa. ▪ Configurar un servicio donde se alojen distintas aplicaciones del proceso de negocio de la empresa. ▪ Implementar servicios de alojamiento y administración de páginas web.
AMENAZAS ▪ Robo de información. ▪ Ciberataques ▪ Daños en los equipos de la red. ▪ Robos de equipos. ▪ Mal uso de la red.	**ESTRATEGIAS (FA)** ▪ Monitorización permanente de los equipos conectados a la red ▪ Transferencia segura de archivos entre los equipos de la red de la empresa.	**ESTRATEGIAS (DA)** ▪ Controlar el acceso a internet a los equipos de la red. ▪ Creación de reglas seguridad para él envió, recepción y traspaso de paquetes de datos a través de la red interna e internet.

4.7 ESQUEMA GENERAL DE LA NUEVA RED DE LA EMPRESA

A continuación, se muestra el esquema general de la red de la empresa Licores Capri una vez se haya implementado el servidor. Como lo muestra la Figura 17 se realiza la conexión de las dos subredes a través de internet utilizando una red virtual privada, permitiendo a los equipos de la subred Centro acceder a los servicios de red de la subred Las Cuadras.

Figura 17. Esquema general nueva red Licores Capri



4.8 DESARROLLO DE LA CONFIGURACIÓN E INSTALACIÓN DEL SERVIDOR

A continuación se explica detalladamente los pasos que se ejecutaron para la instalación y configuración del servidor en la empresa, se debe tener en cuenta que el desarrollo de este capítulo sirve como manual principal para los usuarios encargados de administrar el servidor, donde queda consignado todos los procedimientos realizados, así como todas las recomendaciones, posibles fallas y mantenimientos del equipo, cabe resaltar que este documento sirve como una

referencia bibliográfica, para la implementación de servidores LINUX, en este caso se lo desarrolla bajo la distribución Ubuntu server en su versión 14.04.5 LTS, la cual puede ser adaptada según las necesidades pertinentes.

La distribución del sistema operativo a instalar, soporta la mayoría de arquitecturas de procesamiento conocidas como Intel, AMD y ARM. En la Tabla 6, se muestra los requerimientos de hardware mínimos, así como los recomendados para la instalación básica del sistema operativo Linux Ubuntu server en su versión de 64 bits.

Tabla 6. Requerimientos para instalación del sistema operativo Ubuntu server

TIPO DE INSTALACIÓN	CPU	RAM	ESPACIO EN DISCO SISTEMA BASE	ESPACIO EN DISCO CON TODOS LOS PROGRAMAS INCORPORADOS
Estándar	1 giga Hertz	512	1 gigabyte	1.75 gigabytes
Mínima	300 mega Hertz	192	700 megabytes	1.4 gigabytes

Fuente: Guía Ubuntu server

El proceso de instalación y configuración especifica en la empresa contempla los siguientes servicios descritos en la siguiente Tabla 7.

Tabla 7. Descripción servicios

DESCRIPCIÓN SERVICIOS INSTALADOS EN EL SERVIDOR		
NOMBRE DE SERVICIO	**APLICACIÓN**	**DESCRIPCIÓN**
DNS	BIND9	Se configura los nombres de dominio de la empresa.
DHCP	ISC-DHCPD	Se crea una subred para la asignación automática de direcciones IP de los equipos clientes de la red.
WEB	APACHE	Se configura el sitio web principal de la empresa y una página de administración con autenticación.
SSH	SSH SERVER	Se configura el acceso remoto de usuarios normales del servidor y el usuario con privilegios de administración.
FTP	VSFTPD	Se configura el acceso remoto del administrador de la red a este servicio.

Continuación Tabla 7…

NOMBRE DE SERVICIO	APLICACIÓN	DESCRIPCIÓN
SERVIDOR DE ARCHIVOS	SAMBA	Se crean varias carpetas para el acceso de los equipos clientes de la empresa y del administrador.
CHAT	OPENFIRE	Se crean los usuarios que se deben utilizar y se instalan en las maquinas clientes para su funcionamiento.
STREAMING	MEETINGS	Se configuran la sala por donde se realizan la video llamadas.
PROXY	SQUID	Se crean políticas de acceso a internet a los equipos clientes de la red.
MONITOREO DE RED	NAGIOS	Se configuran los servicios que se requieren monitorear de todas las estaciones de trabajo de la red.
VPN	OPENVPN	Se configura una red virtual privada entre las sucursales añadiendo a la subred local los equipos remotos de la otra sucursal.
APLICACIONES	TOMCAT	Se instala el servicio y se comprueba su funcionamiento.
FIREWALL	IPTABLES	Se configuran las políticas para el acceso solo a los puertos web, ssh y vpn.

Fuente: Guía Ubuntu server

4.9 INSTALACIÓN SISTEMA OPERATIVO UBUNTU SERVER 14.04.5 LTS (Lon Term Support[11])

Se resalta que esta edición del sistema operativo usa un menú de consola basado en las instancias de procesos de instalación, y está disponible su imagen de forma gratuita en la página web oficial de Linux Ubuntu en las versiones de instalación para procesadores de 32 y 64 bits. Para la implementación del servidor se descarga la versión de 64 bits, el enlace directo de descarga es el siguiente. **http://releases.ubuntu.com/trusty/ubuntu-14.04.5-server-amd64.iso**

Una vez descargada la imagen ISO se debe guardarla en un dispositivo de arranque como un CD o en una memoria USB, con el fin de iniciar el sistema desde alguno de estos dos medios, generalmente el equipo detecta automáticamente dispositivos tipo boot (medio de arranque) una vez se reinicia el sistema, en el caso de no arrancar se entra a la configuración del BIOS del equipo para cambiar el orden de inicio de las unidades de arranque.

[11] Soporte a largo plazo

Al momento de iniciar el medio utilizado comienza el proceso de instalación del sistema operativo donde en primera instancia se elige el idioma de preferencia de instalación como se muestra en la Figura 18, en este caso se elige español.

Figura 18. Elección del idioma durante el proceso de instalación

Después, se despliega un menú principal de arranque donde se aprecia opciones de instalar Ubuntu Server, instalación de varios servidores, comprobación de defectos en el disco duro, comprobación de memoria del equipo, arrancar desde un primer disco duro y recuperar un sistema dañado, en este caso se elige la primera opción como se aprecia en la Figura 19.

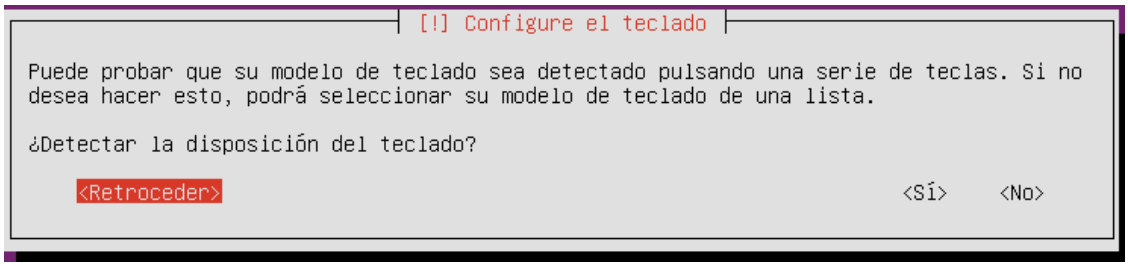
Figura 19 .Página principal de instalación de Ubuntu server.

A continuación, el proceso de instalación despliega una lista de países con el fin de definir la ubicación actual del servidor, determinando su zona horaria, en este caso se elige el País Colombia, como se muestra en la Figura 20.

Figura 20. Selección de ubicación geográfica del servidor

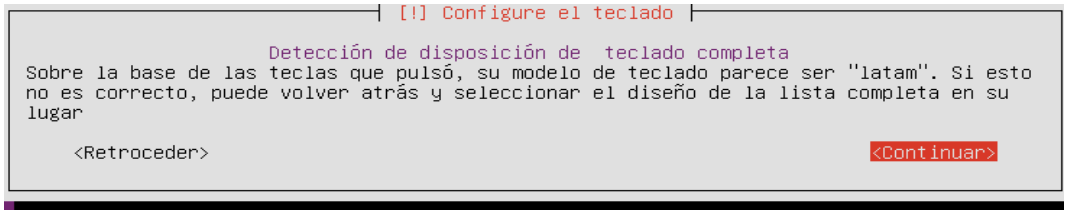
El proceso de instalación procede a configurar el teclado identificando el modelo, se puede elegir la opción auto detectar, o se puede escoger manualmente desde una lista, en este caso se elige la primera opción como se muestra en la Figura 21 .

Figura 21. Configuración del teclado



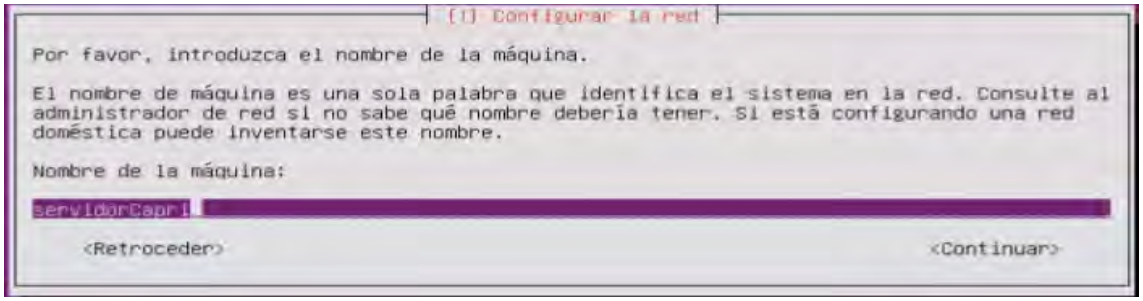
Después de haber elegido la opción si, se deben presionar las teclas tal como lo especifica el proceso de instalación, así como una serie de signos para la correcta detección. Una vez realizado este proceso aparece un mensaje de confirmación sugiriendo un modelo de teclado de acuerdo a las teclas pulsadas, como se aprecia en la Figura 22.

Figura 22. Confirmación configuración del teclado



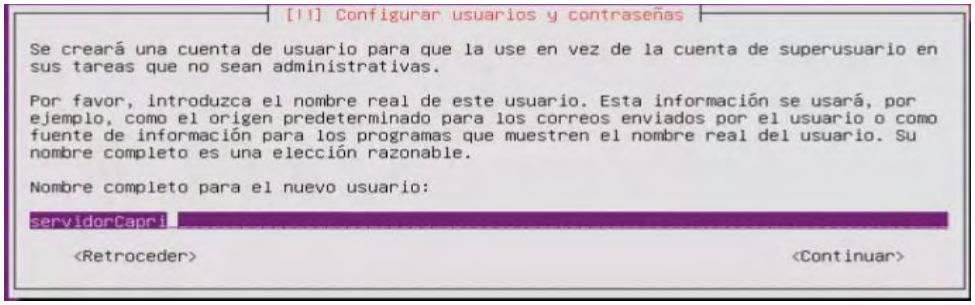
Se recomienda que el servidor esté conectado a internet mediante un cable UTP a la tarjeta de red ethernet del equipo, con el fin de que el instalador detecte y configure automáticamente el hardware, y los ajustes de red conectándose mediante el servicio automático DHCP. Posterior a esta instancia el instalador pregunta por el nombre de la máquina, en este caso se lo identificara como servidorCapri, como se muestra en la Figura 23.

Figura 23. Configuración del nombre de la máquina



Después, según se señala en la Figura 24, se despliega un recuadro que pide que se coloque el nombre completo del usuario dueño del servidor, en este caso se coloca servidorCapri.

Figura 24. Configuración de nuevo usuario



Una vez realizado el anterior paso, el sistema pide un nombre de usuario para la cuenta creada, se coloca en este caso administrador y se coloca la contraseña igual que el nombre de usuario para efectos prácticos del tutorial como se ve en la Figura 25 y la Figura 26, en un contexto real se recomienda utilizar una contraseña segura.

Figura 25. Configuración nombre de usuario para nueva cuenta

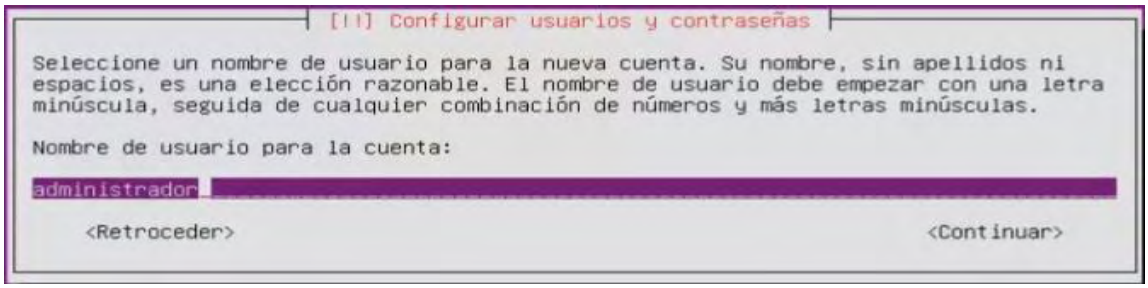
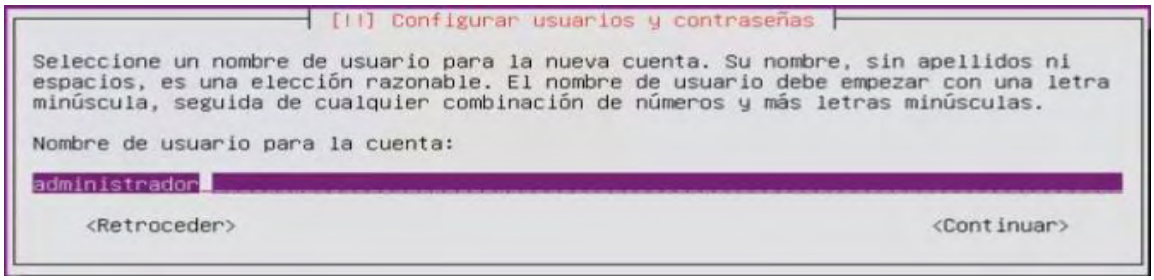
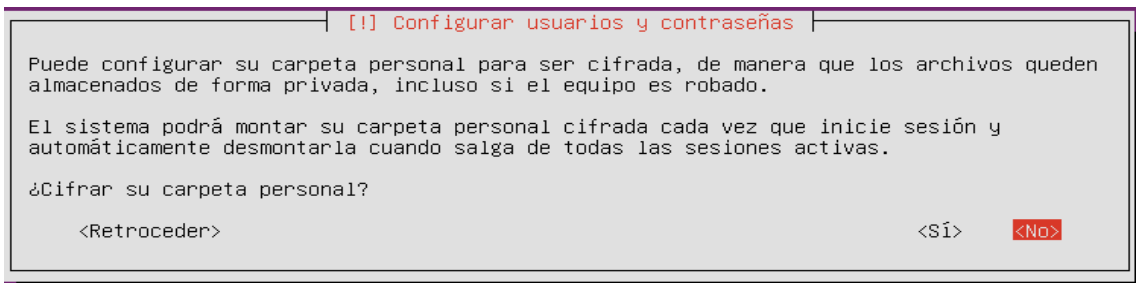


Figura 26. Configuración contraseña de usuario para nueva cuenta



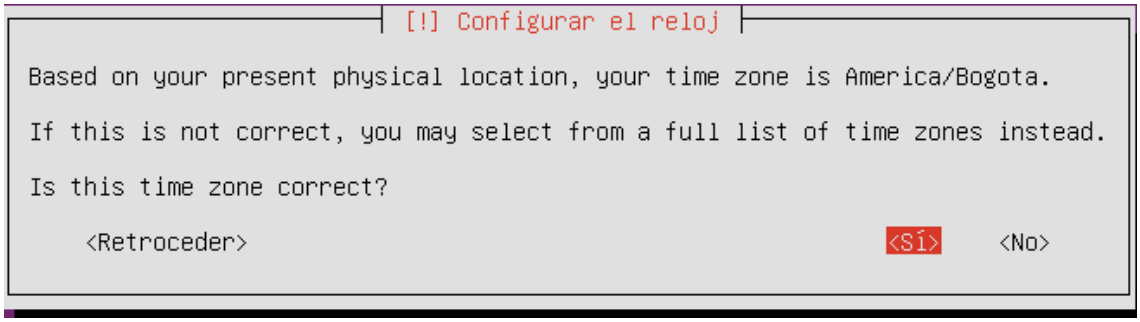
El proceso de instalación muestra la opción de cifrar la carpeta personal del usuario por cuestiones de seguridad, se le da la opción no cifrar, como se ve en la Figura 27.

Figura 27. Cifrar la carpeta personal del usuario



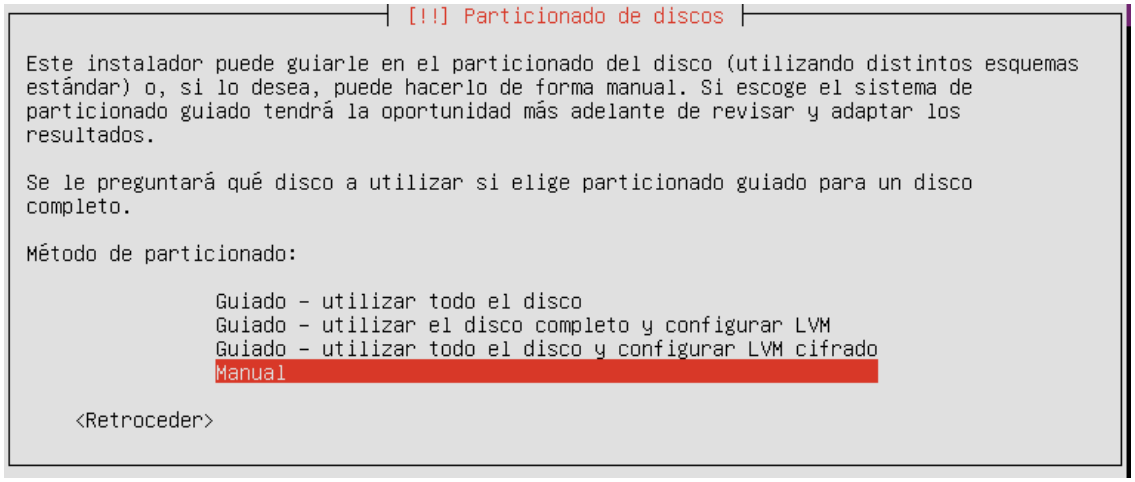
Para la configuración del reloj del sistema, se escoge la zona horaria bajo la locación física que se configura anteriormente, también se puede escoger de una lista, pero se configura de acuerdo con la locación por defecto, como muestra la Figura 28.

Figura 28. Configuración del reloj



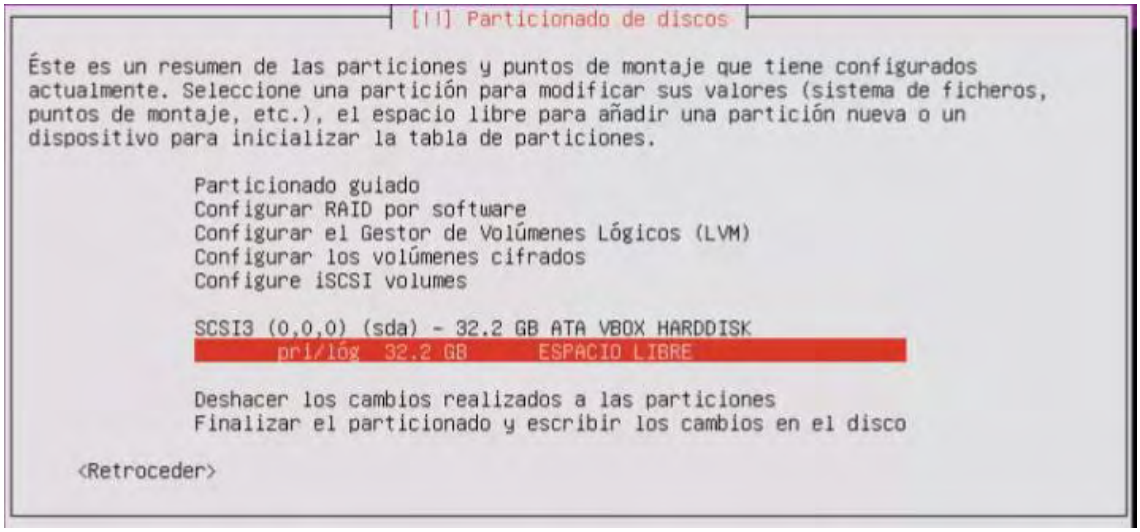
Posteriormente, el proceso de instalación pregunta la forma en la que se desea particionar los discos duros que el servidor contenga, este proceso se puede realizar tanto de forma automática, como manual el cual es la manera más recomendada, como se muestra en la Figura 29.

Figura 29. Particionado de discos



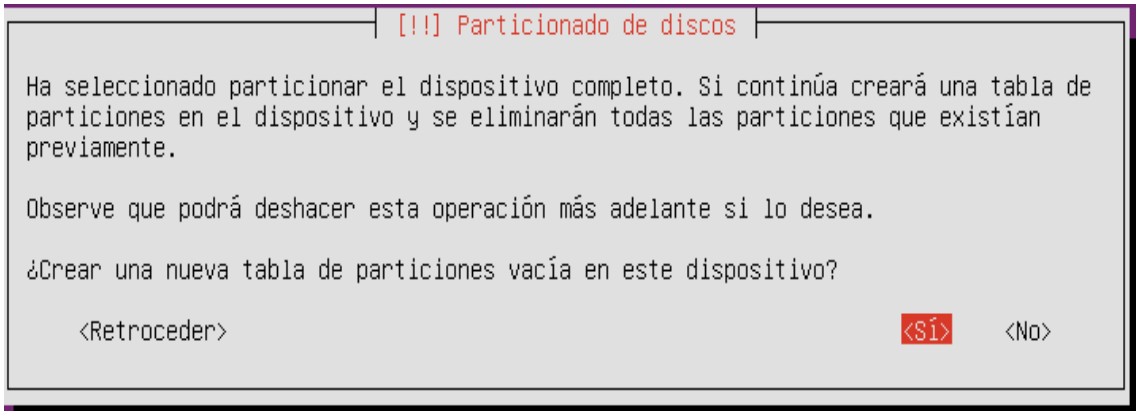
El sistema detecta automáticamente los discos duros físicos del servidor, como se muestra en la Figura 30, en este caso se tiene un disco de tamaño de 32 gigabytes.

Figura 30. Identificación de discos duros



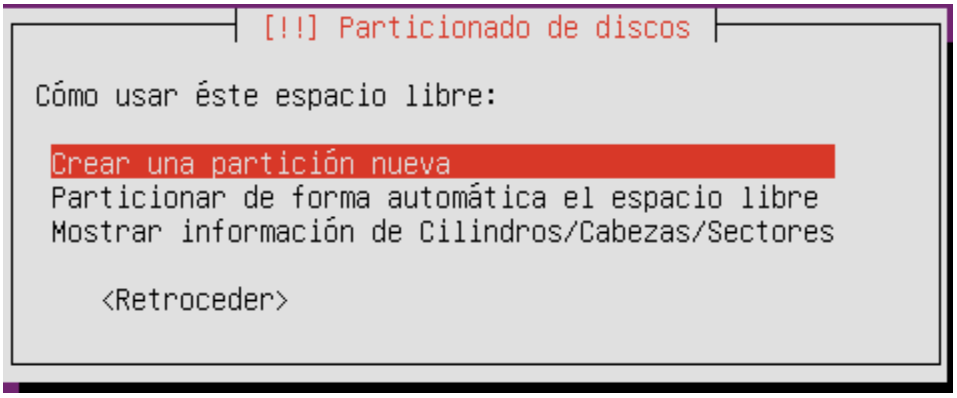
Una vez seleccionado el dispositivo se crean nuevas tablas de particiones eliminando previas, apareciendo un cuadro confirmando si se desea proceder a crear la nueva tabla, se escoge si como se ve en la Figura 31.

Figura 31. Crear tabla de particiones



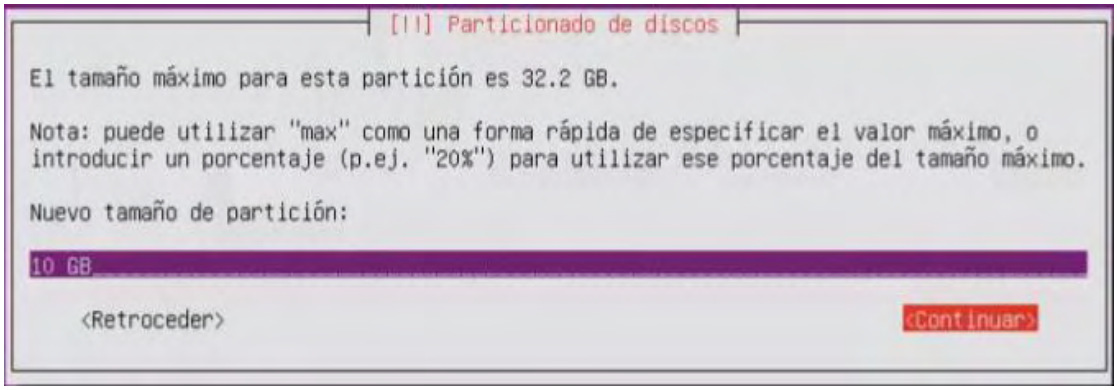
Posteriormente en la opción que pregunta cómo usar el espacio libre, se escoge crear una partición nueva como se ve en la Figura 32.

Figura 32. Creación de partición nueva



En la primera partición se crea el directorio root o raíz, donde se copian los archivos necesarios para el funcionamiento del sistema operativo, y el tamaño de cada una de las particiones depende del tamaño del disco duro, haciendo un cálculo proporcional de acuerdo con los datos digitados en este tutorial, el cual tiene un disco duro de 32 gigabytes, en este caso se añadirá, como se aprecia en la Figura 33, un tamaño de 10 gigabytes.

Figura 33. Tamaño de partición de partición raíz.



El tipo de la partición creada es primaria como se ve en la Figura 34, y su ubicación es al principio del espacio disponible, referenciado en la Figura 35.

Figura 34. Tipo de nueva partición primaria

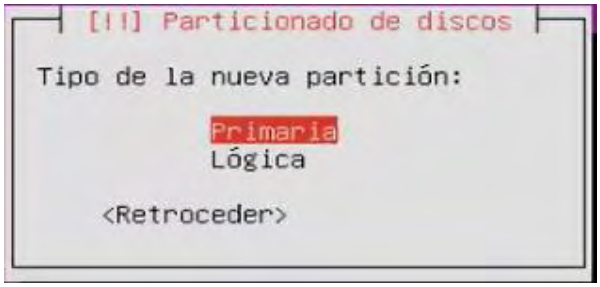
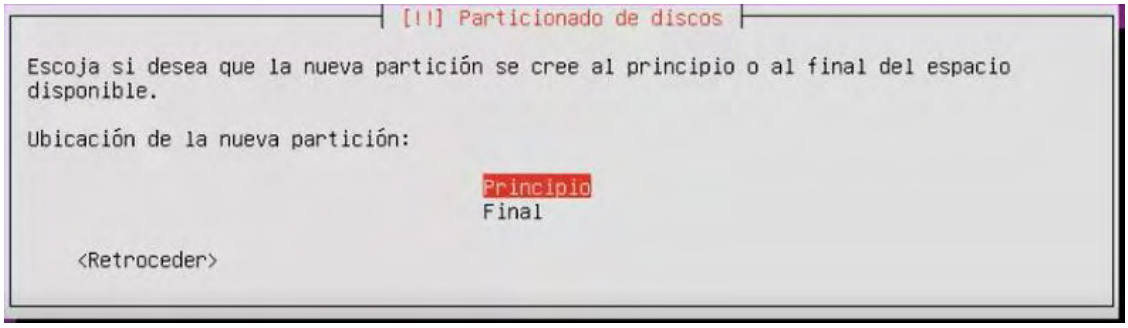
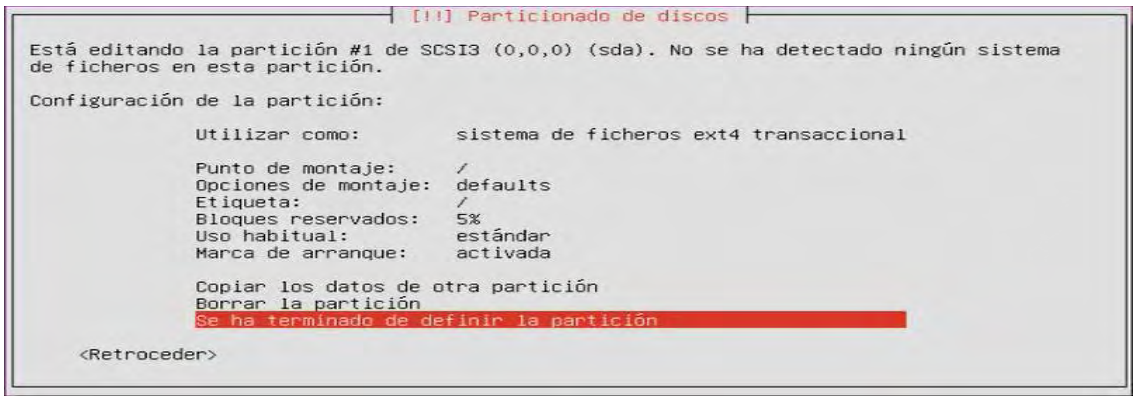


Figura 35. Ubicación de la nueva partición principio



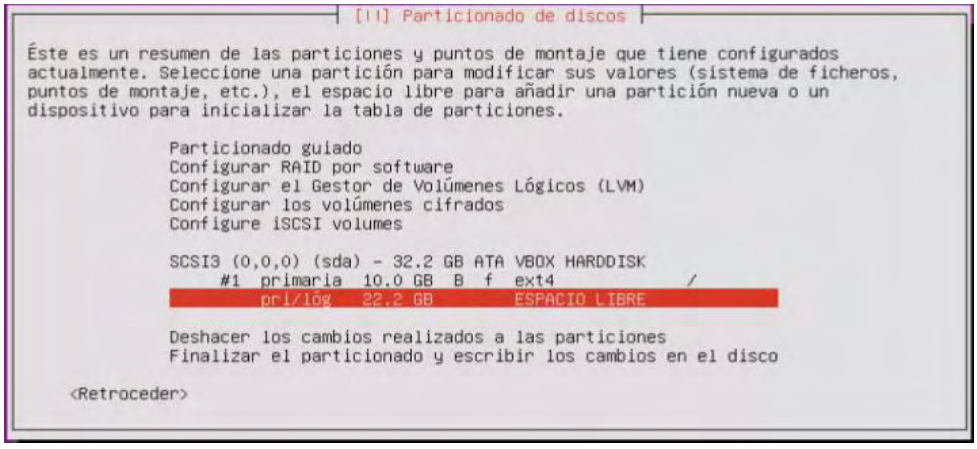
El proceso de instalación muestra la configuración de la partición mostrado en la Figura 36, donde se pueden editar varias características, el punto de montaje es raíz (/) y la etiqueta de identificación igualmente se escribe (/), la marca de arranque debe estar activada, una vez realizados estos pasos se escoge la opción de terminar de definir la partición.

Figura 36. Configuración de la partición raíz



Realizada la anterior configuración se visualiza la partición creada y el espacio libre restante, como se ve en la Figura 37.

Figura 37. Resumen de la partición configurada la partición raíz



En el espacio libre restante se deben hacer las particiones para la carpeta personal del usuario, para la cache, y para el área de intercambio la cual debe tener al menos una capacidad doble de la memoria RAM del servidor, los otros tamaños de las particiones se hacen de acuerdo al tamaño del disco duro del servidor, en este caso se configuran el tamaño de las particiones como se muestran en la Figura 40, Figura 43 y Figura 46, el tipo de partición será lógica como se ve en la Figura 38, y se colocan al final de la partición como describe la Figura 39. En la Figura 41 y la Figura 44 se describe la configuración de las particiones a crear editando las etiquetas y el punto de montaje, en la Figura 45 y la Figura 49, se especifica un resumen de las particiones creadas una vez finalizadas las particiones y escritos los cambios en el disco.

Figura 38. Tipo de nuevas particiones lógicas

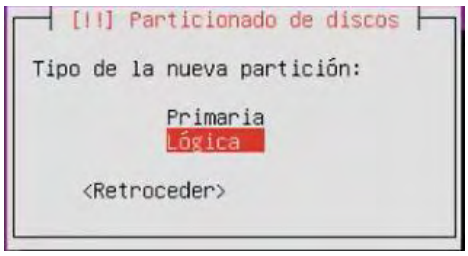


Figura 39. Ubicación de nuevas particiones al final

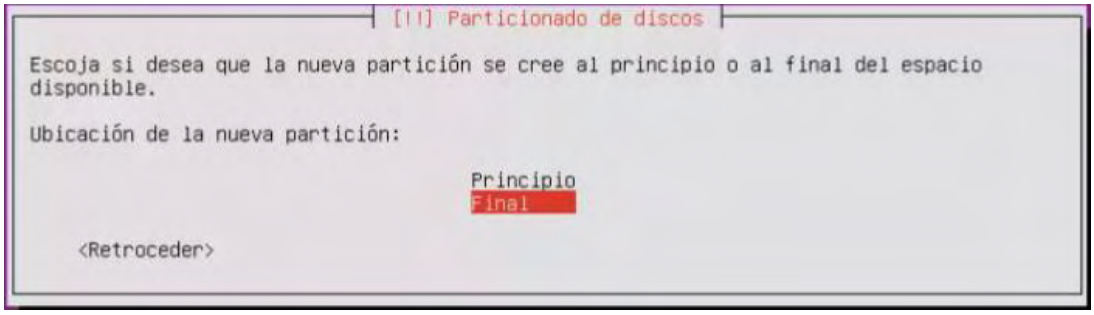


Figura 40. Tamaño de partición directorio de usuario home

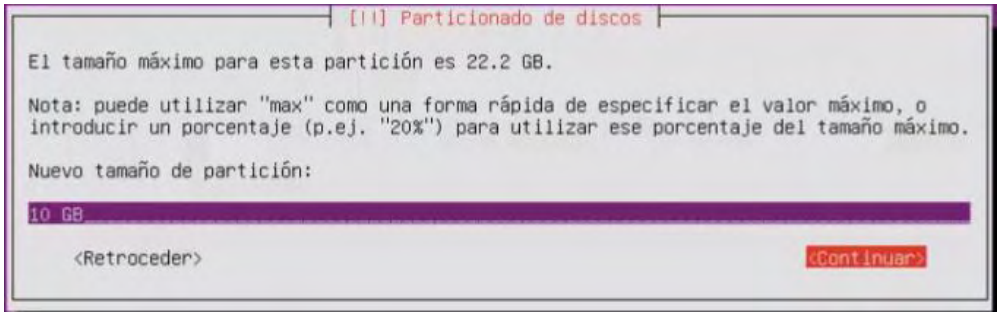


Figura 41. Configuración de partición del directorio de usuario home

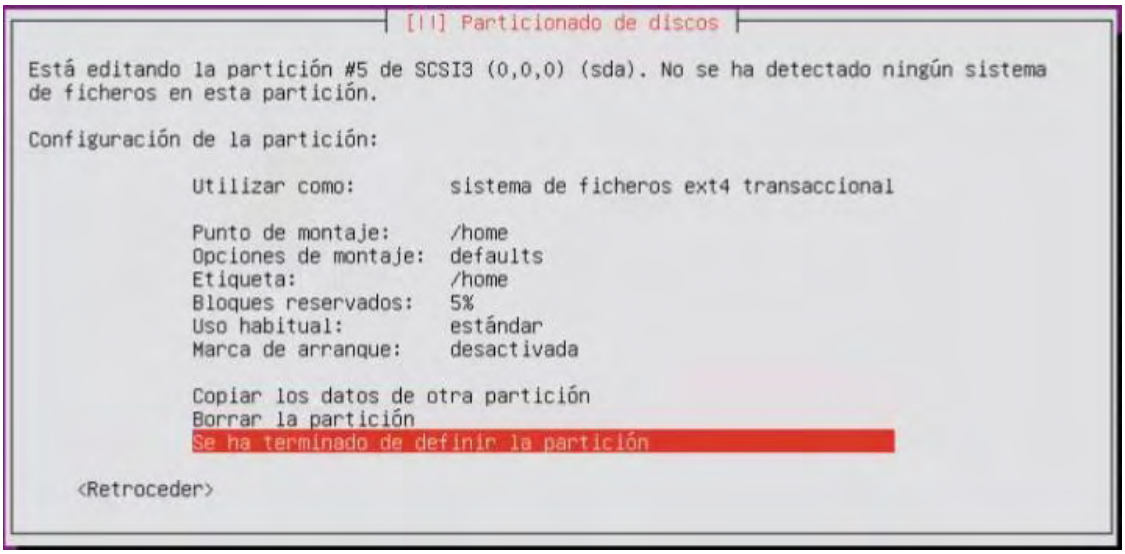


Figura 42. Resumen de partición configurado el directorio de usuario

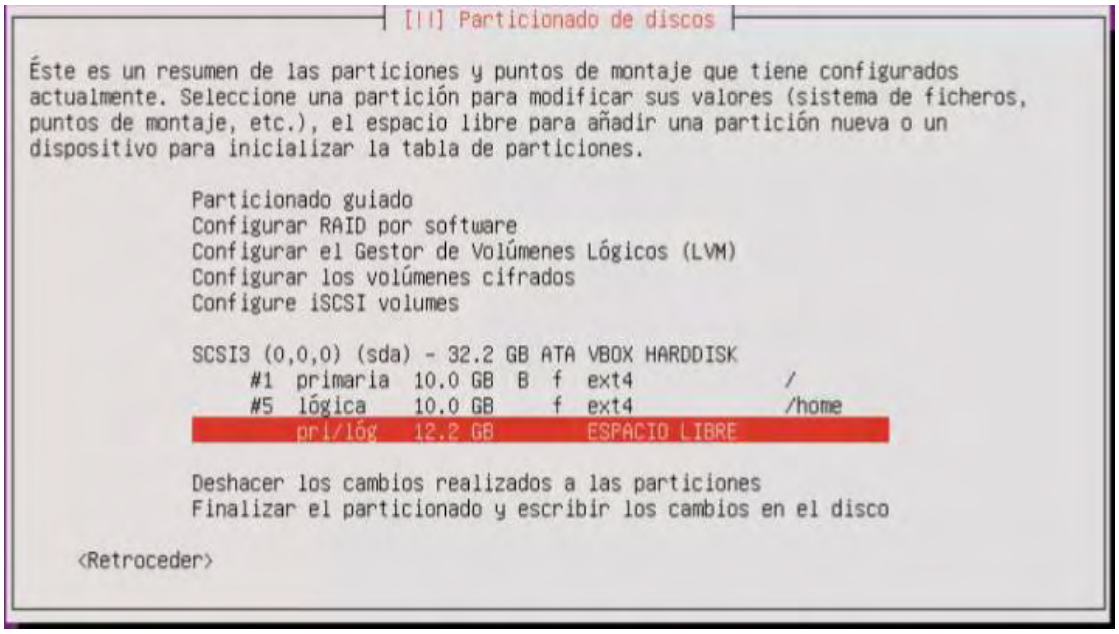


Figura 43. Tamaño de partición memoria cache

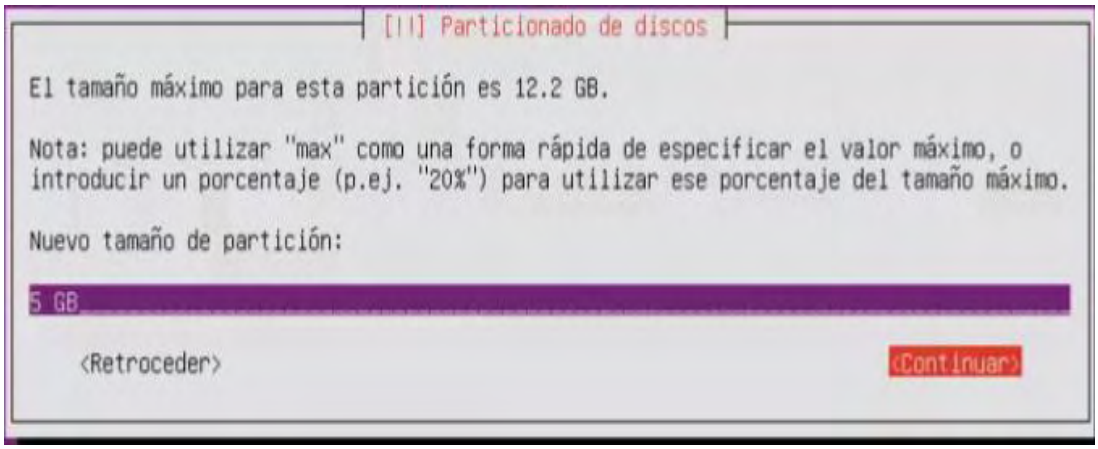


Figura 44. Configuración de la partición memoria cache

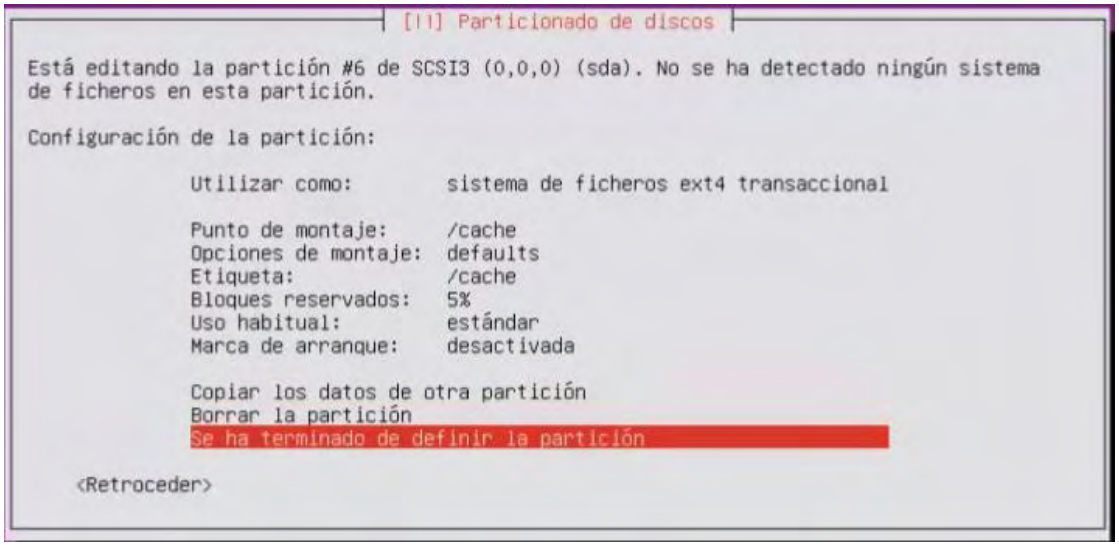


Figura 45. Resumen de la partición configurada partición de cache

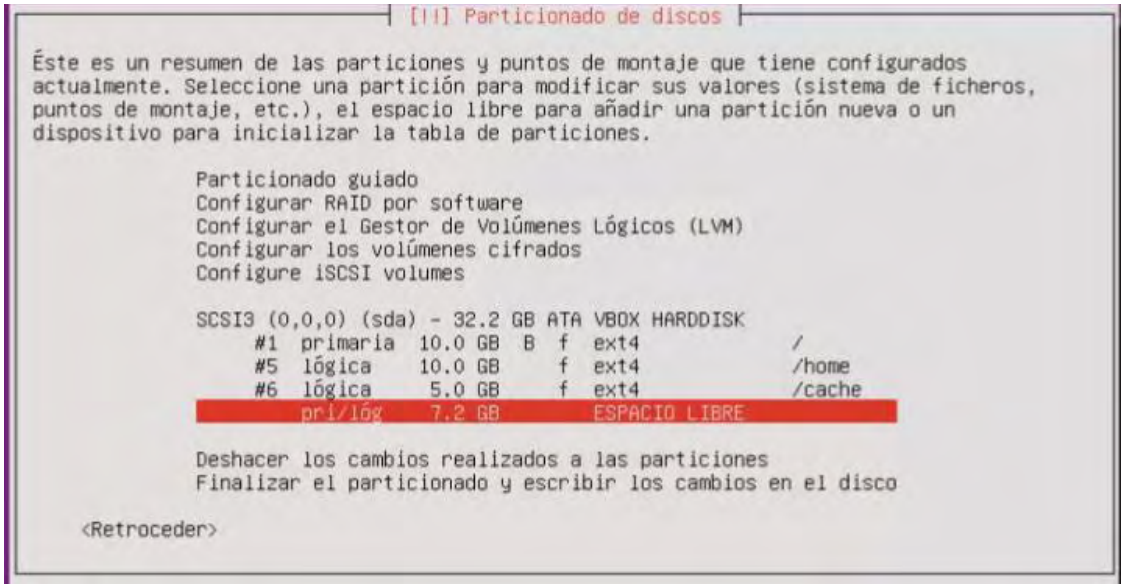
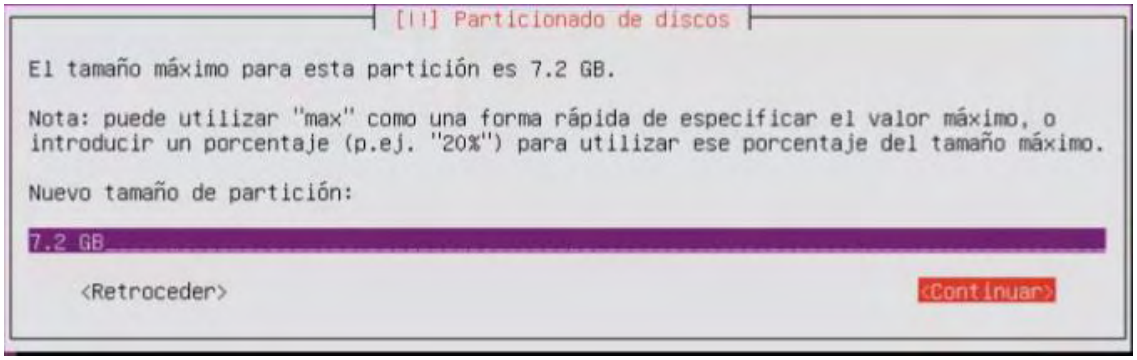
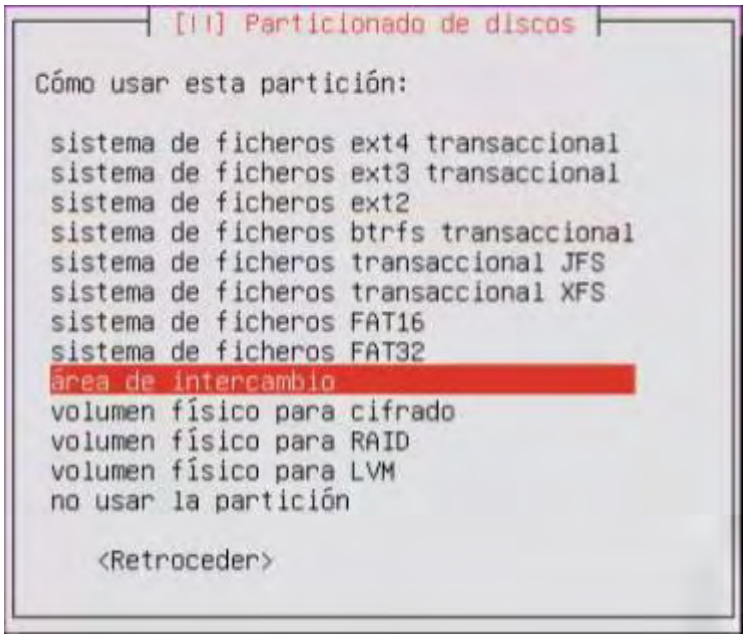


Figura 46. Tamaño de partición para el área de intercambio



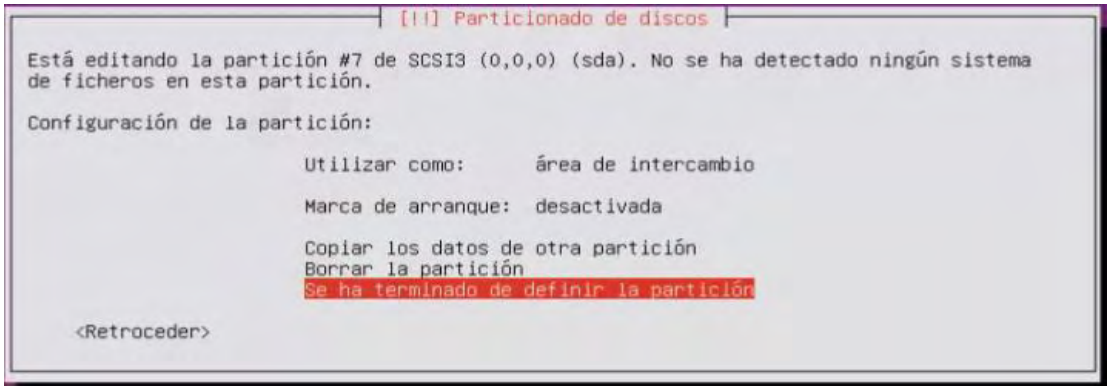
Para la configuración de la partición se debe especificar en su uso, como área de intercambio igual como se aprecia en la Figura 47.

Figura 47. Configuración uso de la partición del área de intercambio



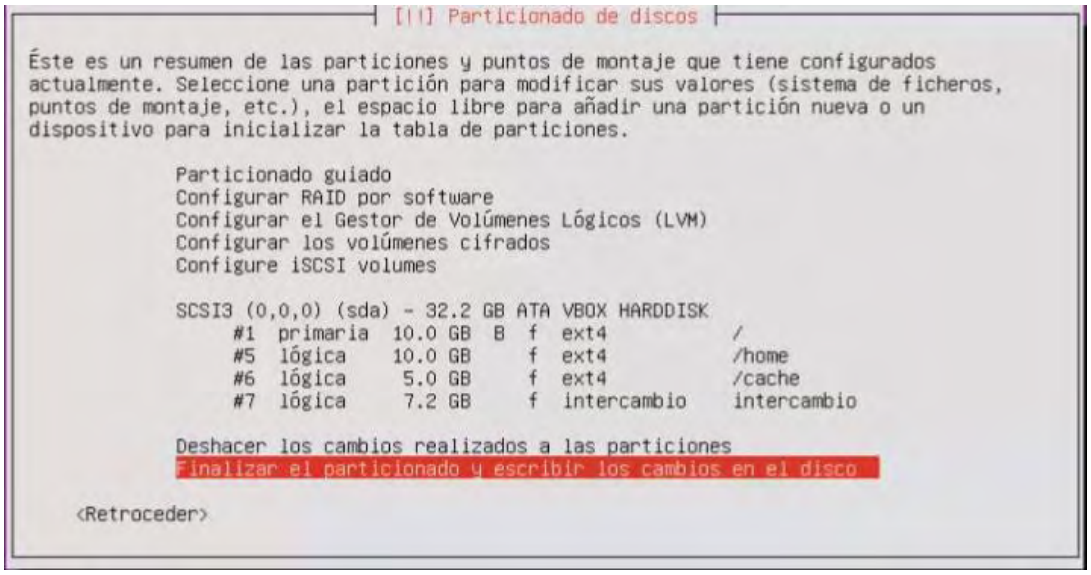
Una vez realizada esta configuración la partición del área de intercambio se debe ver igual a la Figura 48.

Figura 48. Particionado del disco de área de intercambio



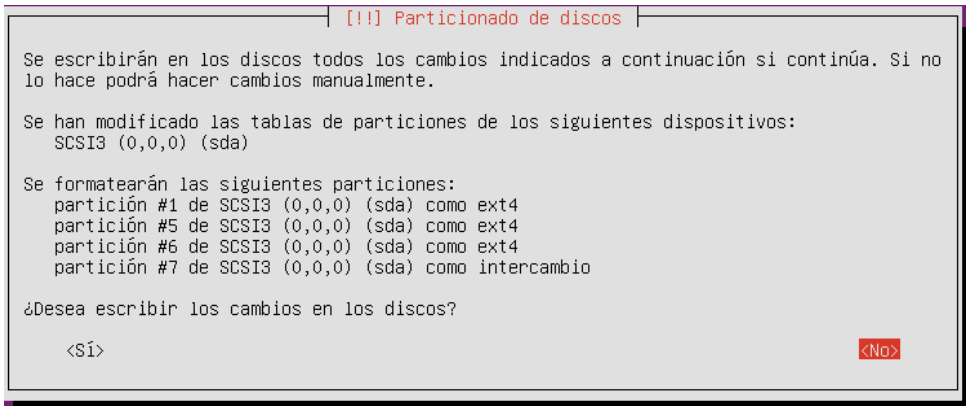
Una vez terminada de definir la partición de área de intercambio se visualizan el resumen de todas las particiones configuradas anteriormente con sus respectivas características. Como se identifica en la Figura 49, se escoge la opción de finalizar el particionado escribiendo los cambios en el disco.

Figura 49. Resumen de la partición configurado el área de intercambio



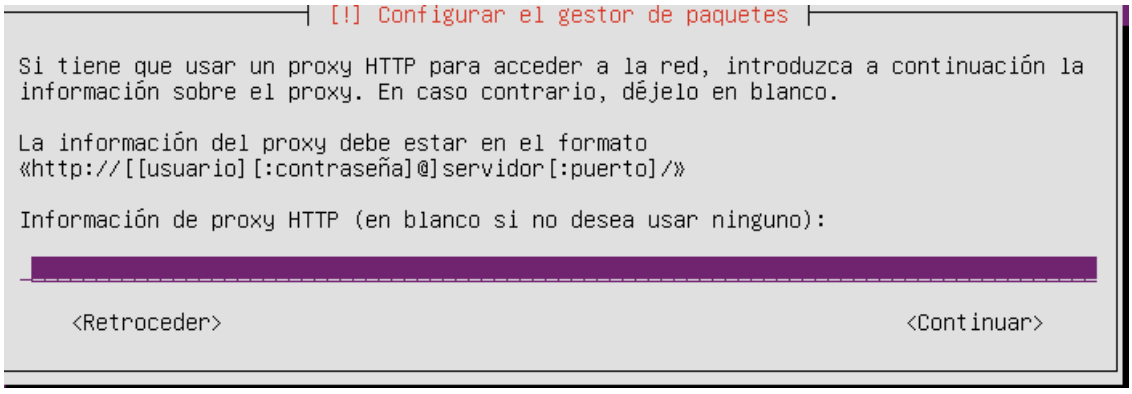
A continuación, se despliega un cuadro de confirmación donde se describen las particiones a formatear en el disco duro del servidor, con su tipo de formato, confirmando la decisión, según se identifica en la Figura 50.

Figura 50. Confirmación de escritura de los cambios en el disco



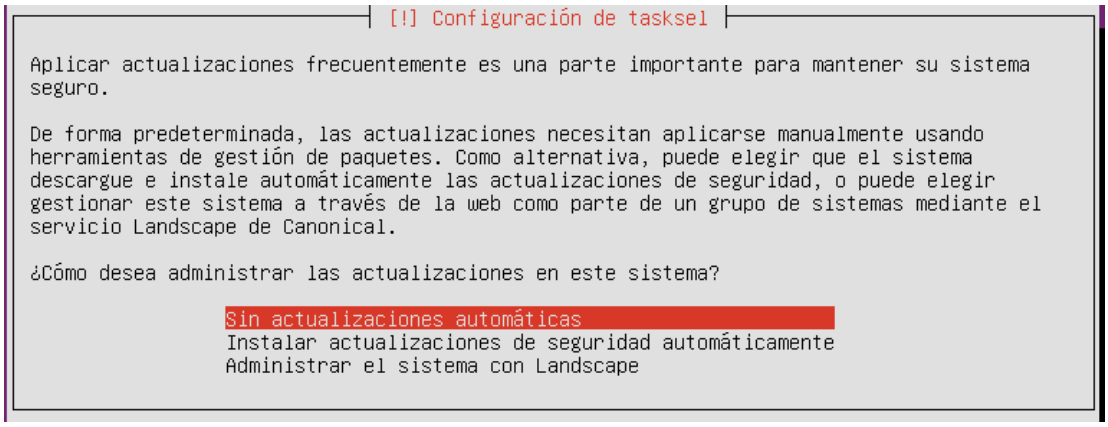
Después el sistema procede a instalar el sistema operativo, configurando las utilidades por defecto, el sistema pregunta si se requiere configurar un gestor de paquetes, configurando una dirección proxy para el acceso a la red, en este caso se lo deja en blanco y se escoge la opción continuar, como se aprecia en la Figura 51.

Figura 51. Configuración de gestor de paquetes



Otra configuración que el sistema pregunta si se desea añadir es la de instalar actualizaciones de forma automática o con la aplicación Landscape, en el caso de la instalación actual del servidor, se debe actualizar por parte del administrador del sistema de forma manual, de tal manera que se escoge como se aprecia en la Figura 52, la opción sin actualizaciones automáticas.

Figura 52. Configuración de actualizaciones automáticas



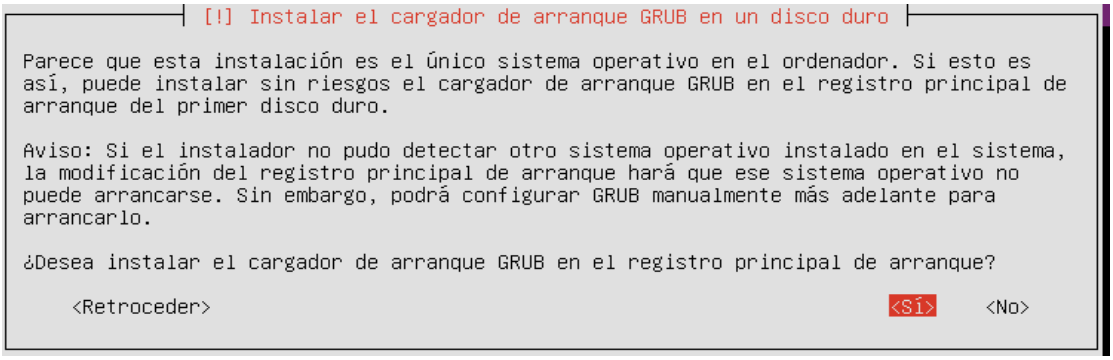
La instalación da a escoger una colección de programas que se incluyen en el instalador para adaptarlo de forma automática según las necesidades de los usuarios, para este caso no se eligen ninguno de los programas disponibles, como se aprecia en la Figura 53, ya que posteriormente se instalan solo los requeridos y se explica de forma detallada su configuración.

Figura 53. Selección de programas por defecto

El instalador configura algunas utilidades necesarias para el funcionamiento básico del sistema, como el gestor de arranque GRUB, el cual es recomendado configurar, como registro principal de arranque, así, que como se ve en la Figura

54, se selecciona la opción si a la pregunta si desea instalar el cargador de arranque.

Figura 54. Instalación del cargador de arranque GRUB en el disco duro

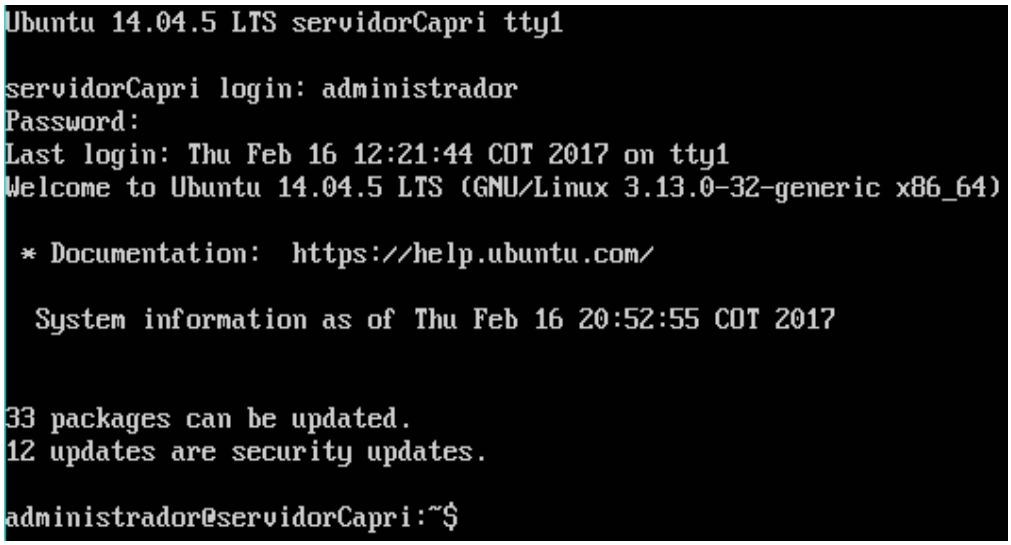


Finalmente aparece un cuadro confirmando el termino de instalación especificando que ya se puede extraer la unidad de arranque de instalación del sistema instalado, descrito en la Figura 55.

Figura 55. Finalización de la instalación

Una vez realizados todos los pasos anteriores, como se aprecia en la Figura 56, el sistema carga la interfaz de autenticación de usuarios del sistema operativo, donde pide un nombre de usuario y su respectiva contraseña.

Figura 56. Interfaz principal autenticación de usuario Ubuntu server.



4.10 CONFIGURACIÓN INTERFACES DE RED

Para la configuración de la dirección IP pública del servidor se debe configurar la interfaz de red en el archivo interfaces del servidor como se muestra en la Figura 57 .

Figura 57. Edición de archivo interfaces

En este archivo se debe verificar que las interfaces de red estén debidamente identificadas, en la interfaz de red eth0, se debe configurar la dirección IP pública, la máscara de subred y el gateway (puerta de enlace), que son asignados por el proveedor de internet de la empresa, en este caso particular a manera de ejemplo se trabajará con la dirección 192.168.0.149, la máscara de subred 255.255.255.0, y el Gateway 192.168.0.1, como se muestra en la Figura 58.

Figura 58. Contenido del archivo interfaces

Se guarda los cambios en el archivo, y se procede a deshabilitar y luego habilitar la interfaz para que las modificaciones surtan efecto como se identifica en la Figura 59 y la Figura 60.

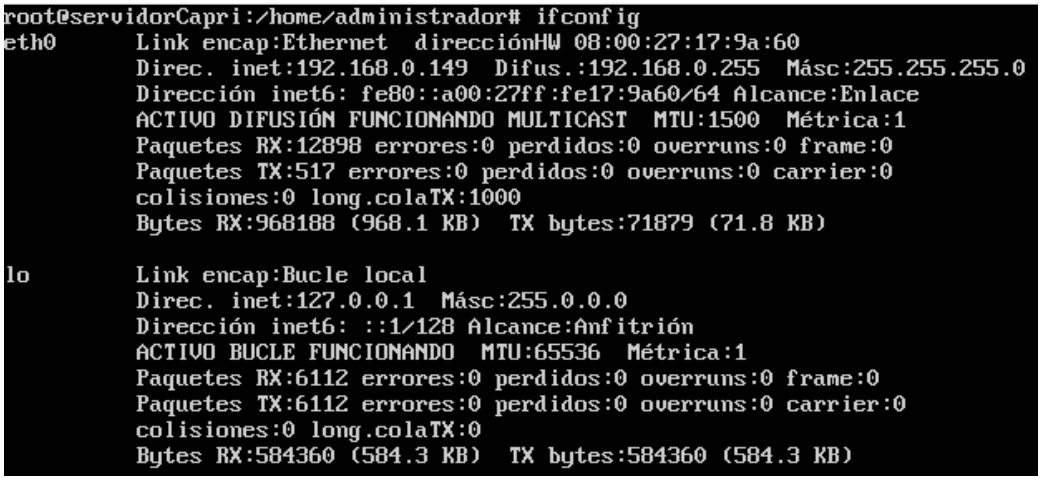
Figura 59. Deshabilitar interfaz de red eth0 para configuración interfaces de red.

Y para habilitar nuevamente.

Figura 60. Habilitar interfaz de red eth0, para configuración de interfaces

Para comprobar que la interfaz de red este configurada y se le haya asignado la IP correspondiente, se utiliza el comando ifconfig como se muestra en la Figura 61, para ver la descripción de las interfaces conectadas.

Figura 61. Descripción interfaces conectadas comando ifconfig

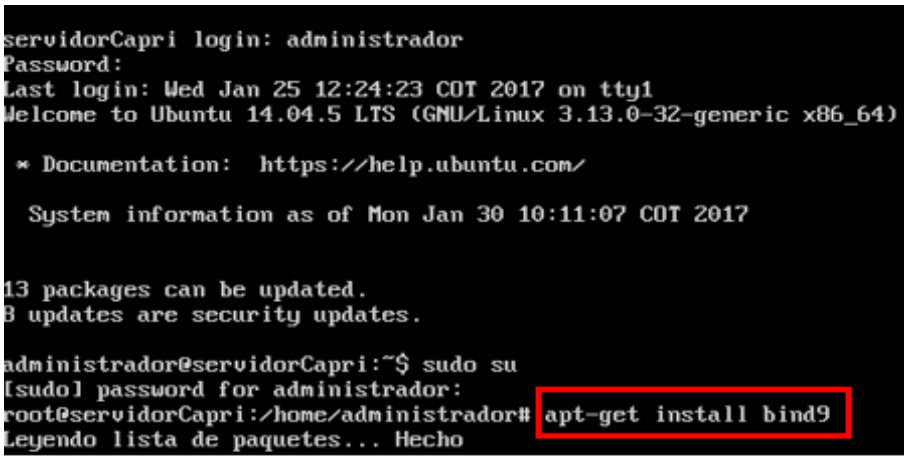


4.11 CONFIGURACIÓN DEL SERVICIO DNS

Para la instalación de un servidor DNS se debe descargar desde los repositorios oficiales del sistema operativo la aplicación BIND9, la cual permite configurar un servidor DNS para el servidor, que resuelva dominios internos y externos. El servidor DNS se encargará de resolver esos dominios con sus respectivas IP, además de resolver otros dominios de Internet como “www.google.com”.

Para la instalación del programa BIND9, se debe utilizar el comando apt-get como aparece en la Figura 62.

Figura 62. Instalación de bind9



Para la configuración de bind9, se debe modificar el archivo named.conf.local ubicado en la ruta /etc/bind, descrito en la Figura 63.

Figura 63. Edición del archivo named.conf.local

```
root@servidorCapri:/home/administrador# cd /etc/bind
root@servidorCapri:/etc/bind# nano named.conf.local
```

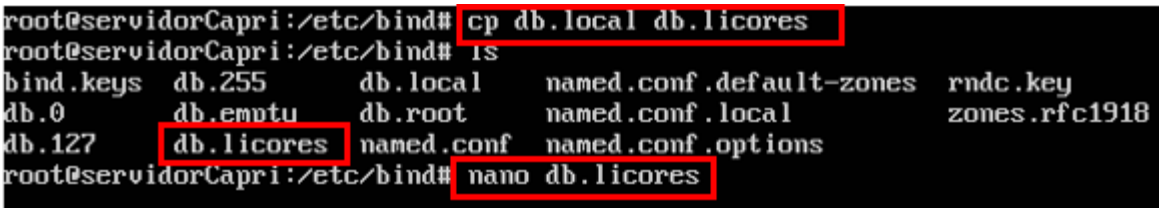
Se debe configurar la zona directa y la zona inversa del dominio licorescapri.com, para esto es recomendable ubicarse en la parte final del documento con el fin de mantener el orden del documento y añadir las líneas de zonas tipo de DNS Master y el archivo de ubicación de las zonas, como se describe en la Figura 64.

Figura 64. Configuración de zona directa DNS bind9

```
  GNU nano 2.2.6       Archivo: /etc/bind/named.conf.local          M

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

//Zona Directa
zone "licorescapri.com"{
type master;
file "/etc/bind/db.licores";
};

//Zona Inversa
zone "0.168.192.in-addr.arpa"{
        type master;
        file "/etc/bind/db.192.licores";
};
```

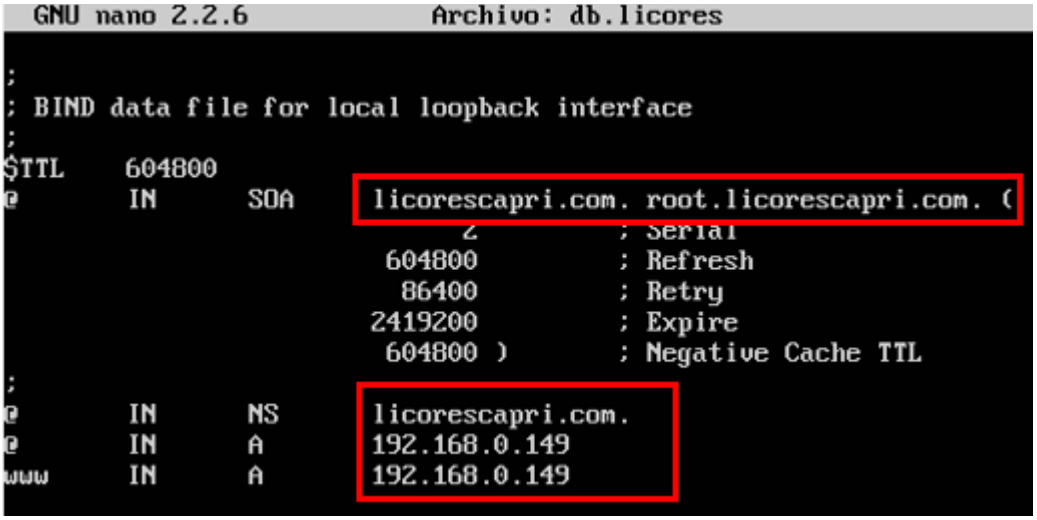
Ahora se crea la base de datos db.licores para la configuración de los registros de la zona directa del servicio DNS, realizando una copia del archivo db.local, y listando con el comando ls en la ruta /etc/bind/ para comprobar que el archivo fue creado, una vez realizado este paso procedemos a modificar el archivo db.licores, todos los pasos anteriores se describen en la Figura 65.

Figura 65. Creación de archivo db.licores



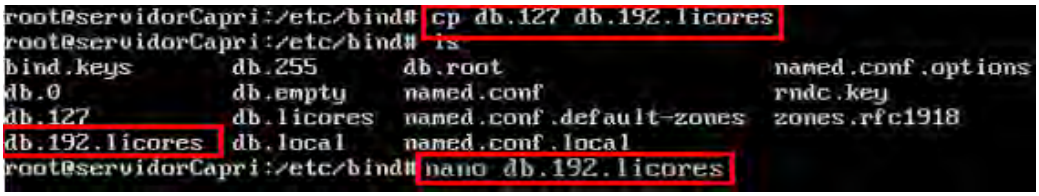
Una vez se empieza a editar el archivo, se debe cambiar el nombre del dominio de localhost al nombre de dominio que se va a utilizar, para este caso sería licorescapri.com. Además del cambio de nombre del dominio se debe agregar la dirección IP asociada a este dominio, como se muestra en la Figura 66.

Figura 66. Edición de archivo db.licores



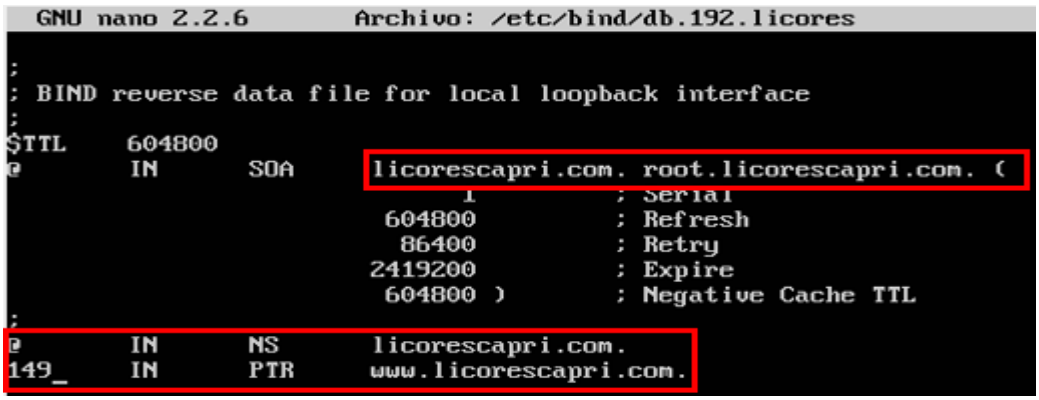
Posteriormente, se crea un archivo el cual va a ser la base de datos en donde se encuentran los diferentes registros de la zona inversa, este archivo se crea con el comando cp, a partir de una copia del archivo db.127, para verificar que el archivo es creado, con el comando ls, se lista todos los archivos dentro de la ruta /etc/bind/ y se edita con el editor nano, como se aprecia en la Figura 67.

Figura 67. Creación y edición del archivo db.192.licores zona inversa



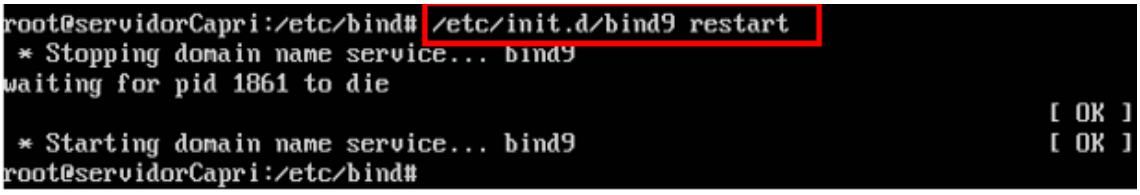
Una vez dentro del archivo, se cambia el nombre de dominio localhost por el nombre de dominio que se ha configurado en este caso licorescapri.com. Además se añade el registro PTR que es el registro de recurso (RR) de un dominio que define las direcciones IP de todos los sistemas en una notación invertida, como se mira en la Figura 68.

Figura 68. Edición de archivo db.192.licores para zona invertida



Al finalizar la configuración del anterior archivo, es necesario reiniciar el servicio de bind9, en la ruta /etc/init.d/ como se aprecia en la Figura 69.

Figura 69. Reinicio de servicio bind9 para zona directa e inversa DNS

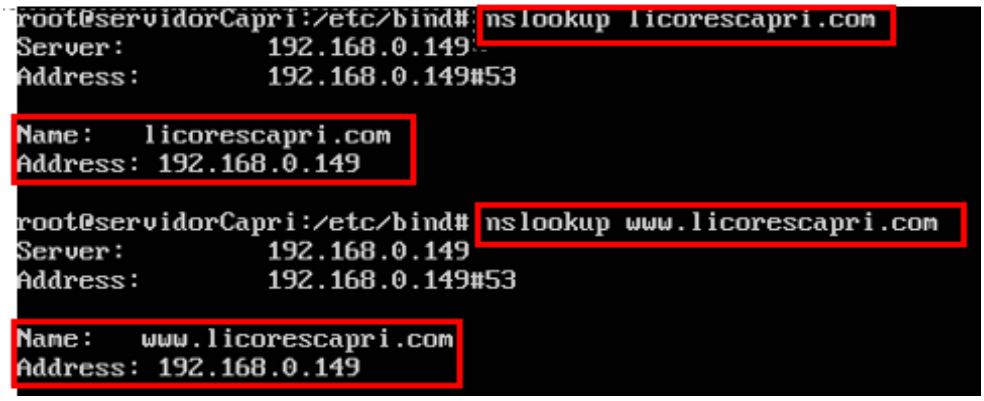


También se debe editar el archivo resolv.conf, ubicado en la ruta /etc/, en el cual se añade la dirección IP del servidor DNS configurado, añadiendo la línea nameserver como se aprecia en la Figura 70.

Figura 70. Edición de archivo resolv.conf

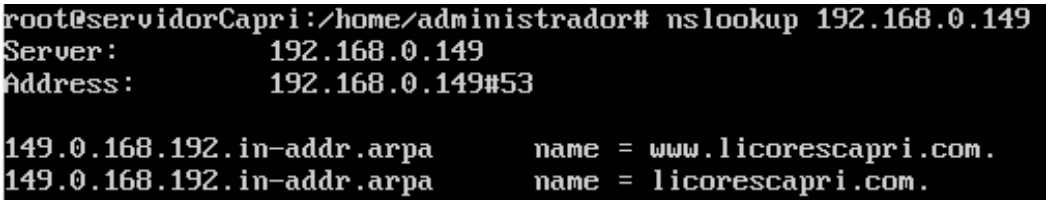
Para comprobar que dirección IP fue asignada al dominio licorescapri.com, se antepone el comando nslookup al nombre del dominio, para comprobar que la zona directa este bien configurada, como se ve en la Figura 71.

Figura 71. Verificación zona directa DNS comando nslookup



Para la comprobación de la zona inversa se debe utilizar el comando nslookup con la dirección IP configurada en los archivos de zonas, el sistema debe asociarla con el nombre de dominio, como se ve en la Figura 72.

Figura 72. Comprobación configuración zona inversa



4.12 CONFIGURACIÓN DE SERVICIO DE RED DHCP

A continuación, se muestra la creación de la subred Las cuadras para los computadores instalados en la red local utilizando la técnica de subnetting, las características de la subred se muestran en la Tabla 8, y son necesarias para la configuración del servicio DHCP.

Tabla 8. Tabla de subnetting subred Licores Capri

Nombre de red	Las cuadras
Número de equipos	14
Mascara	/28
Ip subred	192.168.1.0
Gateway	192.168.1.1
Host Inicial	192.168.1.2
Host final	192.168.1.14
Broadcast	192.168.1.15

Para la instalación del servicio DHCP se debe instalar la aplicación dhcp3-server, la cual se encuentra en los repositorios oficiales del sistema operativo ejecutando el comando apt-get install como se muestra en la Figura 73.

Figura 73. Instalación aplicación dhcp3-server

Para la configuración del servicio DHCP se debe añadir una nueva interfaz de red. Para añadir la interfaz se edita el archivo interfaces con el editor nano, que se encuentra en la ruta /etc/network/, como se aprecia en la Figura 74.

Figura 74. Edición del archivo interfaces para la configuración del DHCP

Se debe añadir al final del archivo, la interfaz de red eth1, configurando una dirección IP privada 192.168.1.1 y mascara de subred 255.255.255.240, creada para la subred de la empresa como se muestra en la Figura 75, esta red está

definida en la tabla de subnetting descrita en el inicio de la sección de configuración del servicio DHCP.

Figura 75. Creación de interfaz de red eth1.

```
#Interfaz para la subred las cuadras (tarjeta de red cableada)
auto eth1
iface eth1 inet static
        address 192.168.1.1
        netmask 255.255.255.240
```

Para que los cambios surtan efecto se debe habilitar la interfaz eth1 configurada en el paso anterior, con el comando ifup como se muestra en la Figura 76.

Figura 76. Habilitación de interfaz de red eth1

```
root@servidorCapri:/home/administrador# ifup eth1
```

Para comprobar los cambios efectuados se ejecuta el comando ifconfig el cual muestra las tarjetas de red conectadas con los nombres de las interfaces descritas en la Figura 77, las direcciones IP y las máscaras de subred que se les asigno en el archivo de configuración:

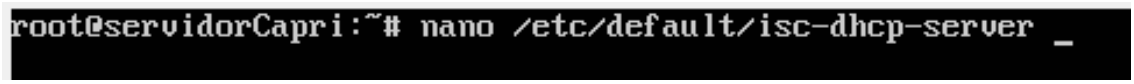
Figura 77. Comprobación configuración tarjeta de red eth1 comando ifconfig

```
root@servidorCapri:/home/administrador# ifconfig eth0
eth0      Link encap:Ethernet  direcciónHW 08:00:27:17:9a:60
          Direc. inet:192.168.0.149  Difus.:192.168.0.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe17:9a60/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:324 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:82 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:47225 (47.2 KB)  TX bytes:7140 (7.1 KB)

root@servidorCapri:/home/administrador# ifconfig eth1
eth1      Link encap:Ethernet  direcciónHW 08:00:27:27:c4:11
          Direc. inet:192.168.1.1  Difus.:192.168.1.7  Másc:255.255.255.248
          Dirección inet6: fe80::a00:27ff:fe27:c411/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:8 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:0 (0.0 B)  TX bytes:648 (648.0 B)
```

Ahora para configurar el servicio DHCP, se debe configurar las interfaces por las cuales se debe realizar el direccionamiento IP, para esto se debe modificar el

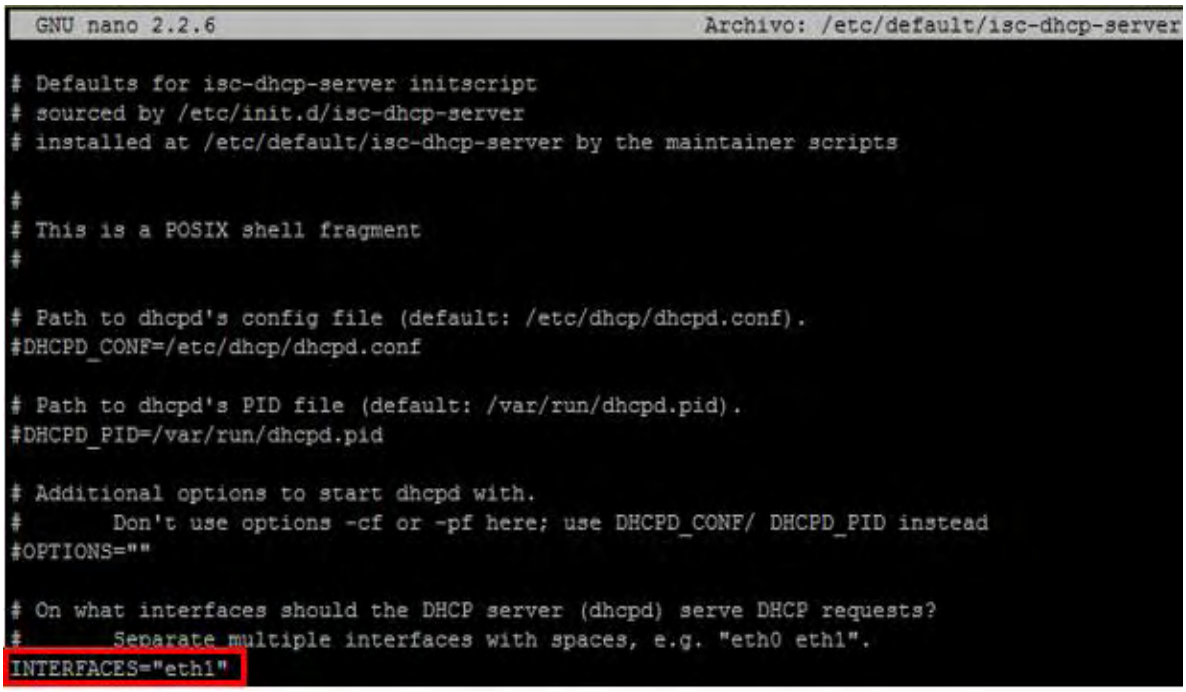
archivo de configuración isc-dhcp-server ubicado en la ruta /etc/default/, ejecutando el comando nano como se muestra en la Figura 78.

Figura 78. Edición archivo isc-dhcp-server



Dentro del archivo al final, se debe buscar y modificar la línea INTERFACES="" por INTERFACES="eth1", como se muestra en la Figura 79.

Figura 79. Modificación línea interfaces archivo isc-dhcp-server

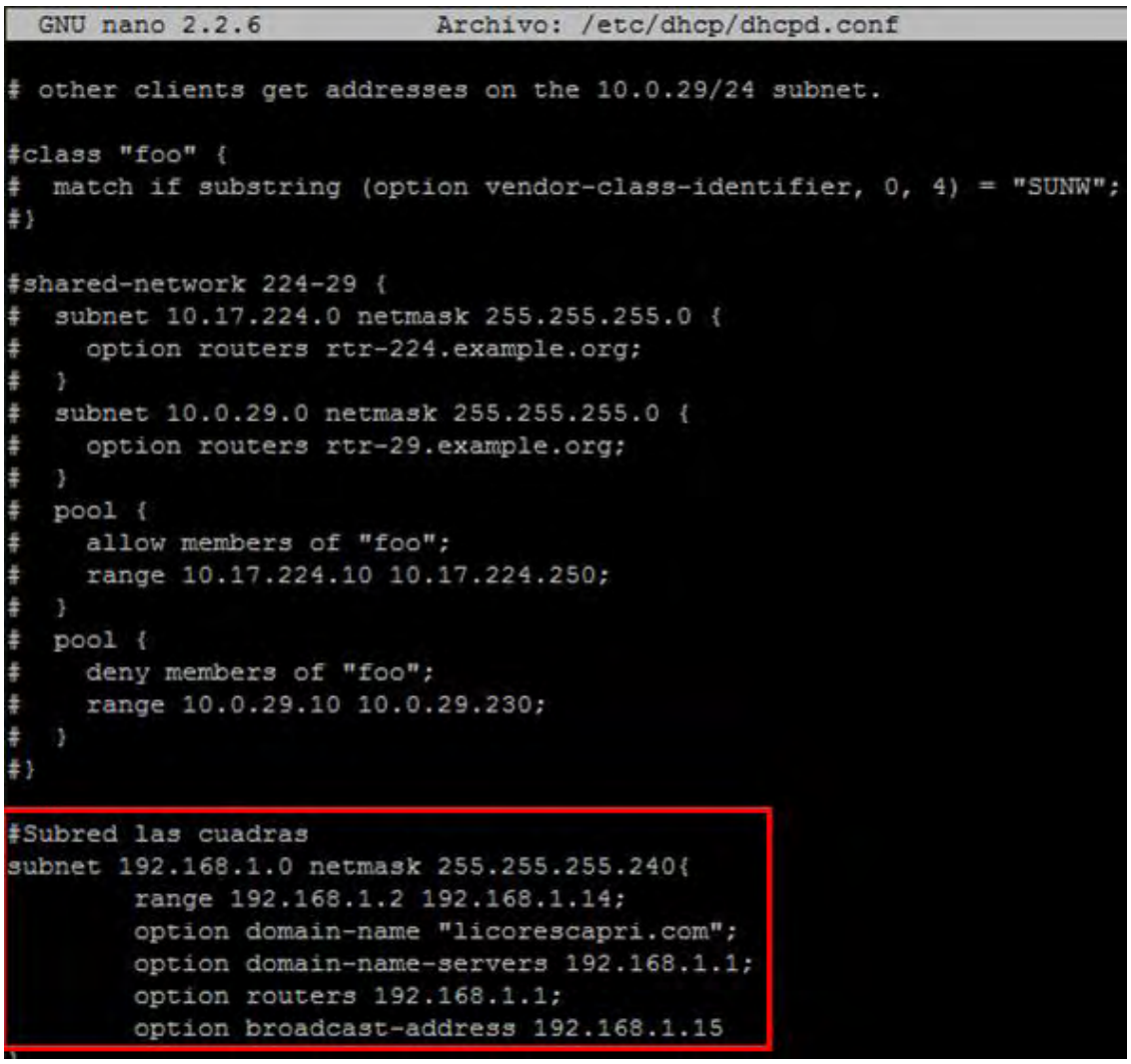


Ahora es necesario editar el archivo de configuración dhcp.conf con el editor nano, como se describe en la Figura 80.

Figura 80. Edición archivo dhcp.conf

Se modifica el archivo de configuración, de tal manera que el servicio DHCP brinde un rango de direcciones IP de forma dinámica a los computadores conectados a la subred, agregando al final algunas líneas en las cuales se especifica la dirección IP de la subred a crear tal como se especifica en la tabla de subnetting, el rango de direcciones IP que se asigna dentro de la subred, un nombre de dominio de la red, la dirección IP de la subred que sirve como puerta de enlace, la dirección IP que sirve como ruta y la dirección IP del broadcast de la subred, como se muestra en la Figura 81.

Figura 81. Creación de subred en el archivo dhcpd.conf



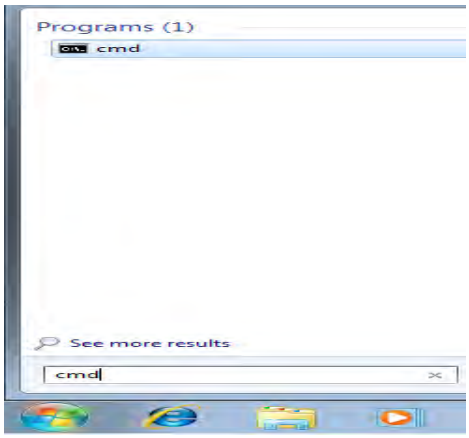
Por último, se debe reiniciar el servicio isc-dhcp-server para que las configuraciones realizadas tengan efecto, como se identifica en la Figura 82.

Figura 82. Reinicio de servicio isc-dhcp-server

```
root@servidorCapri:/etc/dhcp# /etc/init.d/isc-dhcp-server restart
isc-dhcp-server stop/waiting
isc-dhcp-server start/running, process 1440
```

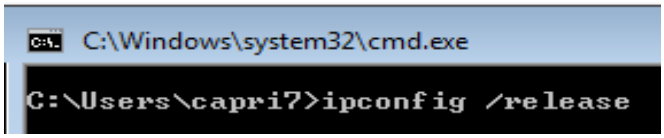
Para verificar que el servicio DHCP este asignando direccionamiento de la subred configurada en el servidor, a los computadores conectados dentro de la subred, se le realizan pruebas en un computador cliente, para que el equipo identifique su re direccionamiento, se procede a abrir una consola de comandos en una maquina cliente con Windows 7, como se ve en la Figura 83.

Figura 83. Abrir consola en Windows 7



En la consola de comandos de Windows se debe hacer un barrido de todas las direcciones IP que estén configuradas por defecto en el computador, con el comando ipconfig /release, como se muestra en la Figura 84.

Figura 84. Reinicio y barrido de direcciones IP en las interfaces de red de Windows



Luego con el comando ipconfig /renew, se procede a asignar automáticamente las direcciones IP que el servidor DHCP le dé a la máquina cliente, en la Figura 85, se muestra la ejecución del comando, y en la Figura 86, se despliega la información de la interfaz de red, configurada con la IP designada por el servidor.

Figura 85. Ejecución del comando ipconfig /renew para asignación de nuevas IP

Figura 86. IP asignada a la interfaz de red ethernet maquina cliente Windows

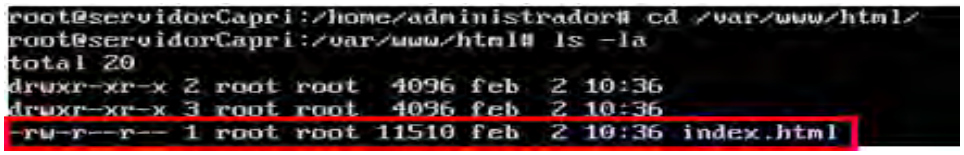
4.13 CONFIGURACIÓN DE SERVIDOR WEB APACHE

Para el servidor web se instala la aplicación apache, la cual se la encuentra en los repositorios oficiales del sistema operativo, se debe descargar con el comando apt-get como se ve en la Figura 87.

Figura 87. Instalación apache2

Por defecto las páginas que se quieran publicar, se guardan en el directorio /var/www/html. Como se ve en la Figura 88, ejecutando el comando ls –la el cual lista de forma detallada archivos en la ruta especificada, se observa que hay un archivo llamado index.html el cual se crea por defecto cuando se instala la aplicación.

Figura 88. Página por defecto apache2



Para cambiar el contenido de esta página existen opciones como: Editarla o borrarla y volverla a crear. En este caso se borrará la página por defecto con el comando rm –r como se ve en la Figura 89.

Figura 89. Eliminar página por defecto en el directorio de publicación

```
root@servidorCapri:/var/www/html# rm -r index.html
```

En la Figura 90, se aprecia la creación nuevamente del archivo index.html, el cual sirve como la página por defecto del directorio de publicación de apache.

Figura 90. Crear nueva página por defecto

```
root@servidorCapri:/var/www/html# nano index.html
```

En el archivo se crea una página web de ejemplo básica tipo HTML para hacer la respectiva prueba de conexión del servidor. Ver Figura 91.

Figura 91. Código HTML básico página por defecto

```
 GNU nano 2.2.6                                  Archivo: index.html

<!DOCTYPE html>
<html>
<head>
  <title>Licores Capri</title>
  <meta http-equiv="Content-Type" content="text/html;  charset="UTF-8">
  <link href="style.css" rel="stylesheet">
</head>
<body>
    <div id="div1">
        <table>
            <tr>
                <td style="text-align: center"><img id="img2" src="Images/IMG5.png"></td>
            </tr>
        </table>
    </div>
    <div>
        <img id="img1" src="Images/IMG4.jpg">
    </div>
    <div id="div2">
        <div id="div3">
            <h1>SERVICIO A DOMICILIO</h1>
            <p>TELEFONOS 7201585 - 7371121</p>
            <p>CELULAR 311 3243767 - 318 3576572</p>
        </div>
        <div id="div4">
            <h1>CONTACTOS</h1>
            <p>CRA 19 #19-159 CENTRO</p>
            <p>CALLE 21 # 31B-08 LAS CUADRAS</p>
            <p>SAN JUAN DE PASTO</p>
        </div>

    </div>
</body>
</html>
```

También se crea el archivo style.css, el cual es el encargado de configurar los estilos que tendrá la página web como se observa en la Figura 92.

Figura 92. Archivo de estilos style.css

```
table{
    margin: auto;
    width: 100%;
}
#div1{
   text-align: center;
}
#div2{
    display: flex;
    justify-content: center;
    background: black;
}
#div3{
    padding: 10px;
  margin: 10px;
}
#div4{
    padding: 10px;
  margin: 10px;
}
h1{
    text-align: center;
    font-family: sans-serif;
    color: blue;
}
p{
    text-align: center;
    color: white;
}
body{
    background: beige;
}
#img1{
    width: 100%;
}
```

En el caso de necesitar imágenes en la creación del sitio web, se debe crear un directorio en el cual se almacenan todas las imágenes a ser utilizadas las cuales son referenciadas desde el archivo HTML que se creó anteriormente. Para este caso se copia el directorio Images en donde se encuentran alojadas las imágenes para la página web, desde el directorio /samba/Capri/Images como se observa en la Figura 93.

Figura 93. Directorio de almacenamiento de imágenes

```
root@servidorCapri:/home/administrador/web/www# cp -r /samba/capri/Images/ .
root@servidorCapri:/home/administrador/web/www# ls
adm  Images  index.html  style.css
```

Se comprueba el funcionamiento de la página web creada en una de las maquinas Windows conectada a la subred, escribiendo el dominio licorescapri.com o www.licorescapri.com en un navegador de internet, como se aprecia en la Figura 94.

Figura 94. Sitio web www.licorescapri.com

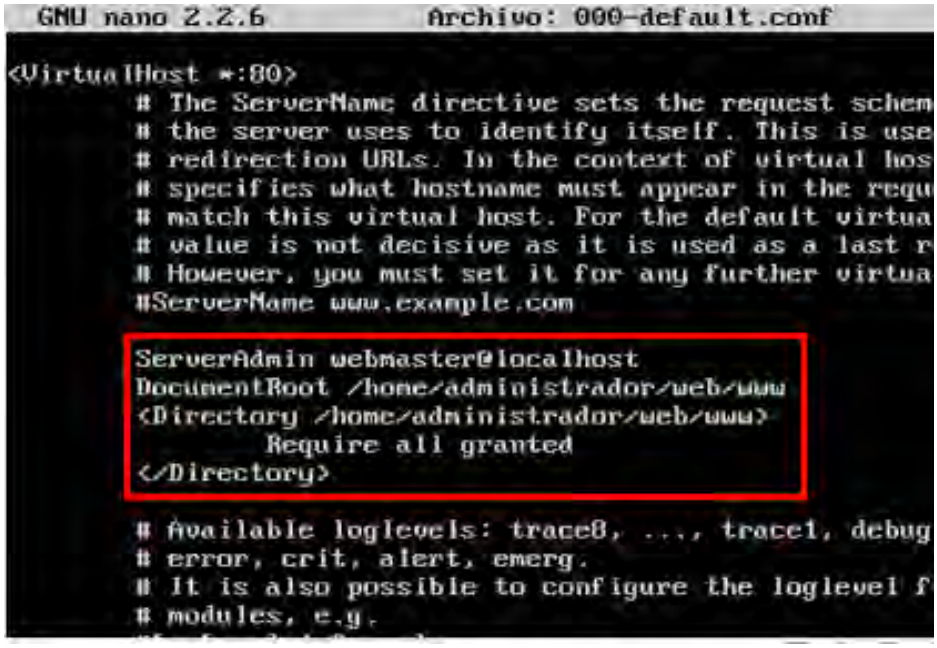
Para cambiar el directorio de publicación del servidor web se debe modificar el archivo 000-default.conf ubicado en la ruta /etc/apache2/sites-available/, como se muestra en la Figura 95.

Figura 95. Ruta y edición archivo 000-default.conf para cambiar ruta de publicación

```
root@servidorCapri:/var/www/html# cd /etc/apache2/sites-available/
root@servidorCapri:/etc/apache2/sites-available# nano 000-default.conf
```

Se modifica la ruta de publicación por defecto por un nuevo directorio que se lo ubica según la conveniencia del administrador del servidor, en este caso la ruta a especificar es /home/administrador/web/www, y se le otorgan los permisos necesarios en la sección Directory, como se muestra en la Figura 96.

Figura 96. Modificación de ruta de publicación de páginas web



Una vez realizadas las modificaciones en el archivo 000-default.conf se crea el nuevo directorio donde se deben almacenar las páginas web del servidor web con el comando mkdir –p /web/www en la ruta /home/administrador, como se aprecia en la Figura 97, comprobando que las carpetas se hayan creado con el comando ls.

Figura 97. Crear directorio de publicación de páginas web apache

Dentro de la ruta creada se añade y edita un nuevo archivo llamado index.html, como se aprecia en la Figura 98.

Figura 98. Crear y editar archivo por defecto en el nuevo directorio de publicación

```
root@servidorCapri:/home/administrador/web/www# nano index.html_
```

En el archivo index.html de la nueva ruta de publicación se crea la estructura HTML de una página web básica, añadiendo la ruta del nuevo directorio, para hacer la comprobación en el navegador, el archivo debe ser similar al que se muestra en la Figura 99.

Figura 99. Código HTML básico página nuevo directorio de publicación

```
  GNU nano 2.2.6                                    Archivo: index.html

<!DOCTYPE html>
<html>
<head>
  <title>Licores Capri</title>
  <meta http-equiv="Content-Type" content="text/html;  charset="UTF-8">
  <link href="style.css" rel="stylesheet">
</head>
<body>
    <div id="div1">
        <table>
            <tr>
                <td style="text-align: center"><img id="img2" src="Images/IMG5.png"></td>
            </tr>
        </table>
    </div>
    <div>
        <img id="img1" src="Images/IMG4.jpg">
    </div>
    <div id="div2">
        <div id="div3">
            <h1>SERVICIO A DOMICILIO</h1>
            <p>TELÉFONOS 7201585 - 7371121</p>
            <p>CELULAR 311 3243767 - 318 3576572</p>
        </div>
        <div id="div4">
            <h1>CONTACTOS</h1>
            <p>CRA 19 #19-159 CENTRO</p>
            <p>CALLE 21 # 31B-08 LAS CUADRAS</p>
            <p>SAN JUAN DE PASTO</p>
        </div>

    </div>
</body>
</html>
```

Una vez se guarda y se crea el archivo de la nueva página web se debe reiniciar el servicio del servidor web conocido como apache2, como se aprecia en la Figura 100.

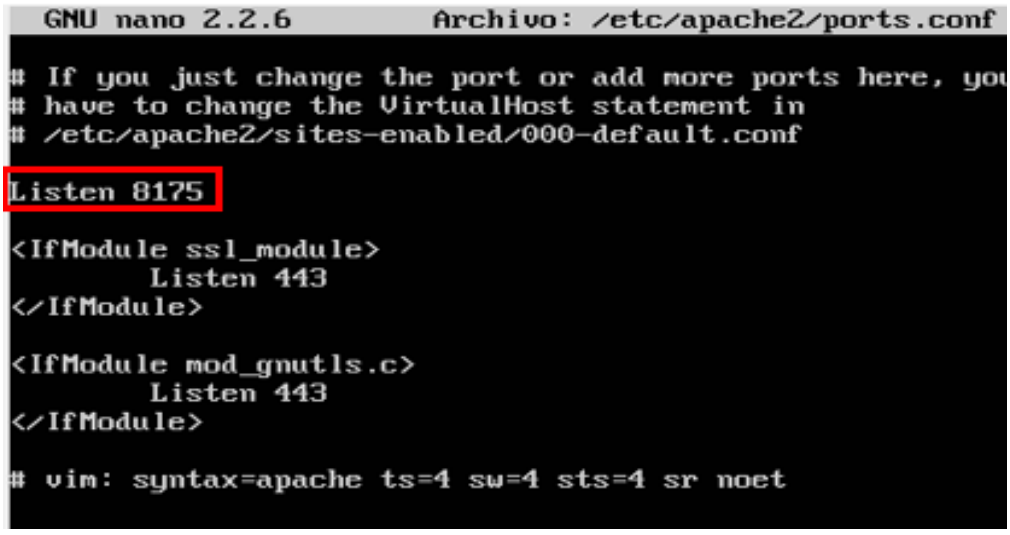
Figura 100. Reinicio del servicio apache2 para nuevo directorio de publicación

Para modificar el puerto por el cual se escuchan las peticiones de apache se debe abrir el archivo ports.conf, ubicado en la ruta /etc/apache2/, como se ve en la Figura 101.

Figura 101. Editar archivo de configuración ports.conf para cambio de puerto

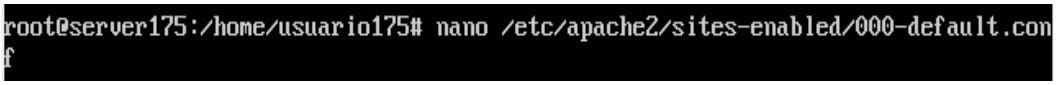
Una vez dentro del archivo ports.conf se debe buscar la línea donde se encuentre el texto Listen 80 y cambiar el numero por 8175, como se identifica en la Figura 102.

Figura 102. Modificar puerto por defecto de apache en el archivo ports.conf



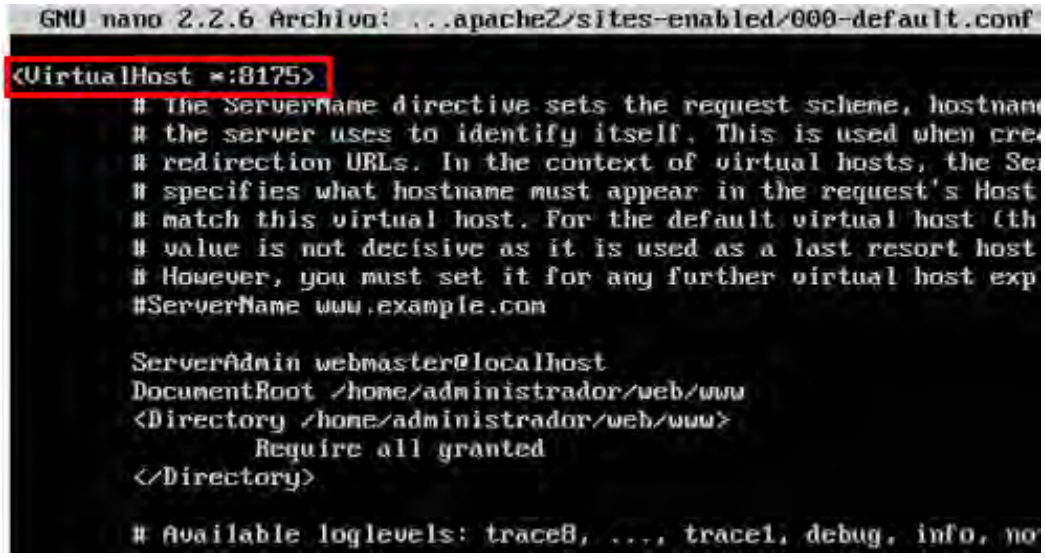
Se guardan los cambios del archivo, y se procede a modificar unas líneas del archivo 000-default.conf para el cambio de puerto, como se aprecia en la Figura 103.

Figura 103. Edición archivo de configuración 000-default.conf, cambio de puerto apache



Una vez dentro del archivo 000-default, se busca la línea <VirtualHost *:80>, y se lo modifica por el numero 8175 como se muestra en la Figura 104.

Figura 104. Modificar puerto por defecto de apache en el archivo 000-default.conf

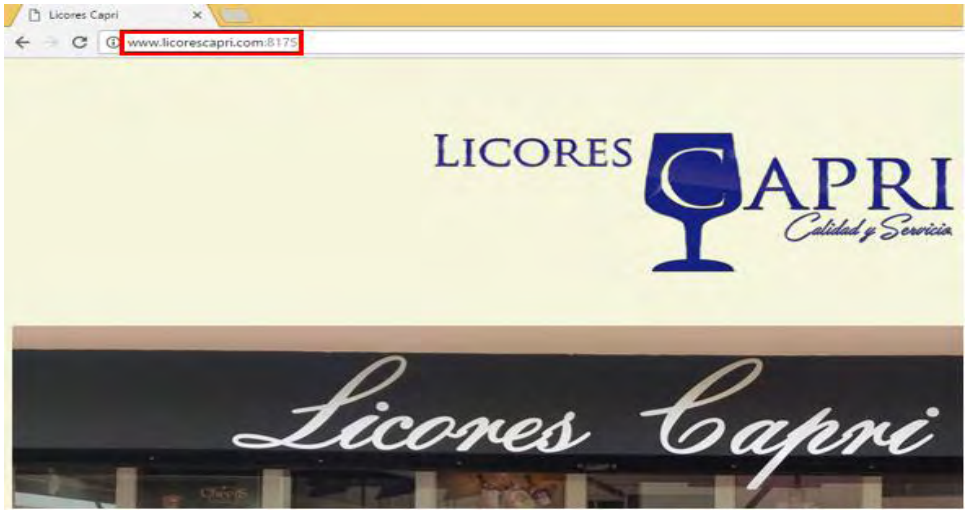


Se reinicia nuevamente el servicio para que todos los cambios surtan efecto, con el comando service apache2 restart, como se aprecia en la Figura 105.

Figura 105. Reiniciar el servicio apache2 para cambio de puerto

Se comprueba el funcionamiento de la página web en el nuevo puerto configurado, mediante un navegador de un equipo Windows conectado a la subred local, escribiendo el dominio www.licorescapri.com y especificando el nuevo puerto de escucha asignado 8175, como se puede verificar en la siguiente Figura 106.

Figura 106. Comprobar cambio de puerto en el navegador web



Para utilizar un método de autenticación en apache para la página web de administración de la empresa, se debe modificar la base de datos del servidor DNS en el directorio /etc/bind/ con el nombre de db.licores, como se ve en la Figura 107.

Figura 107. Editar base de datos db.licores para nuevo sitio de administración

```
root@servidorCapri:~# nano /etc/bind/db.licores
```

En este archivo se debe agregar el nombre adm de tipo address (dirección), que direccione a la misma IP del servidor, como se aprecia en la Figura 108.

Figura 108. Agregar sitio de administración a la base de datos

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     licorescapri.com. root.licorescapri.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      licorescapri.com.
@       IN      A       192.168.0.149
www     IN      A       192.168.0.149
adm     IN      A       192.168.0.149
```

Al finalizar la edición del archivo se debe reiniciar el servicio bind9 para que el servidor DNS agregue el nuevo dominio de administración y poder continuar la configuración, como se aprecia en la Figura 109.

Figura 109. Reiniciar el servicio bind9 para habilitar sitio de administración apache

```
root@servidorCapri:~# service bind9 restart
```

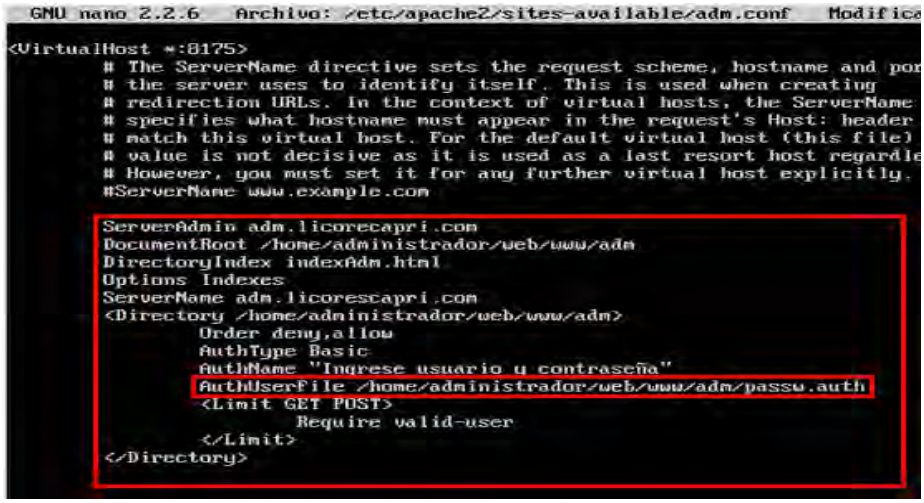
Ahora se crea el archivo de configuración para el nuevo sitio web de administración. Para esto se debe ubicar en el directorio /etc/apache2/sites-available/ y realizar una copia del archivo de configuración 000-default.conf con el nombre de adm.conf y una vez creado este archivo se procede a editarlo, según se muestra en la Figura 110.

Figura 110. Crear archivo de configuración para sitio de administración

```
root@servidorCapri:~# cd /etc/apache2/sites-available/
root@servidorCapri:/etc/apache2/sites-available# cp 000-default.conf adm.conf
root@servidorCapri:/etc/apache2/sites-available# nano adm.conf
```

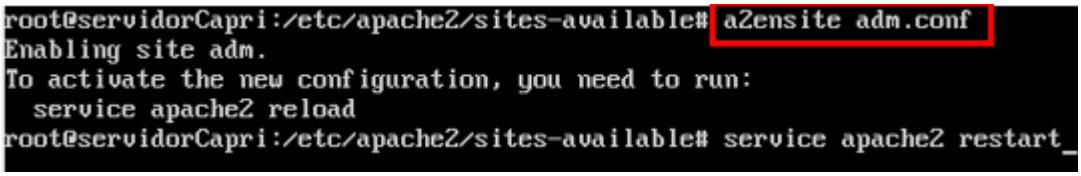
En la Figura 111, se aprecia la nueva configuración que debe tener el nuevo sitio de administración, agregando un nuevo directorio de publicación, ubicado en /home/administrador/web/www/adm, y su archivo web por defecto indexAdm.html, el nombre de la página de administración del servicio adm.licorescapri.com y el nombre de dominio a utilizar, adicionalmente a estas configuraciones básicas para la puesta en marcha de la página web, se adiciona la opción de habilitar un método de autenticación para los accesos al abrir el sitio web adm.licorescapri.com:8175, definiendo la ruta del archivo passwd.auth, ubicado en /home/administrador/web/www/adm que contendrá el nombre del usuario y contraseña del administrador de la página.

Figura 111. Configuración del archivo adm.conf con método de autenticación



Una vez realizada la edición del archivo se lo debe habilitar en el servidor web con el comando a2ensite, como se muestra en la Figura 112.

Figura 112. Habilitar archivo de configuración adm.conf



Ahora se crea el directorio de publicación para el sitio web de administración en la ruta /home/administrador/web/www/ y se crea la nueva página web indexAdm.html, mostrado en la Figura 113.

Figura 113. Crear nuevo directorio de publicación para el sitio de administración

Se escribe un código HTML básico para crear una página de ejemplo para el sitio de administración y copia el archivo de estilos e imágenes de archivo index.html como lo descrito en la Figura 114 y Figura 115.

Figura 114. Código HTML básico para el nuevo sitio web de administración

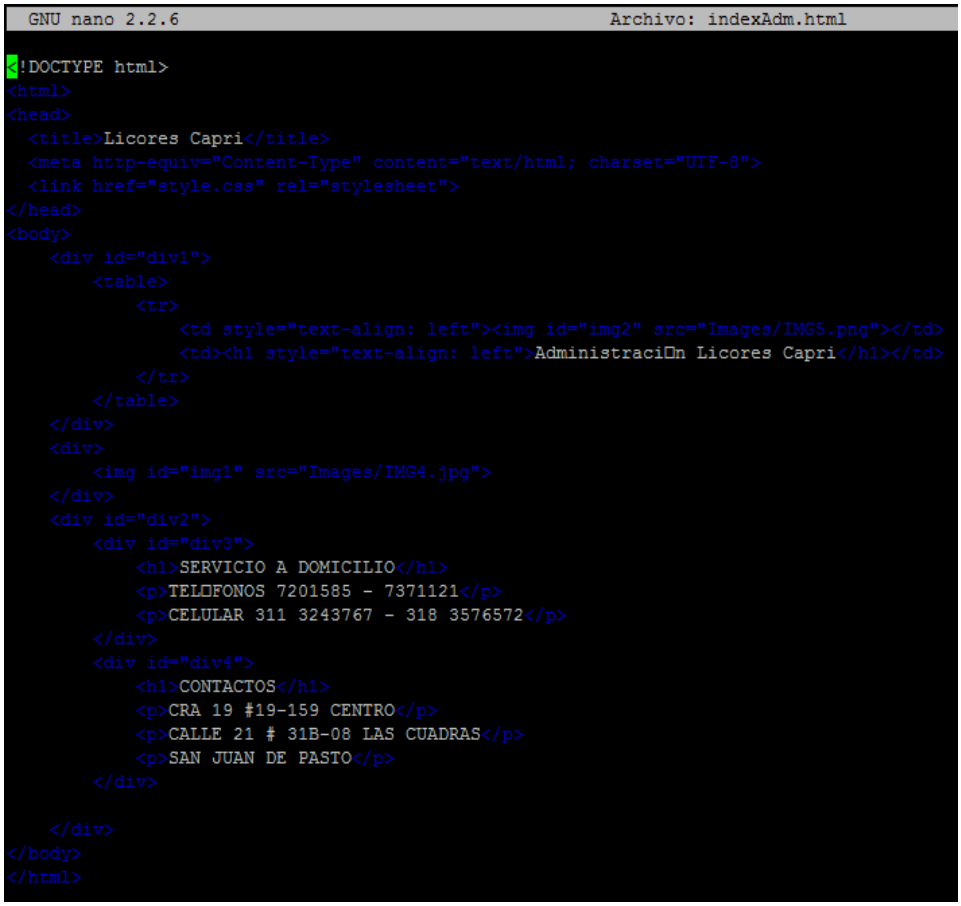
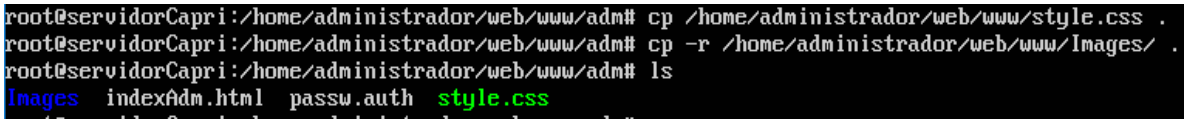
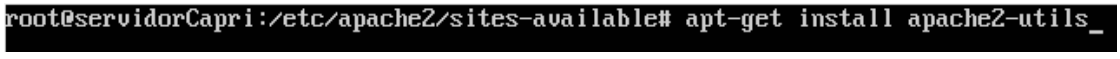


Figura 115. Archivo de configuración e imágenes sitio de administración



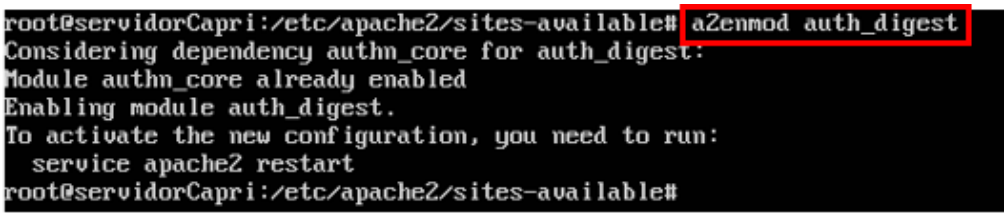
Para la creación de la contraseña de acceso al sitio web de administración es necesario instalar apache2-utils, el cual está disponible en los repositorios oficiales del sistema operativo, mediante la digitación del comando apt-get mostrado en la Figura 116, donde se consigue el paquete necesario.

Figura 116. Instalar apache2-utils



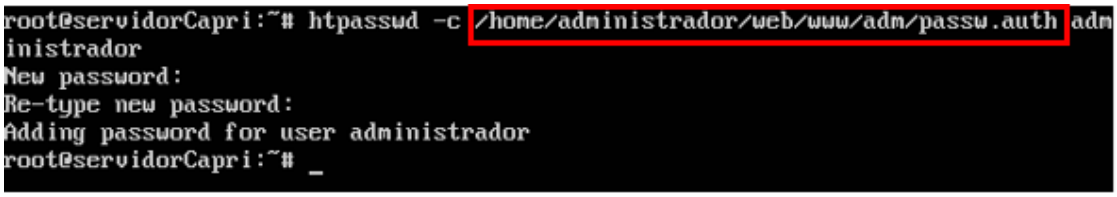
También se habilita el método de autenticación mediante el comando a2enmod mostrado en la Figura 117.

Figura 117. Habilitar método de autenticación



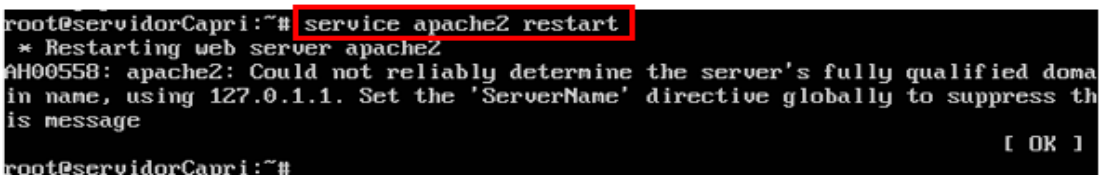
Se crea la contraseña de acceso para el sitio web mediante el comando htpasswd. Es muy importante especificar la ruta en donde se almacenará la contraseña seguida del usuario al cual se le crea la contraseña, esta ruta debe ser la misma que se eligió en el archivo de configuración adm.conf en la sección AuthUserFile, la Figura 118, muestra de forma detallada la ruta a la cual se debe especificar.

Figura 118. Crear contraseña para el usuario administrador



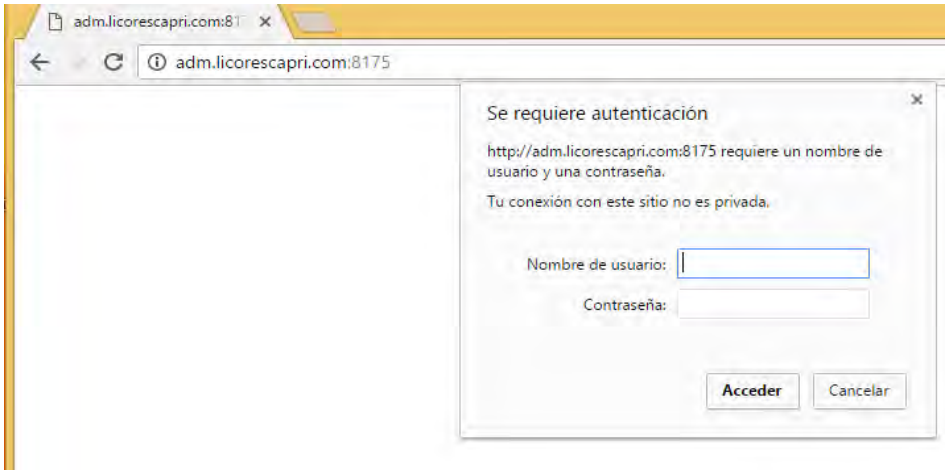
Finalmente, como se aprecia en la Figura 119, se debe reiniciar el servicio de apache2 para efectuar los cambios realizados

Figura 119. Reiniciar el servicio apache2 para habilitar la autenticación de usuarios



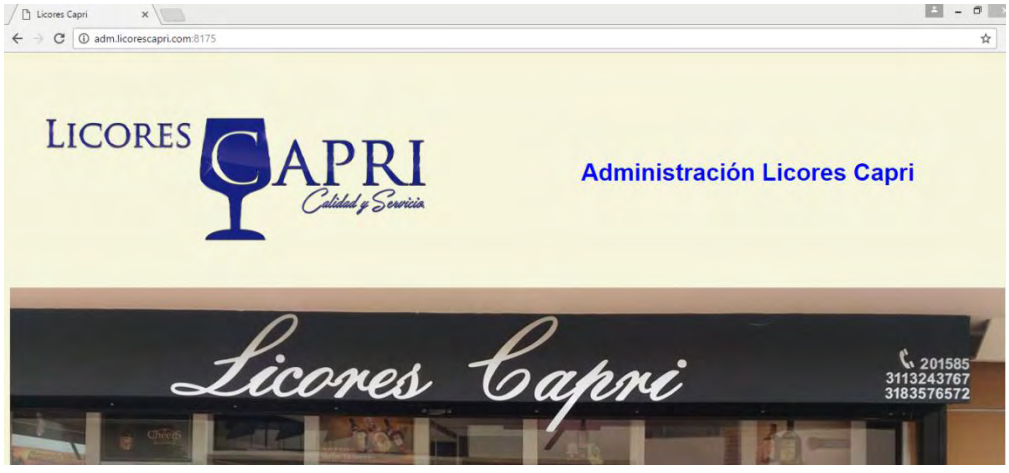
Se comprueba que el método de autenticación de usuarios para el sitio web de administración está funcionando accediendo al navegador desde una maquina Windows escribiendo el dominio adm.licorescapri.com y especificando el puerto 8175, ver Figura 120.

Figura 120. Comprobar autenticación de usuarios en navegador web



Una vez ingresado el nombre de usuario y la contraseña correctamente se ingresa al sitio web de administración, como se ve en la Figura 121.

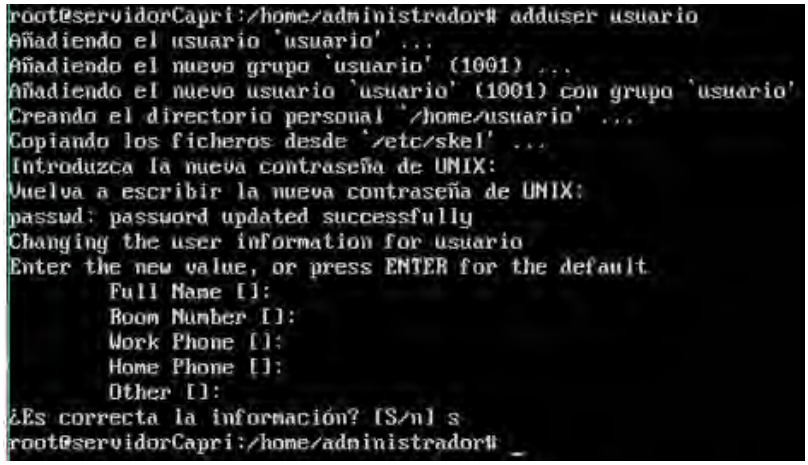
Figura 121. Sitio web de administración licores Capri



4.14 CONFIGURACIÓN DEL SERVICIO DE RED SSH

Para realizar una conexión remota mediante un servidor SSH se debe crear un nuevo usuario con cualquier nombre, para este caso se añade usuario. La creación de este nuevo usuario debe realizarse con el rol de súper usuario mediante el comando sudo su. Una vez dentro de este rol se crea el nuevo usuario como se ve en la Figura 122.

Figura 122. Añadir nuevo usuario Ubuntu server para acceso a SSH

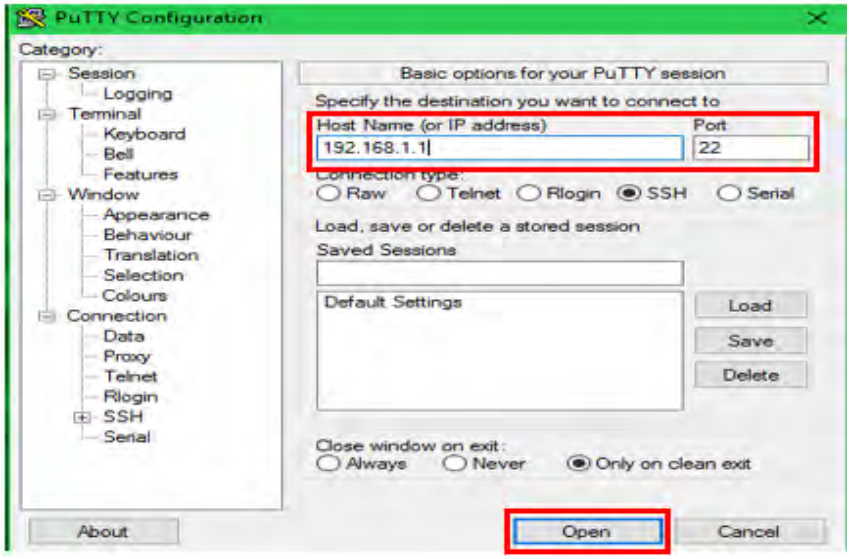


Para el servidor SSH se instala la aplicación con el mismo nombre, la cual se la encuentra en los repositorios oficiales del sistema operativo, se debe descargar con el comando apt-get como se ve en la Figura 123.

Figura 123. Instalar servicio SSH

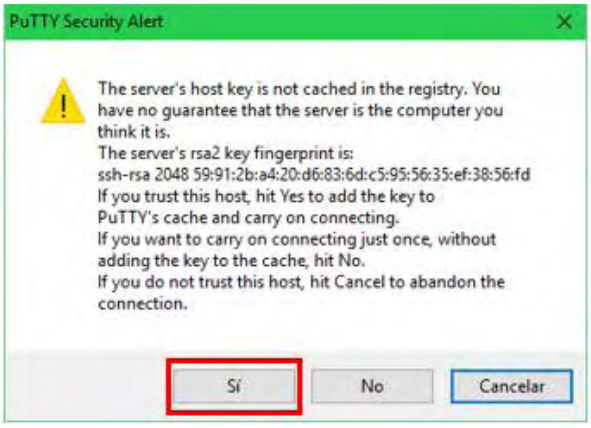
Para realizar la conexión remota se utiliza la herramienta PuTTY desde una maquina Windows e ingresando la dirección IP del servidor SSH y autenticándose como el usuario creado en el paso anterior como muestra la Figura 124.

Figura 124. Acceso al servidor mediante la herramienta PuTTY



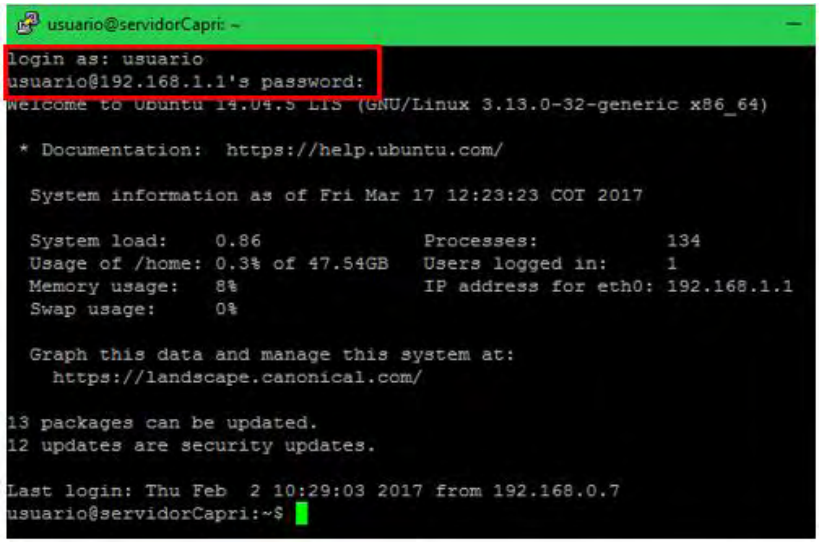
Si no hay ningún problema de conexión, debe aparecer una ventana con una alerta de seguridad confirmando la entrada al servidor, se escoge la opción Si, como aparece en la Figura 125.

Figura 125. Alerta de seguridad de ingreso al servidor



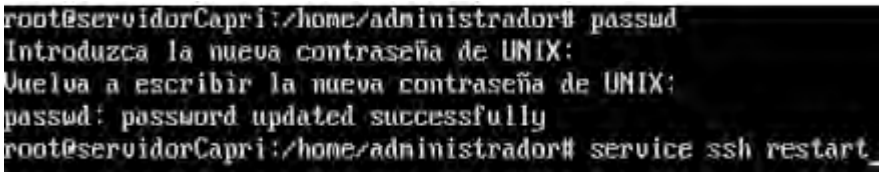
En la Figura 126, se muestra una pantalla de autenticación y se ingresan los datos del usuario creado y la contraseña. Al ingresar aparece la pantalla de inicio del servidor.

Figura 126. Autenticación de usuarios en el servidor mediante SSH



Para poder acceder al servidor como el usuario root es necesario modificar el archivo de configuración sshd_config, y también establecer una contraseña para este usuario, esto se hace de acuerdo a lo hecho en la Figura 127.

Figura 127. Crear contraseña para usuario root y reiniciar el servicio SSH



.

Se debe modificar el archivo de configuración sshd_config, ubicado en la ruta /etc/ssh/ mediante el comando nano, como se muestra en la Figura 128.

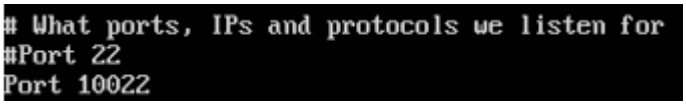
Figura 128. Editar el archivo sshd_config para el ingreso como root

Para permitir el acceso del usuario root al servidor por ssh, se debe buscar en el archivo de configuración la línea PermitRootLogin y cambiar la palabra no por si como muestra la Figura 129.

Figura 129. Modificar el archivo de configuración para el acceso como usuario root

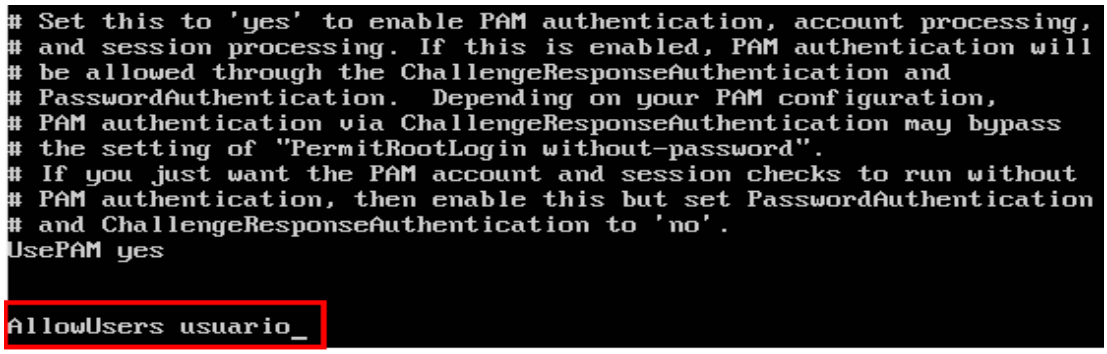
Para cambiar el puerto de escucha, se debe comentar el puerto 22 y establecer el nuevo puerto 10022 en la línea Port, mostrado en la Figura 130.

Figura 130. Modificar puerto por defecto



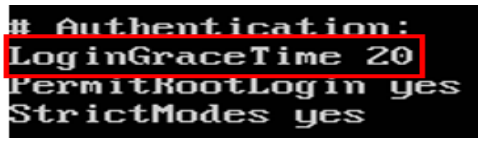
Si se desea que solo algunos usuarios puedan ingresar al servidor, se debe añadir la línea AllowUsers seguido de los usuarios que tendrán acceso al servidor por SSH, como se ve en la Figura 131.

Figura 131. Permitir conexión al servidor de usuarios predeterminados



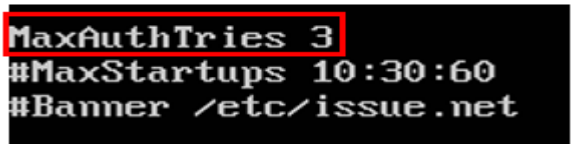
Para mantener la seguridad del servidor SSH es importante tener en cuenta algunas reglas que son muy importantes y sirven de protección para el acceso al servidor. Entre estas reglas se encuentra el tiempo que se muestra la interfaz de autenticación de usuario en pantalla para que un usuario se identifique, para establecer este tiempo en 20 segundos se debe modificar el archivo en la línea LoginGraceTime, como se aprecia en la Figura 132.

Figura 132. Tiempo límite de autenticación de usuarios en el servidor



De la misma manera que se puede limitar el tiempo, es posible limitar el número de intentos que un usuario puede hacer al momento de ingresar la contraseña, para esto se debe modificar el número de intentos, 3 intentos para este caso, en la línea MaxAuthTries, mostrado en la Figura 133.

Figura 133. Número máximo de intentos para autenticarse como usuario



También se puede limitar el número de sesiones sin autenticar que se pueden abrir al tiempo en el servidor, de esta manera se evitan ataques que intentan obtener el nombre y la contraseña del usuario haciendo múltiples pruebas en diferentes ventanas de autenticación hasta lograr conseguir esta información. Para modificar este parámetro se modifica la línea MaxStartUps mostrada en la Figura 134.

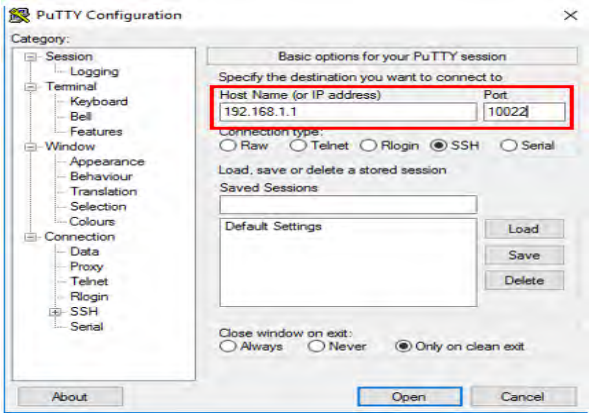
Figura 134. Número máximo de sesiones sin autenticar en el servidor

Después de cada modificación realizada al archivo de configuración sshd_config, se guardan los cambios y es necesario reiniciar el servicio SSH con el comando service ssh restart. Ver Figura 135.

Figura 135. Reiniciar el servicio SSH para acceso como usuario root

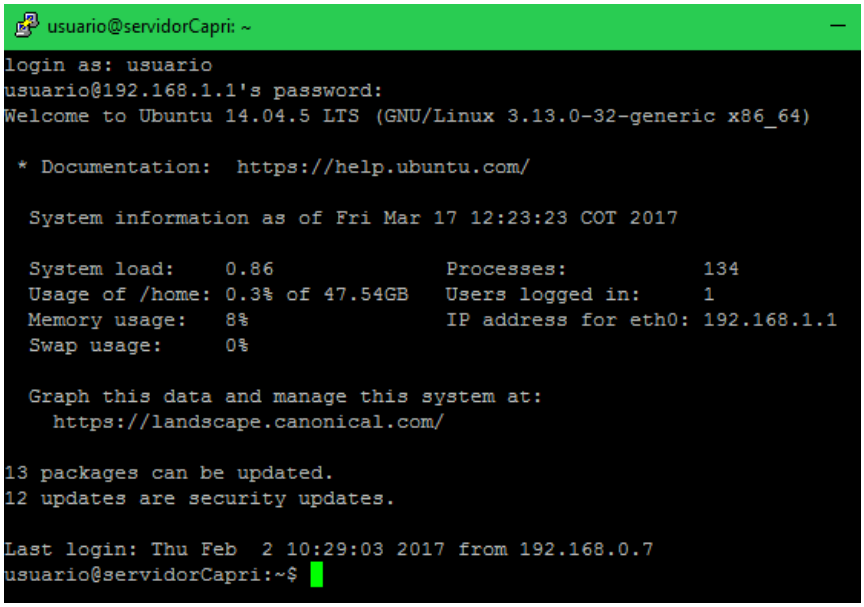
Una vez el servicio sea reiniciado se comprueba nuevamente el ingreso como usuario desde una maquina Windows a la herramienta PuTTY, se debe colocar la dirección IP privada del servidor y el puerto 10022 como se ve en la Figura 136.

Figura 136. Acceso al servidor mediante la herramienta PuTTY puerto modificado



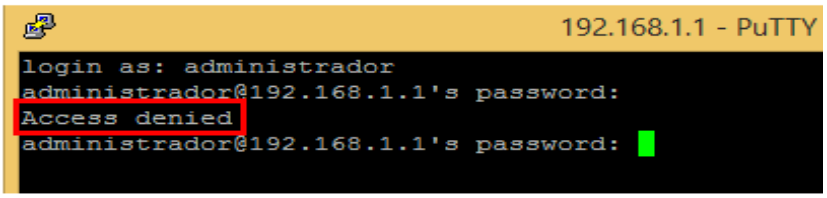
El acceso se debe hacer como usuario y su contraseña, una aceptada la identidad, se muestra la pantalla de inicio del servidor lo cual confirma el acceso mediante el nuevo puerto de conexión, como se aprecia en la Figura 137.

Figura 137. Conexión al servidor mediante el nuevo puerto establecido



En la Figura 138, se comprueba la denegación de acceso al servidor conectándose con el usuario administrador:

Figura 138. Acceso denegado al usuario administrador



Por último, se realizan las pruebas desde las máquinas Windows para verificar que las reglas de seguridad, tiempo de espera (Figura 139), y exceso de intentos fallidos (Figura 140), funcionan de manera correcta.

Figura 139. Mensaje de error por tiempo de espera agotado para la autenticación

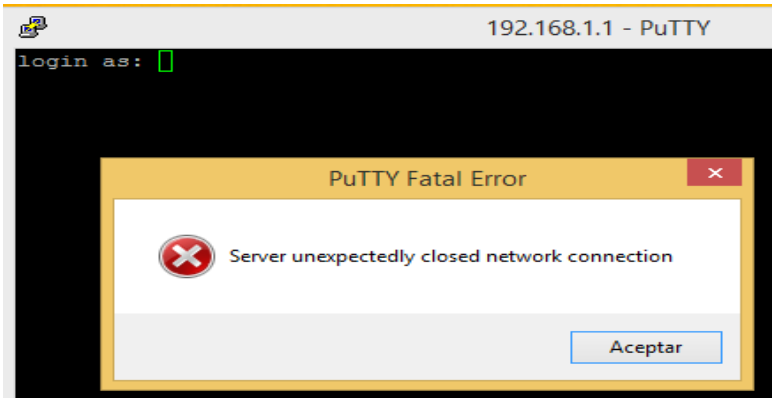
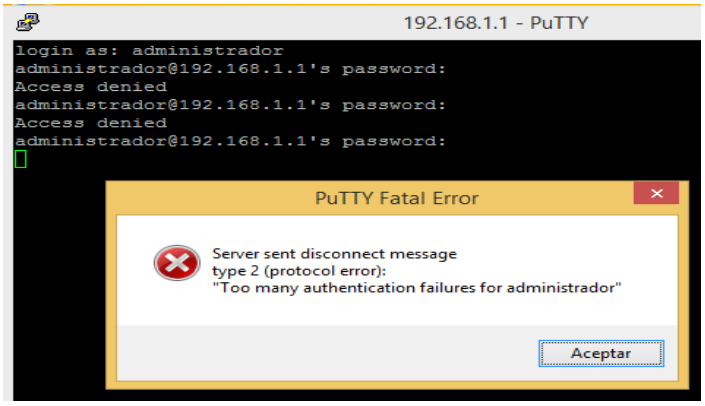


Figura 140. Mensaje de error por exceso de intentos fallidos de autenticación



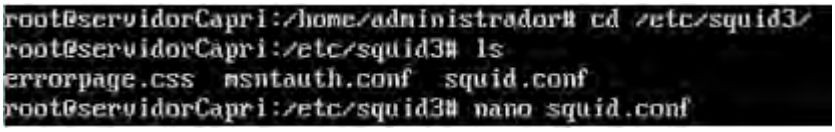
4.15 CONFIGURACIÓN DEL SERVICIO DE RED PROXY

Para gestionar los servicios de acceso a la web mediante un servidor proxy se debe instalar la aplicación squid3, la cual puede ser descargada de los repositorios de Ubuntu con el comando apt-get install squid3 como lo indica la Figura 141.

Figura 141. Instalación aplicación squid3

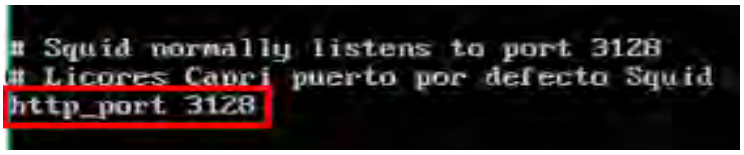
Al finalizar la instalación se debe ubicar en el directorio /etc/squid3/ y editar el archivo de configuración llamado squid.conf mediante el comando nano como lo muestra la Figura 142.

Figura 142. Editar archivo de configuración squid.conf



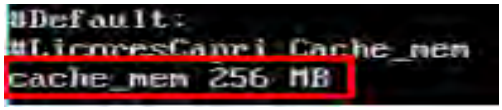
Una vez dentro del archivo, se puede proceder a realizar las diferentes configuraciones para poner en marcha el servicio de proxy. Una de las opciones a modificar es el puerto por el cual se realizan las peticiones. Para su modificación, se debe ubicar en la sección de configuración de puerto navegando a través del documento o presionando las teclas CTRL+W, se escribe la palabra port y presionar Enter. Este proceso se repite cuantas veces sea necesario hasta ubicarse en la línea http_port 3128, como se observa en la Figura 143. Se puede observar que el puerto por defecto es el puerto 3128 el cual es posible modificar en caso de ser necesario.

Figura 143. Modificar puerto por defecto



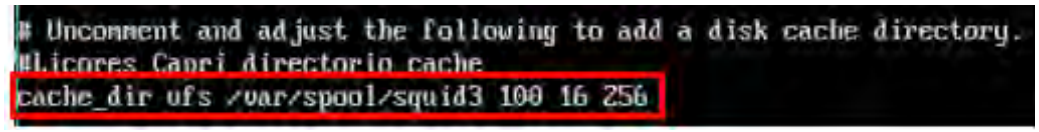
Otra opción importante dentro de la configuración es la asignación de memoria caché para el servidor. Esta opción se configura en la sección se puede ubicar presionando nuevamente las teclas CTRL+W y se escribe la palabra cache_mem en donde se puede cambiar la cantidad de memoria caché (Figura 144).

Figura 144. Asignar memoria caché



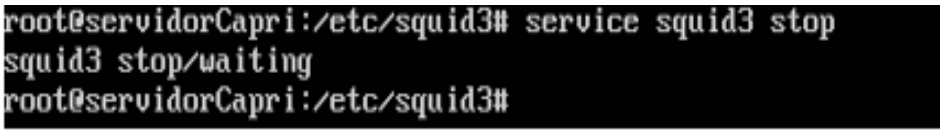
Es importante también, definir la ruta en la cual se almacena la caché y establecer otro tipo de parámetros como el tamaño de disco y la cantidad de directorios y subdirectorios en los cuales se almacena esta información. Se ubica esta sección con las teclas CTRL+W y ahora buscar la palabra cache_dir. En la Figura 145, se observa la ruta de almacenamiento de la caché, seguido del número 100 para especificar el tamaño del disco, el número 16 para la cantidad de directorios que se crean para almacenar la cache y el 256 el número de subdirectorios.

Figura 145. Directorio de almacenamiento de caché



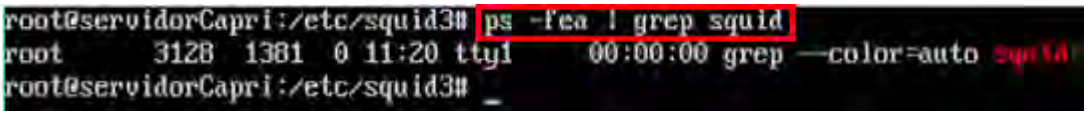
Una vez modificado el archivo de configuración, es necesario detener el servicio para la creación de los directorios y subdirectorios en la ruta que se especificó en el paso anterior. Se ejecuta el comando service squid3 stop para detener el servicio como se muestra en la Figura 146.

Figura 146. Detener el servicio squid3



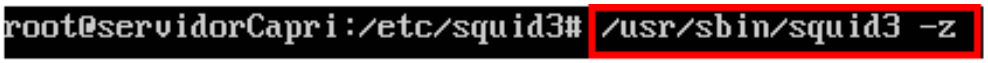
Para verificar que se ha detenido el servicio se ejecuta el comando ps –fea | grep squid, ver Figura 147.

Figura 147. Procesos en ejecución para squid



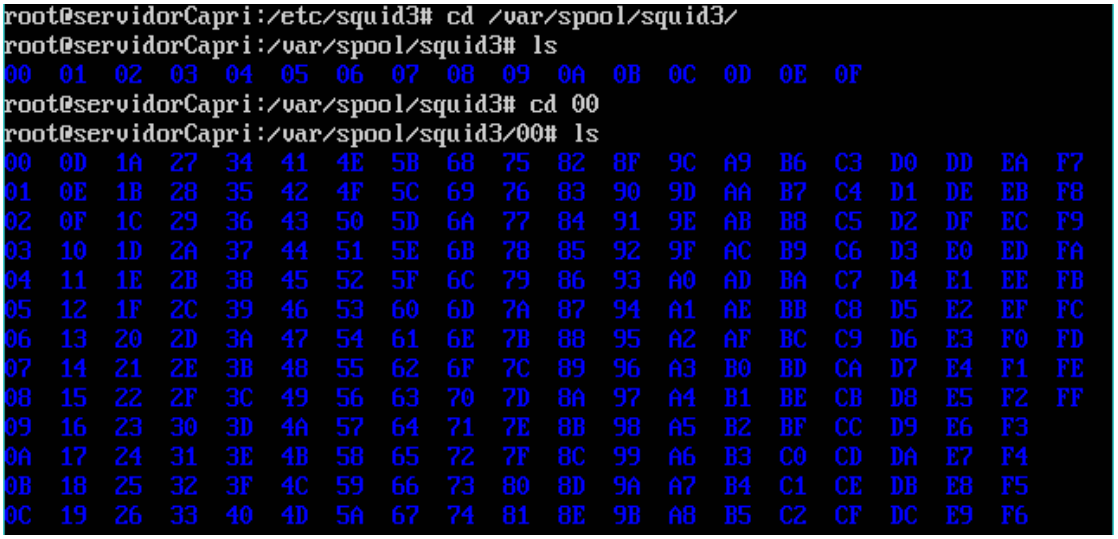
Una vez detenido el servicio squid3, se debe que crear los directorios y subdirectorios que se definió en el paso anterior mediante el comando /usr/sbin/squid3 –z, como se muestra en la Figura 148.

Figura 148. Crear directorios de almacenamiento de caché



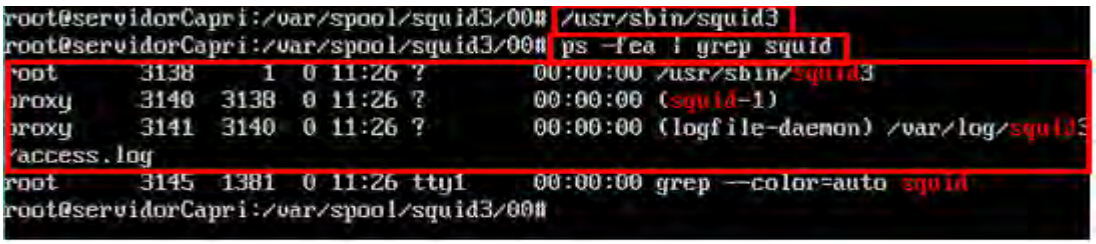
Para comprobar que los directorios y subdirectorios fueron creados se debe cambiar de ubicación a /var/spool/squid3/ y listar los directorios, ver Figura 149.

Figura 149. Directorios y subdirectorios de almacenamiento de caché



Luego se debe levantar el servicio nuevamente con el comando /usr/sbin/squid3, se verifica su funcionamiento y puesta en marcha haciendo uso del comando ps –fea | grep squid, como lo muestra la Figura 150.

Figura 150. Reiniciar servicio squid3



Hasta el momento, ya está configurado el servicio de proxy con la aplicación squid3 en el servidor. Ahora es necesario añadir las listas de control de acceso (acl´s), las cuales son reglas que establece el administrador de la red según las políticas de la empresa. Algunos ejemplos de estas reglas son el permitir o denegar el acceso a internet de una determinada dirección IP o de toda una subred, también se puede denegar el acceso a páginas web, restringir la descarga de cierto tipo de archivos o denegar el acceso a páginas que contengan palabras no deseadas en su URL.

Para realizar este tipo de configuraciones se edita nuevamente el archivo de configuración squid.conf como en la Figura 151.

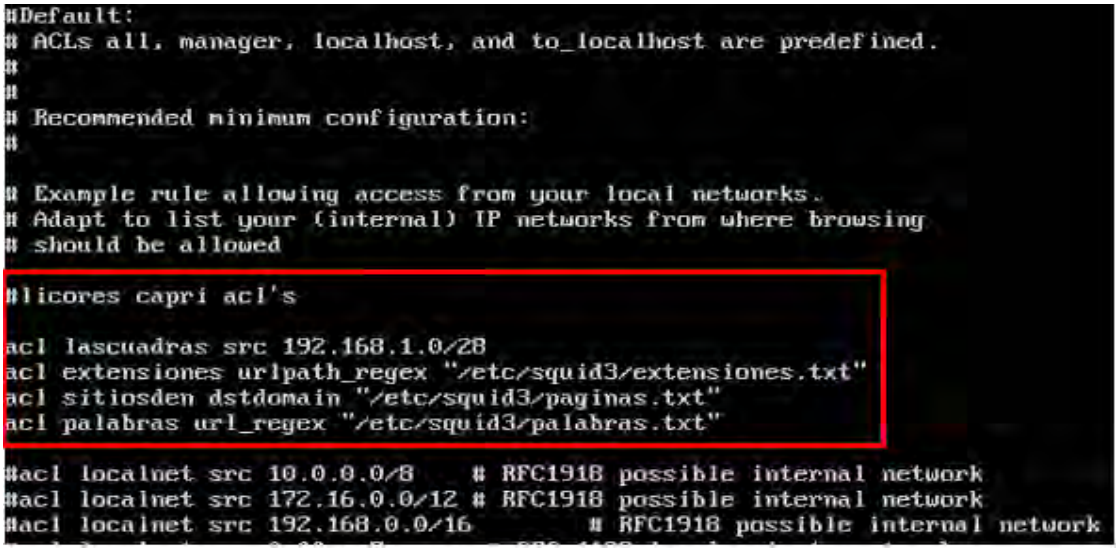
Figura 151. Editar archivo de configuración squid.conf

Una vez dentro del archivo de configuración, se debe localizar la sección de listas de control de acceso, para esto se presiona las teclas Ctrl+W y se escribe la palabra localnet. Sobre esta sección, como se muestra en la Figura 152, se deben ingresar las listas de control de acceso que se han definido acorde con las políticas de la empresa. Como primera medida se debe permitir el acceso a internet a través del proxy a la subred de la empresa, esta lista debe tener un nombre para su identificación, seguido del tipo de regla que se le va a aplicar y la dirección IP de la red con su respectiva máscara de subred.

Las siguientes listas que se configuran, son las de denegación de descarga para ciertos tipos de archivos que pueden consumir el ancho de banda del internet de la red, la lista de control para denegar el acceso a determinadas páginas web y la lista para denegar páginas las cuales en su URL tengan palabras no deseadas.

Como a la lista anterior también se les debe asignar un nombre, el tipo de regla que se va a aplicar y, por último, la ruta en donde se encuentra el archivo de texto que contiene las extensiones de tipo de archivo, las páginas web y las palabras que se van a denegar.

Figura 152. Listas de control de acceso



Al finalizar la definición de las listas de control de acceso, es necesario establecer las reglas que permitirá o denegaran el acceso a estas listas. Para ello se presiona las teclas Ctrl+W y se escribe la palabra http_access para ubicarse en la sección de reglas. Dentro de esta sección se debe tener mucho cuidado en el orden que se escriben las reglas, ya que el acceso o denegación se realiza en forma secuencial y se ejecutan estrictamente en el orden en que aparecen en esta sección. La primera regla que se debe implementar, es la de denegación de acceso a determinadas páginas web. Se debe escribir la palabra http_access, seguida del tipo de regla a implementar que en este caso es denny para denegar el acceso, y por último la lista a la cual se le va a aplicar esa regla.

La siguiente regla es la de permitir el acceso a internet a la red de la empresa, esto se hace de la misma forma que la regla anterior, pero modificando la palabra denny por allow para permitir el acceso de la red a internet.

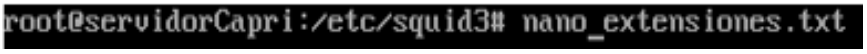
En esta misma regla se puede realizar excepciones para denegar algunos servicios a los equipos de la subred. En este caso para denegar la descarga de determinados tipos de archivo y denegar sitios web en los cuales se encuentren palabras no deseadas en su URL se debe escribir el signo !, seguido del nombre de la lista que se desea denegar. Las anteriores reglas se observan en la Figura 153.

Figura 153. Reglas de acceso o denegación de acl´s

Con eso ya se han configurado las listas de control de acceso y las reglas para el proxy. Ahora es necesario crear los archivos de texto que contienen las extensiones de tipo de archivo, las palabras y los sitios a denegar, en las rutas y con los mismos nombres que se especificaron en las listas de control.

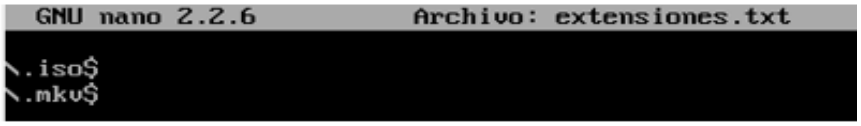
Primero se crea el archivo de texto extensiones.txt en la ruta /etc/squid3, como lo indica la Figura 154.

Figura 154. Crear archivo de texto extensiones.txt



En este archivo, se añade las extensiones de tipo de archivo a las que se desea denegar la descarga. Lo más recomendable es bloquear archivos que tienden a ser muy pesados, ya que su descarga puede ocasionar un excesivo congestionamiento en la red. Algunas de las extensiones de tipo de archivo que suelen ser restringidas por su tamaño son .iso, .nrg y .mkv. Para que estas extensiones sean bloqueadas al momento de su descarga se deben escribir en el archivo de texto, añadiendo el signo \, seguido de la extensión a denegar y finalmente el signo $, ver Figura 155.

Figura 155. Archivo de texto extensiones.txt



También se crea el archivo de texto paginas.txt, como lo muestra la Figura 156.

Figura 156. Crear archivo de texto paginas.txt

```
root@servidorCapri:/etc/squid3# nano paginas.txt
```

En la Figura 157, se ve como se añaden las páginas web que se desea restringir.

Figura 157. Archivo de texto paginas.txt

```
  GNU nano 2.2.6          Archivo: paginas.txt                Modificado

www.facebook.com
www.youtube.com
www.instagram.com
www.twitter.com
```

Del mismo modo se crea y edita el archivo con las palabras a denegar como en la Figura 158 y la Figura 159.

Figura 158. Crear archivo de texto palabras.txt

```
root@servidorCapri:/etc/squid3# nano palabras.txt
```

Figura 159. Archivo de texto palabras.txt

```
  GNU nano 2.2.6          Archivo: palabras.txt               Modificado

mp3
porn
sex
xxx
juegos
videojuego
rom
game
```

Finalmente se reconfigura el servicio squid3 para que se realicen los cambios con el comando /usr/sbin/squid3 –k reconfigure, como se observa en la Figura 160.

Figura 160. Reconfigurar servicio squid3

```
root@servidorCapri:/etc/squid3# /usr/sbin/squid3 -k reconfigure
```

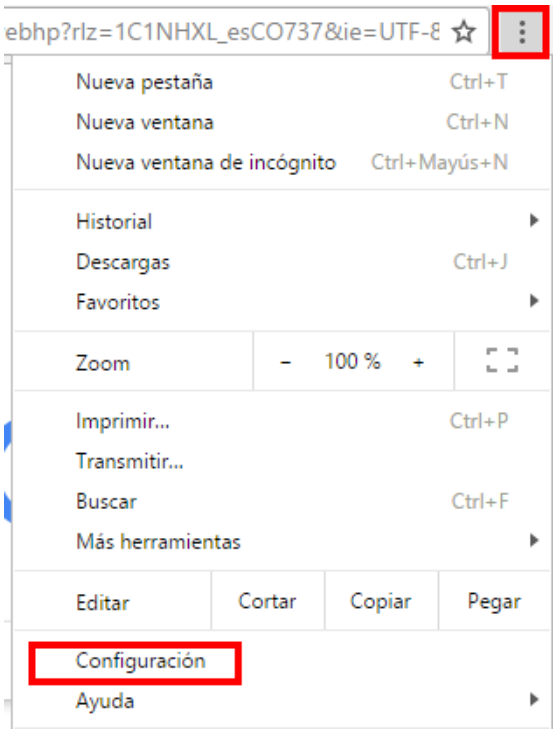
Una vez se reinicia el servicio ya se encuentra disponible el servicio proxy configurado para la red. Se prueba su funcionamiento mediante una máquina Windows dentro de la misma red a la cual se le permitió el acceso.

Antes de iniciar la navegación, se debe realizar la configuración del navegador web en las máquinas cliente, para esto se deben seguir los pasos que se muestran a continuación.

Nota: En este trabajo se configura el servicio de proxy mediante el navegador web Google Chrome.

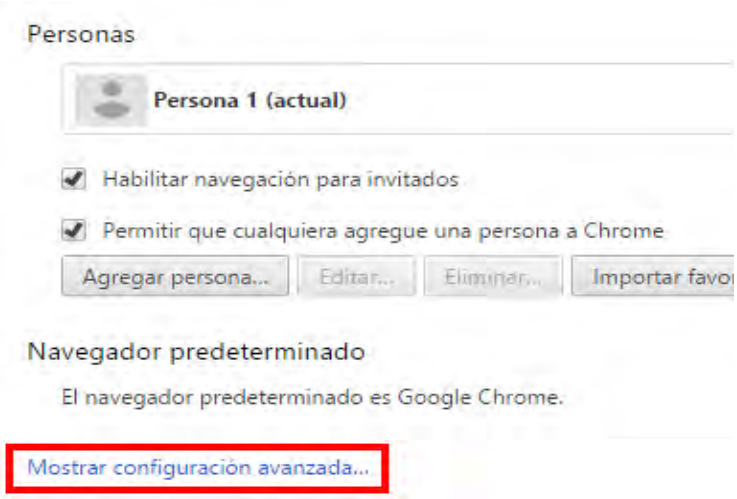
Abrir el navegador web y en la parte superior derecha desplegar el menú al hacer clic sobre el icono de Personaliza y controla Google Chrome. Escoger la opción Configuración, ver Figura 161.

Figura 161. Menú del botón Personaliza y controla tu Google Chrome



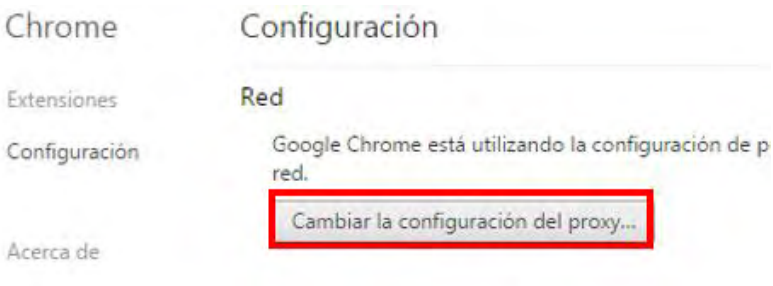
Se muestra la interfaz de configuración del navegador y escoger la opción Mostrar configuración avanzada, ver Figura 162.

Figura 162. Interfaz de configuración de Google Chrome



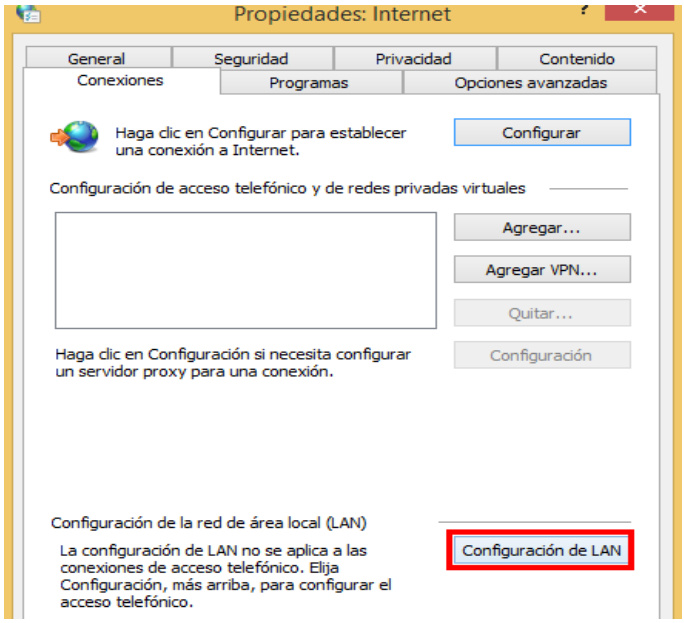
Avanzar hacia la sección de Red y seleccionar el botón Cambiar la configuración del proxy, ver Figura 163.

Figura 163. Configuración de red del navegador



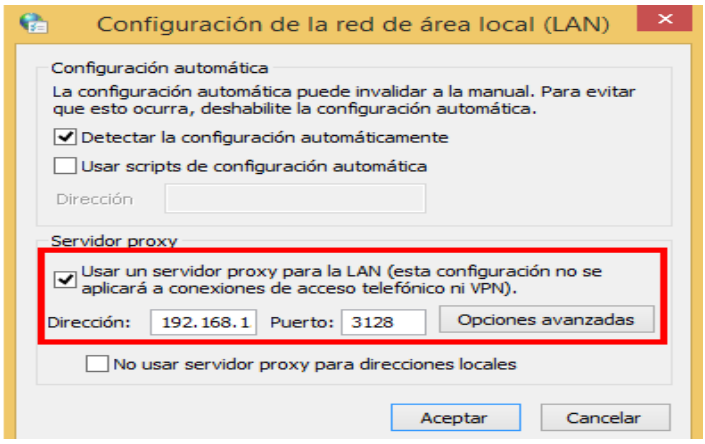
Se despliega una nueva interfaz de Propiedades: Internet en la cual se debe seleccionar el botón Configuración de LAN (Figura 164).

Figura 164. Interfaz Propiedades: Internet



Se debe activar la casilla Usar un servidor proxy para la LAN e ingresar la dirección IP del servidor 192.168.1.1 y el puerto por el cual está escuchando proxy 3128 como se muestra en la Figura 165.

Figura 165. Configuración de la red de área local



Con esta configuración ya es posible realizar la comprobación de las listas de control de acceso y las reglas establecidas en la configuración del proxy. Se

ingresa una URL en la cual está contenida la palabra mp3, la cual está definida como prohibida en el archivo de texto palabras.txt. El servidor deniega la petición y muestra la información de la Figura 166.

Figura 166. Denegación de acceso por palabras no deseadas en la URL

También se comprueba la denegación de acceso a la pagina web www.youtube.com, la cual se denegada por el archivo paginas.txt, ver la Figura 167.

Figura 167. Denegación de servicios por paginas no permitidas

4.16 CONFIGURACIÓN DEL SERVICIO DE RED FTP

Para disponer de un servidor FTP para la transferencia de archivos es necesario instalar la aplicación vsftpd, la cual se encuentra alojada en los repositorios oficiales del sistema operativo y puede ser descargada e instalada mediante el comando apt-get install vsftpd como se indica en la Figura 168.

Figura 168. Instalar aplicación vsftpd

```
root@servidorCapri:/home/administrador# apt-get install vsftpd
```

Una vez instalada la herramienta se debe realizar la configuración del archivo vsftpd.conf, el cual se puede encontrar en la ruta /etc/vsftpd.conf y se edita mediante el comando nano como se puede observar en la Figura 169.

Figura 169. Editar archivo de configuración vsftpd.conf

```
root@servidorCapri:/home/administrador# nano /etc/vsftpd.conf
```

En este archivo se puede encontrar toda la configuración necesaria para configurar el servidor. En él se debe especificar aspectos tales como los permisos que se otorgan a los usuarios como por ejemplo que los usuarios únicamente puedan realizar cambios en sus directorios personales. Es posible también, realizar una lista determinada de usuarios a los cuales se les limiten los cambios a dichos directorios, la cual debe ser especificada de igual manera en este archivo de configuración. Para realizar la configuración de estos parámetros se debe modificar las líneas que se muestran en la Figura 170.

Figura 170. Configurar permisos de usuario

```
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
```

Otra de las configuraciones importantes es que por defecto los usuarios únicamente pueden descargar archivos del servidor. Es posible modificar esta configuración para permitir a los usuarios subir archivos al servidor habilitando la línea write_enable=YES. Además, se puede permitir a un usuario en específico ser el propietario de los archivos que se cargan en el servidor editando las líneas que se muestran en la Figura 171.

Figura 171. Permitir la carga de archivos hacia el servidor

Al finalizar la modificación del archivo es necesario reiniciar el servicio ftp para llevar a cabo las modificaciones realizadas al archivo de configuración mediante el comando restart vsftpd mostrado en la Figura 172.

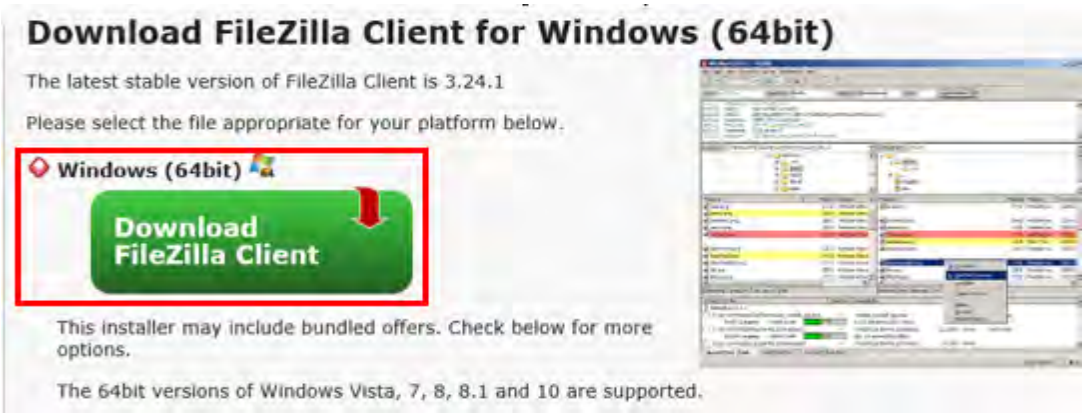
Figura 172. Reiniciar servicio vsftpd

Con los pasos realizados anteriormente, se ha finalizado la configuración del lado del servidor, para poder comenzar la transferencia de archivos es necesario descargar la aplicación FileZilla desde las maquinas Windows. Esta aplicación se puede descargar de la página oficial como lo indica la Figura 173.

Figura 173. Página oficial de la aplicación FileZilla

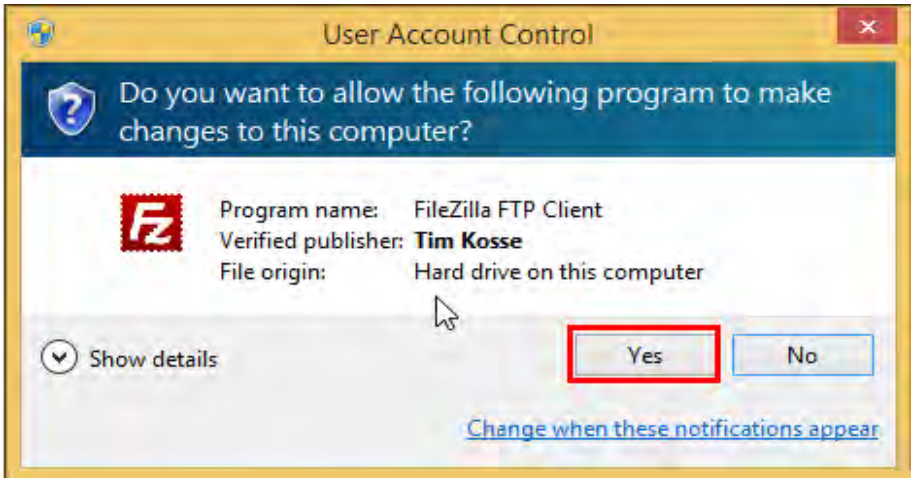
Se muestra una nueva página y en la cual se debe seleccionar la versión de 32-bits o 64-bits acorde al sistema operativo en el cual se está trabajando. En este caso se elige la versión de 64-bits como en la Figura 174.

Figura 174. Selección de versiones compatibles para Windows



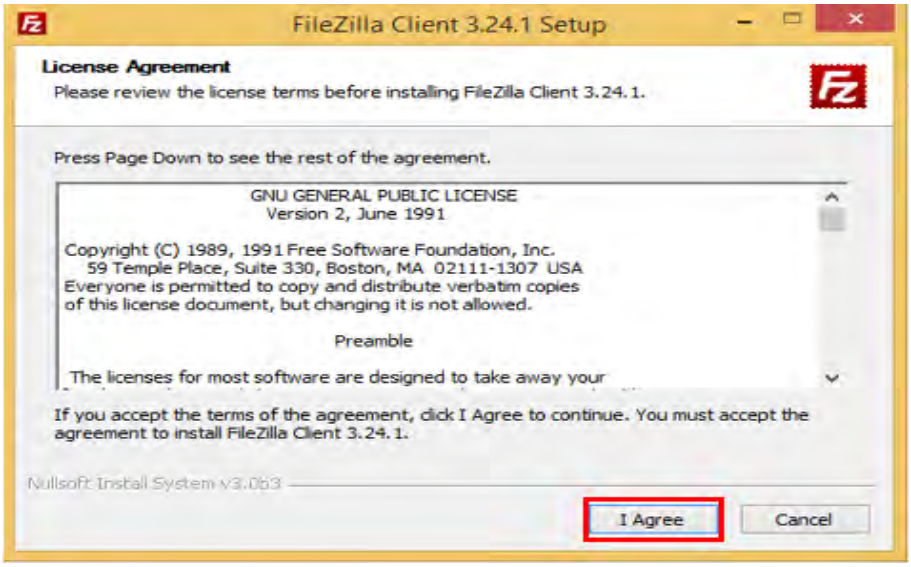
Una vez finalizada la descarga, se ejecuta el instalador de la aplicación la cual necesita permisos de control de usuario los cuales se aceptan presionando el botón Aceptar (Yes), ver Figura 175.

Figura 175. Control de cuentas de usuario



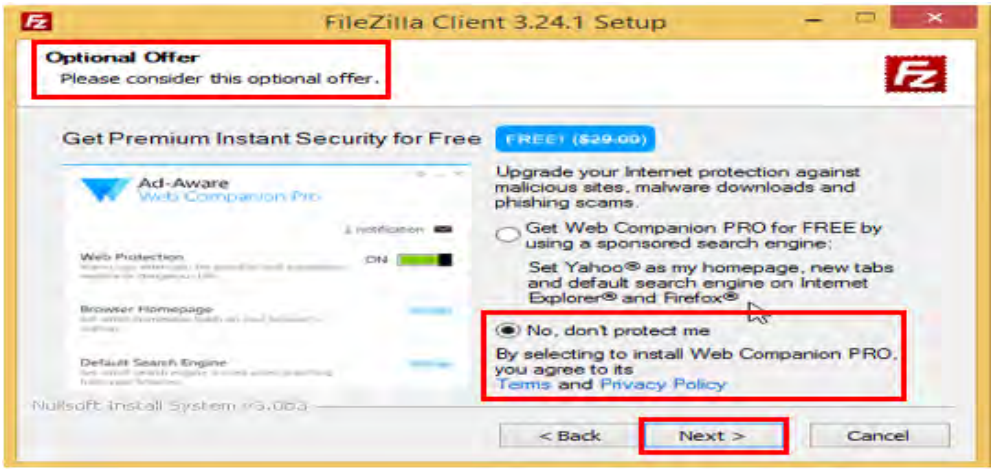
Aceptar los términos de licencia del programa en el botón Acepto (I Agree), ver Figura 176.

Figura 176. Aceptar términos de licencia FileZilla



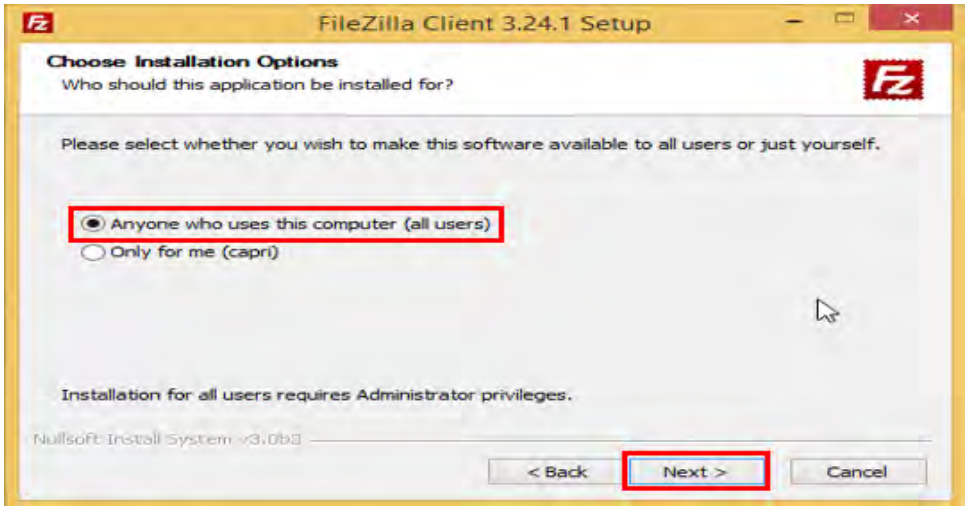
Es muy común que, en este tipo de programas gratuitos, se presenten ofertas de otros programas que no tienen nada que ver con la instalación del programa que se está instalando así que es recomendable leer muy bien lo que se instala y rechazar las ofertas que propone el instalador como se muestra la Figura 177.

Figura 177. Rechazar ofertas adicionales



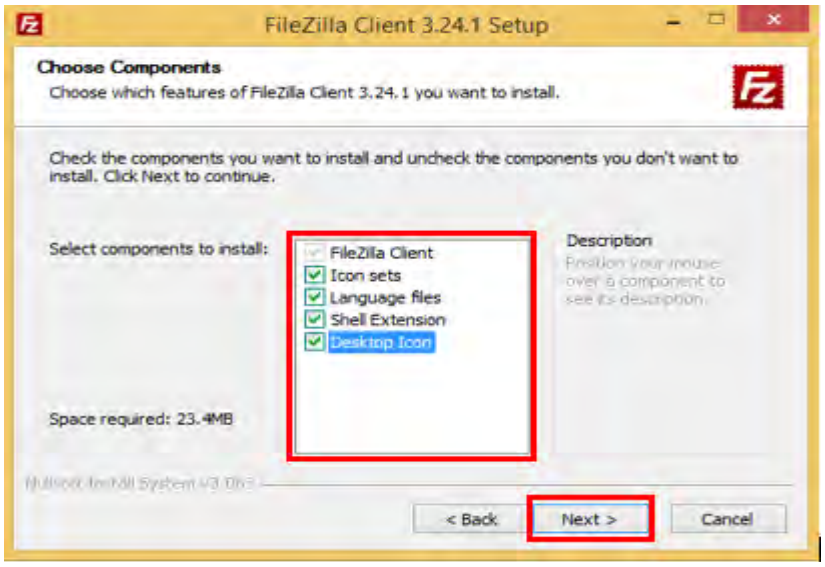
Siguiendo con el asistente de instalación se muestran las opciones para elegir a que cuentas de usuario creadas en Windows se les permite el uso de la aplicación. Escoger la opción Cualquiera que use este equipo (Anyone who uses this computer) y presionar el botón Siguiente (Next) como en la Figura 178.

Figura 178. Elegir cuentas de usuario



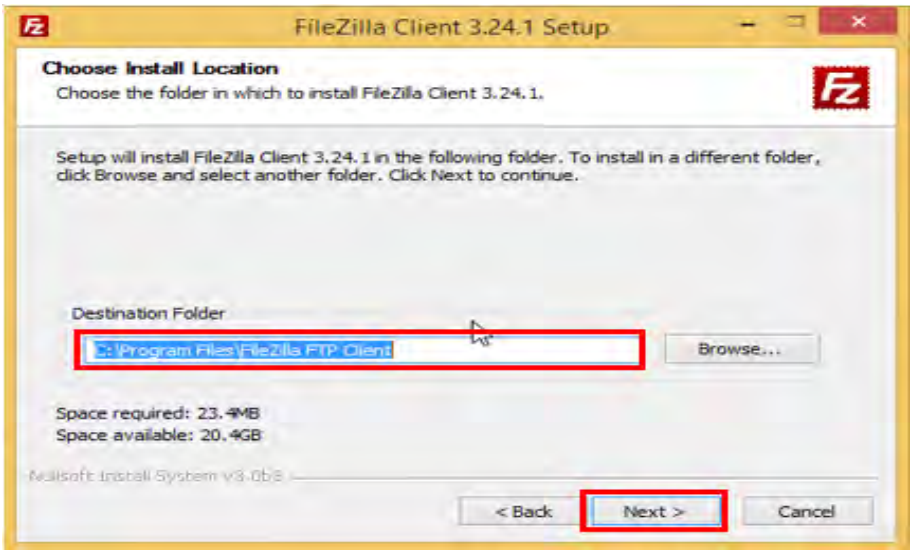
Luego, se muestra un listado de las características de la aplicación que se pueden instalar. Seleccionar todas las opciones y presionar el botón Siguiente (Next), ver Figura 179.

Figura 179. Componentes y características de la aplicación



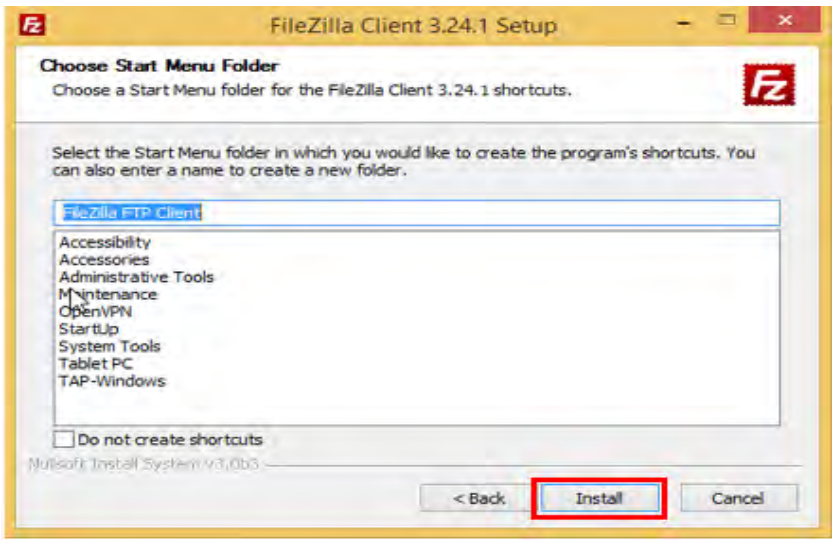
Seleccionar la ruta de instalación del programa la cual se recomienda dejarla por defecto como lo muestra la Figura 180 y presionar el botón Siguiente (Next):

Figura 180. Ruta de instalación FileZilla



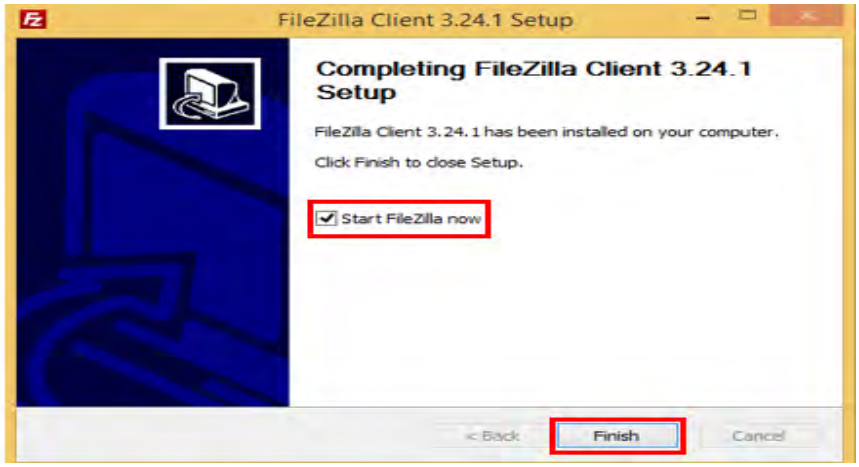
Escoger el directorio dentro del cual aparecerá el icono, el cual se debe dejar por defecto como lo indica la Figura 181. Hacer clic en el botón Instalar (Install) para comenzar la instalación:

Figura 181. Ubicación del icono de FileZilla



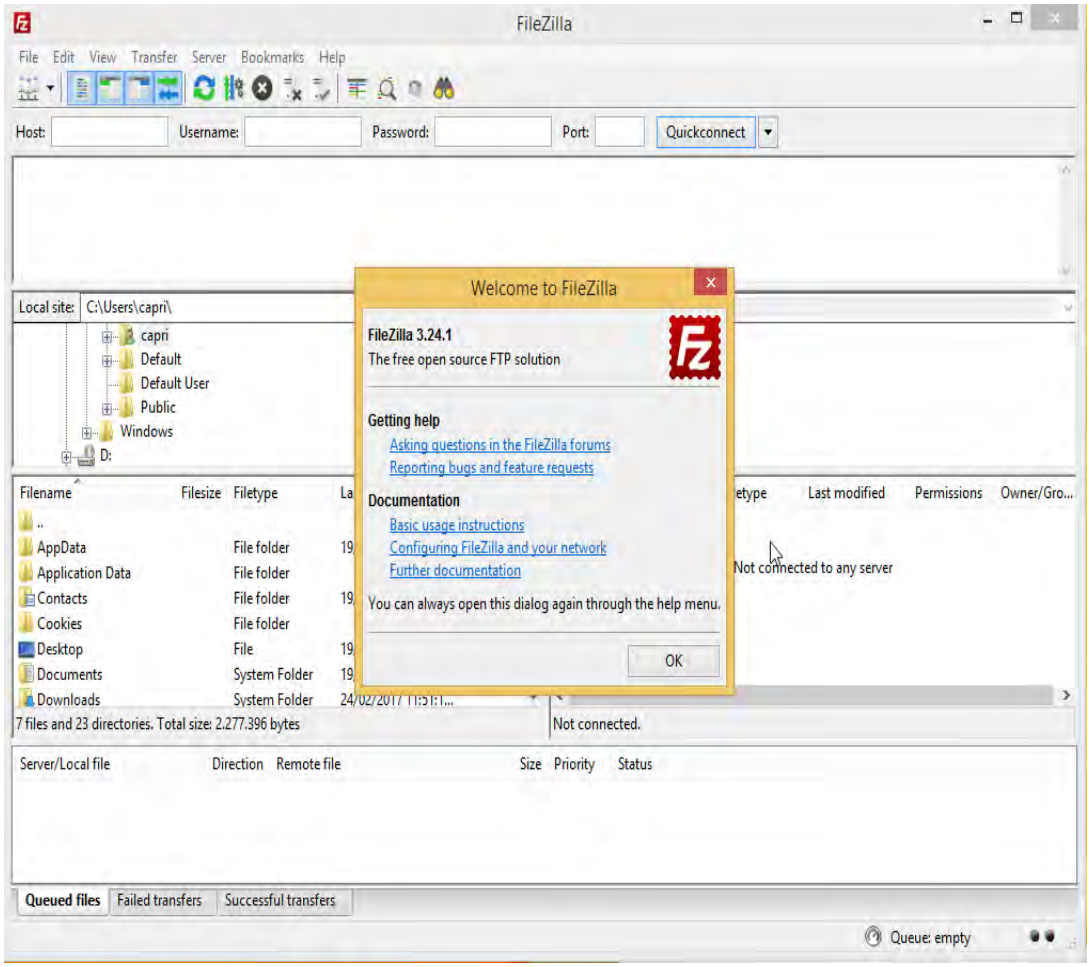
Al finalizar la instalación, se deja marcada la opción Start FileZilla now (Iniciar Filezilla ahora) y cerrar el asistente mediante el botón Finalizar (Finish), como en la Figura 182.

Figura 182. Finalizar la instalación de FileZilla



Como se observa en la Figura 183, se inicia la interfaz de la aplicación la cual tiene un aspecto como el siguiente:

Figura 183. Interfaz del programa FileZilla

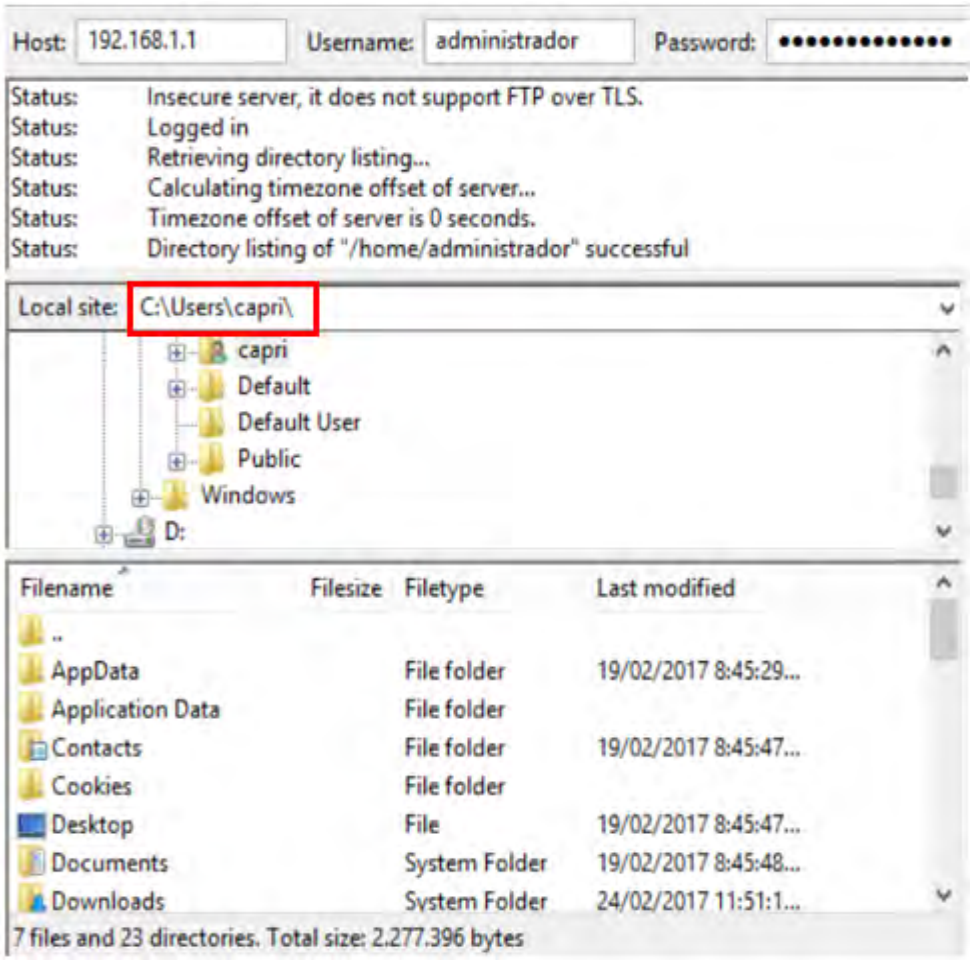


Para acceder al servidor se ingresa la dirección IP del servidor, el usuario con permisos definido en el archivo de configuración y su respectiva contraseña. También se debe especificar el puerto por el cual se debe ingresar, en caso de haberlo modificado. Una vez ingresada esta información presionar el botón Quickconnect. Ver Figura 184.

Figura 184. Conexión al servidor

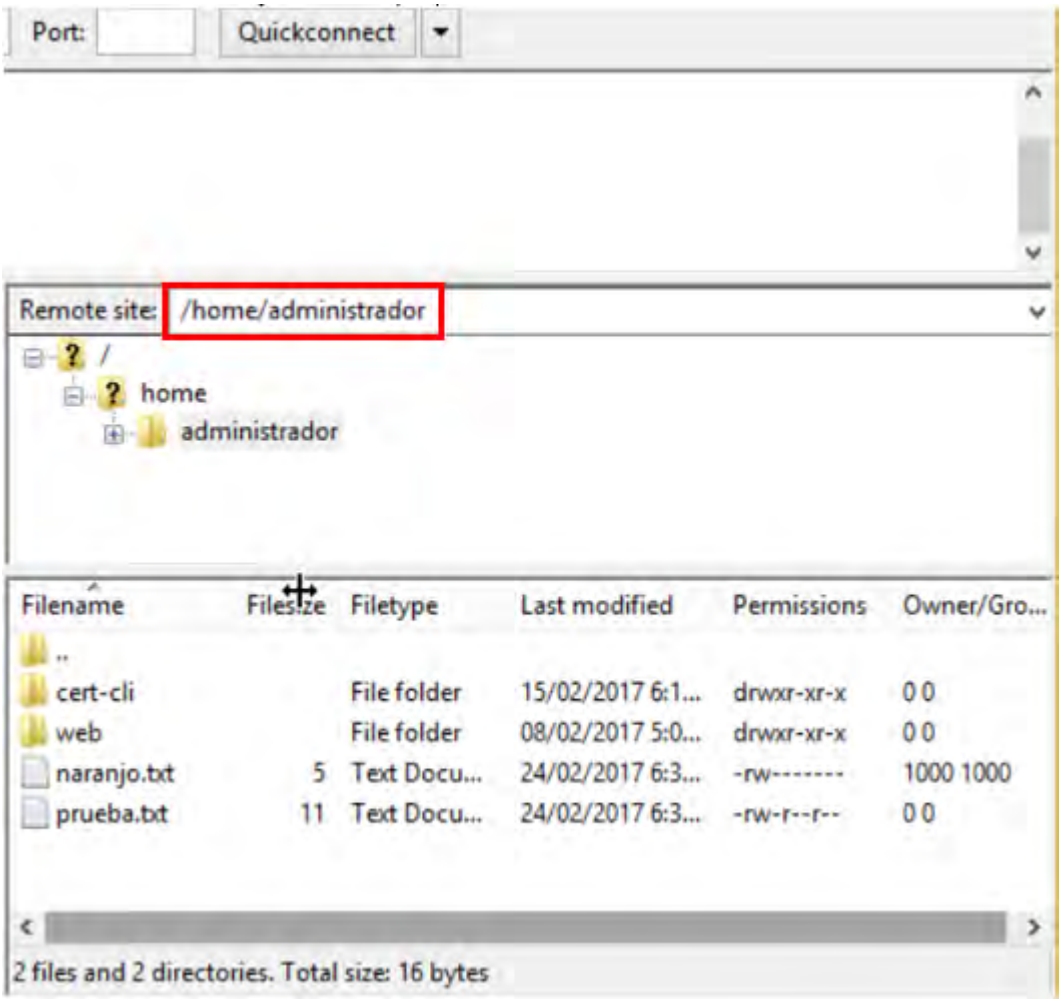
Si la conexión se realizó satisfactoriamente se mostrará del lado izquierdo de la pantalla todos los directorios y archivos presentes en la maquina Windows y que pueden ser transferidos al servidor, ver Figura 185.

Figura 185. Directorios y archivos presentes en la máquina Windows



Del lado derecho de la pantalla, como se muestra en la Figura 186, se encuentran los directorios y archivos disponibles para ser transferidos desde el servidor a la máquina Windows:

Figura 186. Directorios y archivos presentes en el servidor



4.17 CONFIGURACIÓN DEL SERVICIO DE RED SAMBA

Para instalar un servidor de archivos mediante la aplicación samba se ejecuta el comando que se observa en la Figura 187, en el cual se instalan tanto la aplicación como algunas herramientas que son necesarias para su funcionamiento. Todas estas herramientas son descargadas de los repositorios oficiales del sistema operativo.

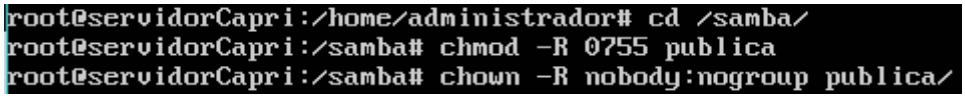
Figura 187. Instalar aplicación samba

Ahora se deben crear los directorios a compartir entre los usuarios del sistema, se crea un directorio con el nombre de pública, el cual será visible y al que tendrán acceso todos los usuarios de la red. Para crear el directorio se utiliza el comando mkdir como lo muestra la Figura 188.

Figura 188. Crear directorio compartido publica

Se debe ubicar en el directorio samba y se modifican los permisos que se le otorgan al directorio público como se observa en la Figura 189.

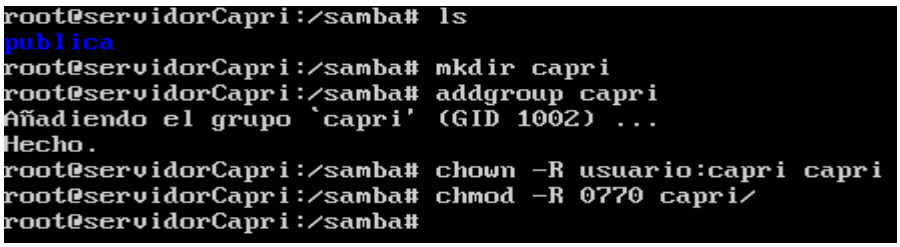
Figura 189. Modificar permisos del directorio publica



También es posible compartir un directorio con un grupo determinado de usuarios. Para el acceso a estos directorios es necesario la autenticación de usuario, lo cual crea un nivel de seguridad para la información contenida en ellos.

Para esto se crea el directorio que se desea compartir, el grupo al cual tiene acceso el directorio, se agregan los usuarios al grupo junto con el directorio a compartir y por último se brindan los permisos necesarios al directorio, como se observa en la Figura 190.

Figura 190. Crear y configurar directorio capri



Ahora, como se muestra en la Figura 191, se debe unir el usuario al grupo creado capri.

Figura 191. Añadir usuarios al grupo capri

```
root@servidorCapri:/samba# usermod -a -G capri usuario
```

Además, es necesario crear una contraseña para el usuario agregado, ver Figura 192.

Figura 192. Añadir contraseña para el usuario

```
root@servidorCapri:/samba# smbpasswd -a usuario
New SMB password:
Retype new SMB password:
Added user usuario.
```

Siguiendo todos los pasos anteriores de creación de directorio seguro se ha creado el directorio administrador y el grupo admcapri. Además, se ha añadido al usuario administrador al grupo capri para que pueda compartir también sus archivos en ese directorio. Esto se realiza como lo muestra la Figura 193.

Figura 193. Agregar usuario administrador al grupo capri

```
root@servidorCapri:/samba# chown -R administrador:capri capri
root@servidorCapri:/samba# usermod -a -G capri administrador
```

Una vez creados los directorios y concediendo los respectivos permisos se edita el archivo de configuración smb.conf mediante el comando nano como en la Figura 194.

Figura 194. Editar archivo de configuración smb.conf

```
root@servidorCapri:/samba# nano /etc/samba/smb.conf _
```

Se debe ubicar la sección [global] y después de sus parámetros de configuración, se añade la configuración para los directorios a compartir que se crearon anteriormente. Entre los parámetros a configurar en estas secciones están la ruta en la que se crearon los directorios, si desea permitir el acceso al directorio,

permitir la creación de archivos dentro de los directorios y los usuarios que tendrán acceso a los directorios seguros, como se muestra en la Figura 195.

Figura 195. Configuración de directorios en el archivo smb.conf

```
#Carpeta publica
[publica]
path = /samba/publica
browsable = yes
writable = yes
guest ok = yes
read only = no

#Carpeta privada usuarios capri
[capri]
path = /samba/capri
valid users = @capri
guest ok = no
writable = yes
browsable = yes

#Carpeta privada administrador capri
[administrador]
path = /samba/administrador
valid users = @admcapri
guest ok = no
writable = yes
browsable = yes
```

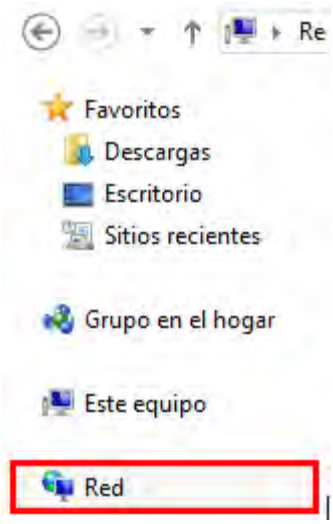
Al finalizar de editar el archivo de configuración se debe reiniciar el servicio samba para que las nuevas configuraciones empiecen a funcionar. Para esto se utiliza el comando service smbd restart como se observa en la Figura 196.

Figura 196. Reiniciar servicio samba

```
root@servidorCapri:/samba# service smbd restart
smbd stop/waiting
smbd start/running, process 1544
```

Para verificar el funcionamiento del servicio samba, debe acceder desde una maquina Windows de la red y dirigirse al explorador de archivos y en la parte izquierda de la pantalla seleccionar la pestaña Red, ver Figura 197.

Figura 197. Ver equipos conectados en la red

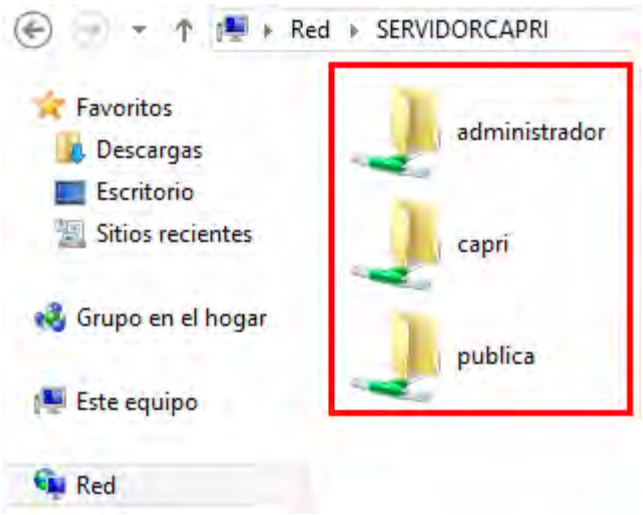


Aparece un icono como el que se muestra en la Figura 198, con el nombre de SERVIDORCAPRI sobre el cual se accede con doble clic:

Figura 198. Listado de equipos conectado a red

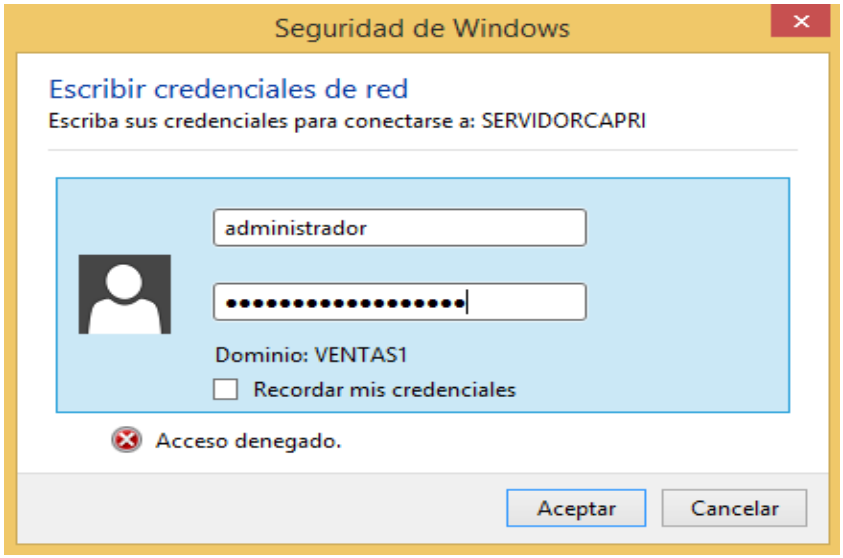
Dentro del servidor ya se encuentran los directorios publica, capri y administrador, visibles para todos los usuarios, pero necesitará autenticación para poder acceder a los directorios seguros capri y administrador, ver Figura 199.

Figura 199. Directorios compartidos



Para ingresar a los directorios seguros, se introduce el nombre de usuario y la contraseña del usuario, ver Figura 200.

Figura 200. Autenticación de usuarios

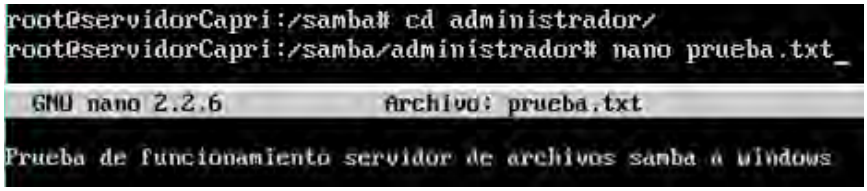


Una vez autenticado el usuario, ya se puede obtener acceso al directorio administrador, ver Figura 201.

Figura 201. Directorio administrador

Para verificar el funcionamiento de la transferencia de archivos, se crea un archivo de nombre prueba.txt en el directorio administrador desde el servidor como lo muestra la Figura 202.

Figura 202. Archivo de texto prueba.txt



Y se comprueba la creación del archivo en la máquina Windows, ver Figura 203 y Figura 204.

Figura 203. Listado de archivos del directorio administrador

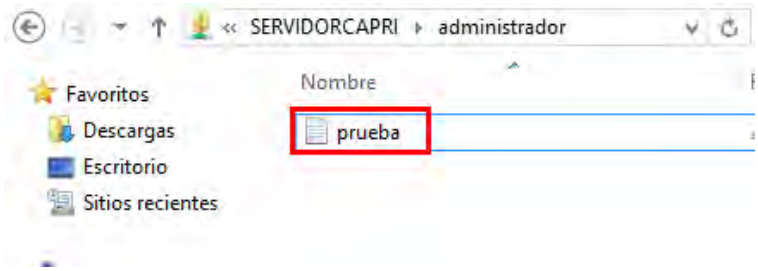
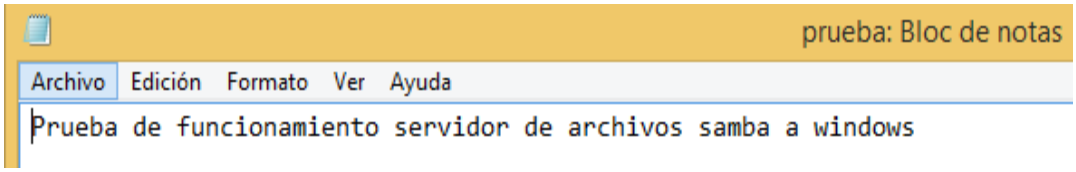
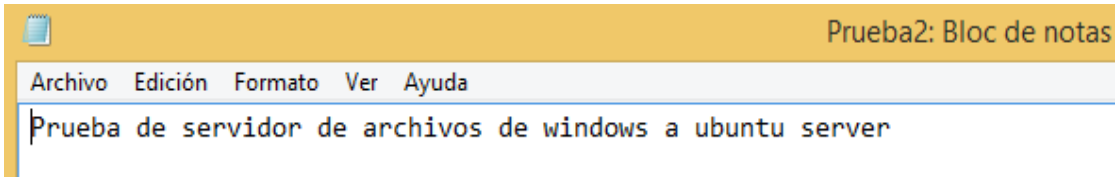


Figura 204. Archivo de texto prueba.txt en Windows



Del mismo modo se crea un archivo desde la maquina Windows con el nombre Prueba2.txt dentro del directorio administrador, ver Figura 205.

Figura 205. Archivo de texto Prueba2.txt



Y posteriormente, se comprueba en el servidor la creación del archivo como lo muestran la Figura 206 y la Figura 207.

Figura 206. Listado de archivos del directorio administrador

Figura 207. Archivo de texto Prueba2.txt en el servidor

4.18 CONFIGURACIÓN DEL SERVICIO DE RED VPN

Para instalar una red virtual privada (VPN) para la empresa mediante la aplicación OpenVPN se debe ejecutar el comando apt-get install openvpn con el cual empieza la descarga desde los repositorios oficiales de Ubuntu, ver Figura 208.

Figura 208. Instalar aplicación openvpn

Además, se debe que instalar una herramienta llamada bridge-utils para permitir la interacción de la VPN con la red local. Para instalar esta herramienta se utiliza el comando apt-get install bridge-utils, como se muestra en la Figura 209.

Figura 209. Instalar herramienta bridge-utils

También es necesaria la creación de dos scripts bridge-start.sh y bridge-stop para la configuración en modo puente de la tarjeta de red. Estos scripts, se crean con el comando nano como se observa en la Figura 210 y la Figura 211.

Figura 210. Crear script bridge-start.sh

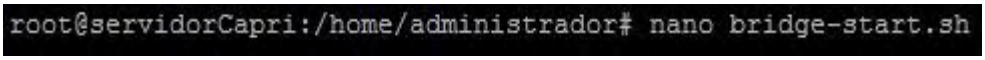
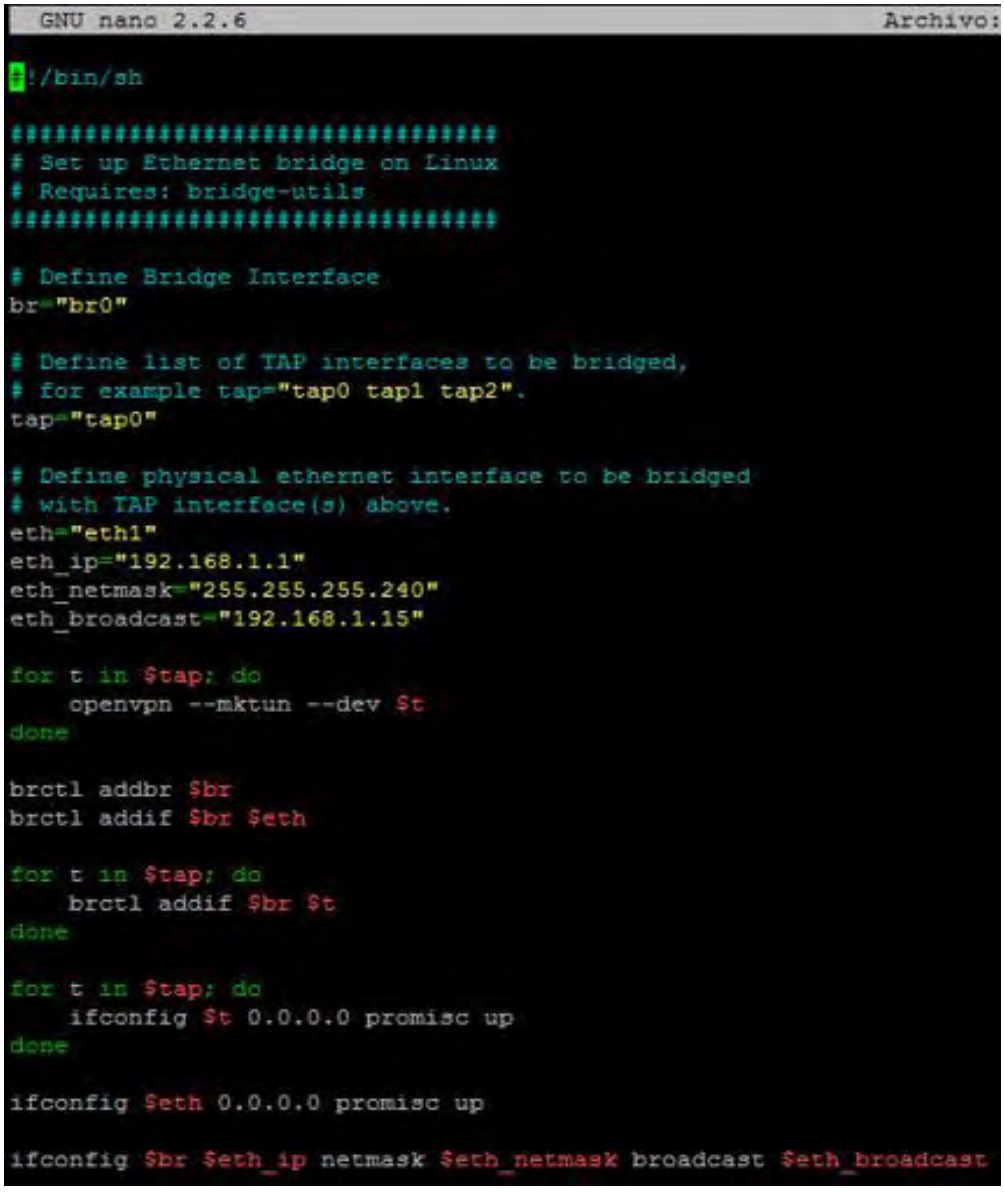


Figura 211. Crear script bridge-stop.sh

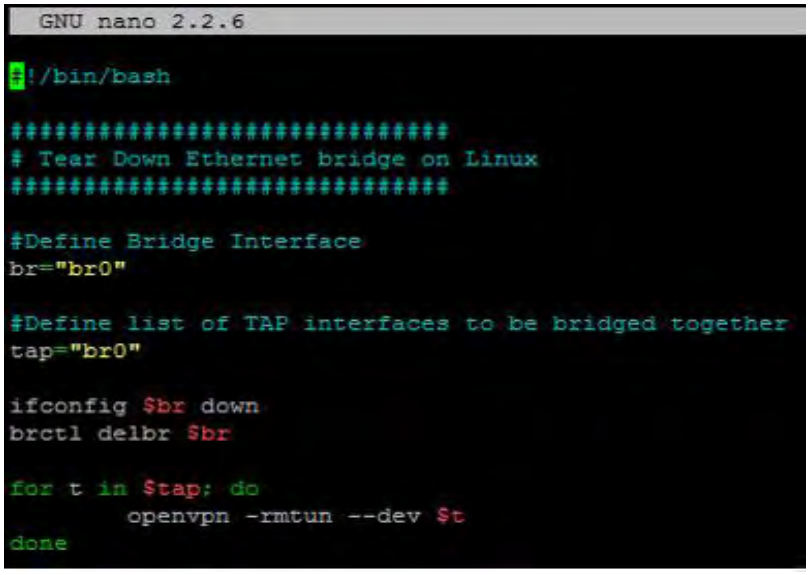
Dentro del script bridge-start.sh se deben especificar valores como: Los nombres del túnel y puente que se crearán, la tarjeta de red mediante la cual se va a realizar el puente, el direccionamiento IP configurado en dicha tarjeta de red, activar el modo promiscuo, entre otros. Esta configuración se puede observar en la Figura 212.

Figura 212. Script bridge-start.sh



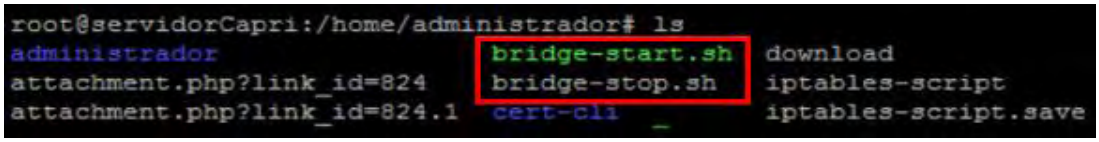
El script bridge-stop.sh sirve para remover la configuración creada para el túnel y puente especificada en el archivo anterior y se lo utiliza al finalizar la sesión de la VPN. El archivo debe contener la información indicada en la Figura 213.

Figura 213. Script bridge-stop.sh



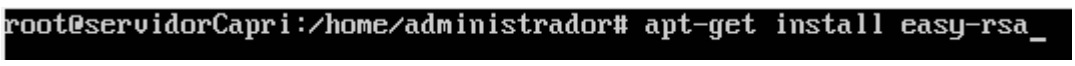
Finalmente se puede comprobar la creación de los scripts mediante el comando ls, ver Figura 214.

Figura 214. Listado de archivos del directorio administrador



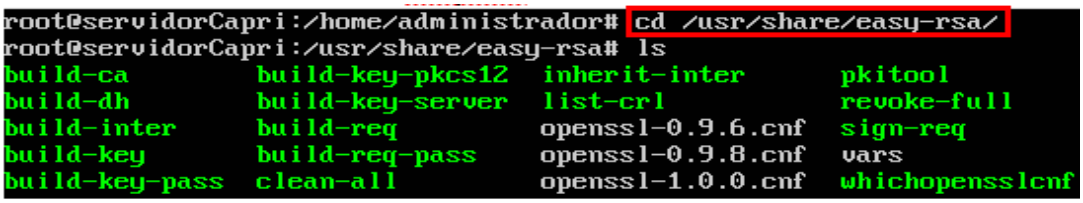
Ahora se debe realizar la Configuración de Autoridad de Certificación. Para esto se debe utilizar una herramienta llamada easy-rsa, la cual es la encargada de generar los diferentes certificados que necesita OpenVPN para su autenticación. La Figura 215, muestra el comando apt-get install easy-rsa mediante el cual se instala la aplicación.

Figura 215. Instalar easy-rsa



Al finalizar la instalación, se debe ubicar en el directorio easy-rsa para ver los archivos y directorios que contiene. Este directorio se encuentra en la ruta /usr/share/easy-rsa como se indica en la Figura 216.

Figura 216. Contenido del directorio easy-rsa

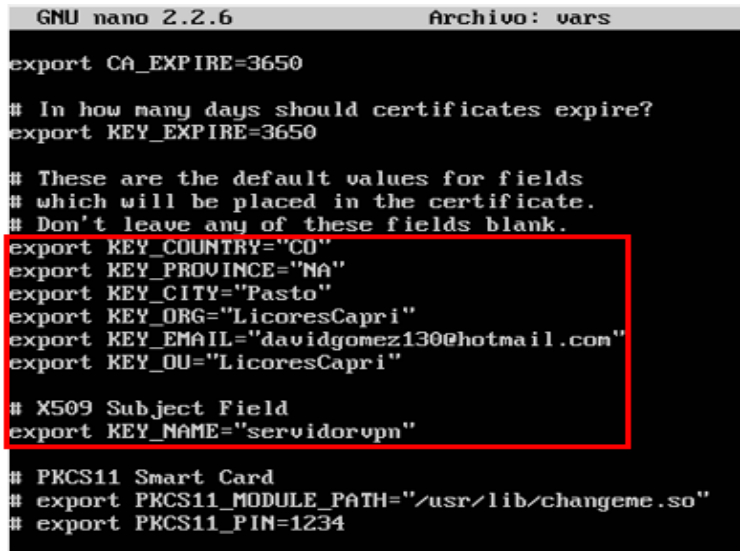


Editar el archivo vars con el comando nano vars como se muestra en la Figura 217, para generar la autoridad de certificación(CA), el certificado y la clave:

Figura 217. Editar archivo vars

Dentro de este archivo se debe ubicar la sección de información del certificado como se muestra en la Figura 218, y modificar los valores por defecto para agregar la información correspondiente a la ubicación, dirección de correo electrónico y nombre de la organización con las que se configura el certificado.

Figura 218. Archivo de configuración vars



Se debe utilizar el comando source vars para ejecutar el uso de la plantilla vars las cuales se modifican anteriormente, ver Figura 219.

Figura 219. Utilizar plantilla vars

```
root@servidorCapri:/usr/share/easy-rsa# source vars
```

También se ejecuta el comando ./clean-all para limpiar cualquier certificado que exista, en caso de no existir ningún certificado se creará el directorio keys para almacenar los certificados que vamos a crear, como se muestra en la Figura 220.

Figura 220. Crear directorio de publicación de certificados

```
root@servidorCapri:/usr/share/easy-rsa# ./clean-all
root@servidorCapri:/usr/share/easy-rsa# ls
build-ca            build-key-server  list-crl            sign-req
build-dh            build-req         openssl-0.9.6.cnf   vars
build-inter         build-req-pass    openssl-0.9.8.cnf   whichopensslcnf
build-key           clean-all         openssl-1.0.0.cnf
build-key-pass      inherit-inter     pkitool
build-key-pkcs12    keys              revoke-full
```

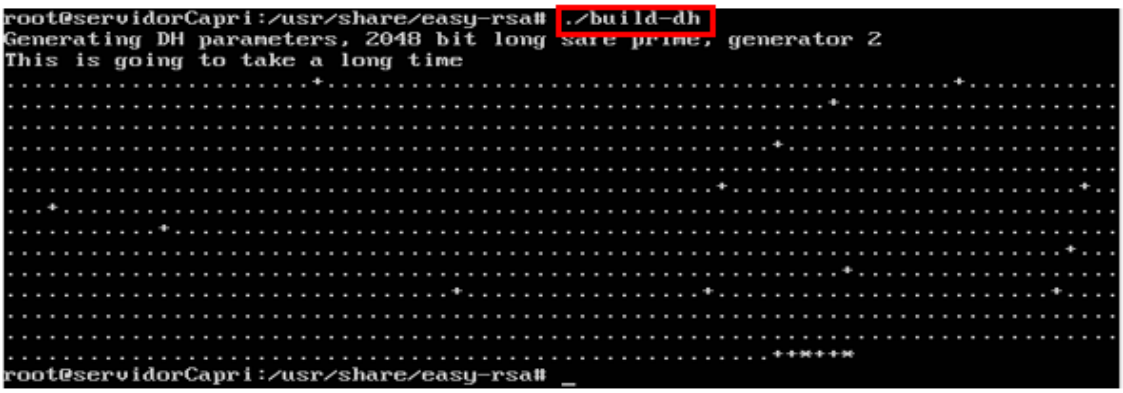
Para construir la autoridad de certificación se ejecuta el comando ./build-ca. Aparecen las opciones que se muestran en la Figura 221, las cuales deben dejarse por defecto presionando la tecla Enter.

Figura 221. Construir autoridad de certificación

```
root@servidorCapri:/usr/share/easy-rsa# ./build-ca
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CO]:
State or Province Name (full name) [NA]:
Locality Name (eg, city) [Pasto]:
Organization Name (eg, company) [LicoresCapri]:
Organizational Unit Name (eg, section) [LicoresCapri]:
Common Name (eg, your name or your server's hostname) [LicoresCapri CA]:
Name [servidorvpn]:
Email Address [davidgomez130@hotmail.com]:
root@servidorCapri:/usr/share/easy-rsa#
```

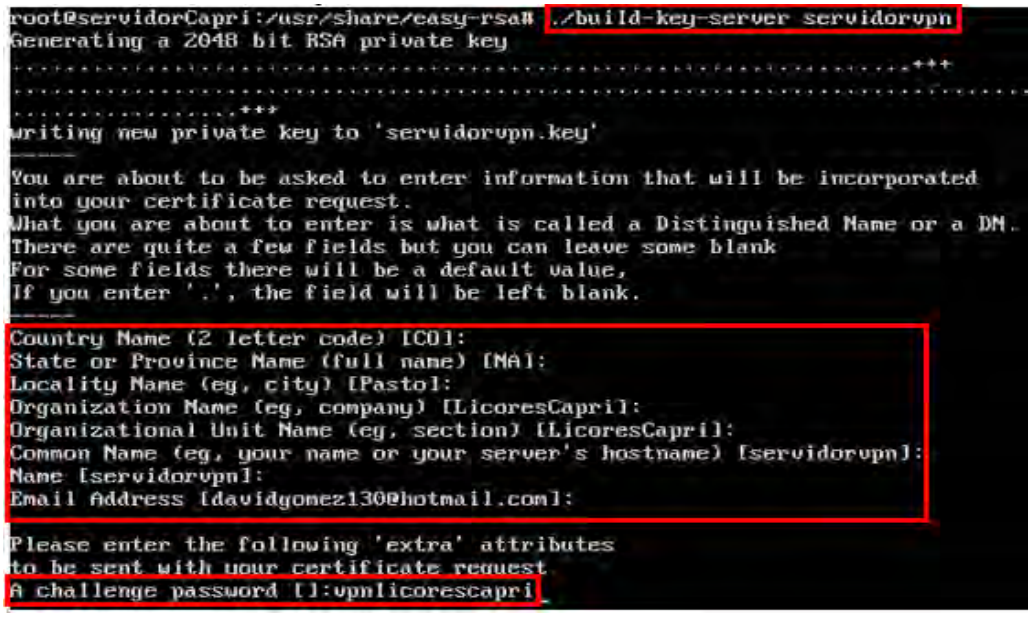
Para generar los parámetros de seguridad Deffie-Hellman, se debe ejecutar el comando ./build-dh. Esto tomará al menos un minuto y en la pantalla se muestra la creación del archivo como se observa en la Figura 222.

Figura 222. Definición de parámetros Deffie-Hellman



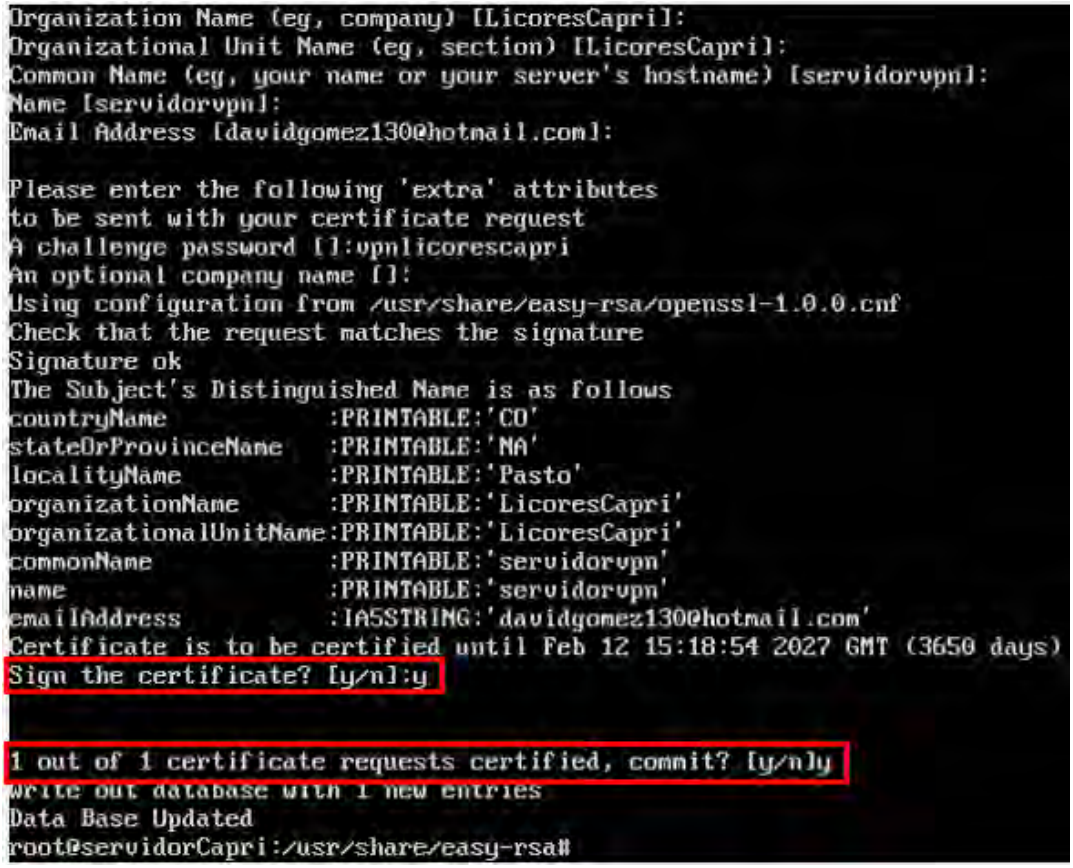
Ahora hay que generar un certificado y la clave privada para el servidor, para esto se usa el comando ./build-key-server servidorvpn. Se debe aceptar los valores predeterminados a excepción de la opción challenge password en donde se digita una contraseña de seguridad, ver Figura 223.

Figura 223. Crear certificados y claves del servidor



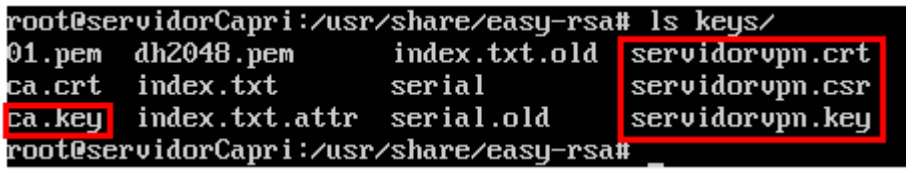
Luego se debe firmar el certificado y confirmar la creación del certificado presionando la letra y cuando lo requiera como se indica en la Figura 224.

Figura 224. Firmar certificados de autenticación



Al finalizar este proceso, ya se han generado los certificados y las claves, se han guardado en el directorio keys, como se observa en la Figura 225.

Figura 225. Certificados y claves de servidor



Estos archivos generados deben permanecer protegidos ya que el equipo que desee conectarse, necesita de estos certificados además de la dirección IP del servidor para conectarse a la VPN, por lo cual se realiza una copia en un directorio diferente como se muestra en el ejemplo de la Figura 226.

Figura 226. Copia de seguridad de los certificados

```
root@servidorCapri:/usr/share/easy-rsa# cd keys/
root@servidorCapri:/usr/share/easy-rsa/keys# cp servidorvpn.crt servidorvpn.key
dh2048.pem ca.crt /etc/openvpn
```

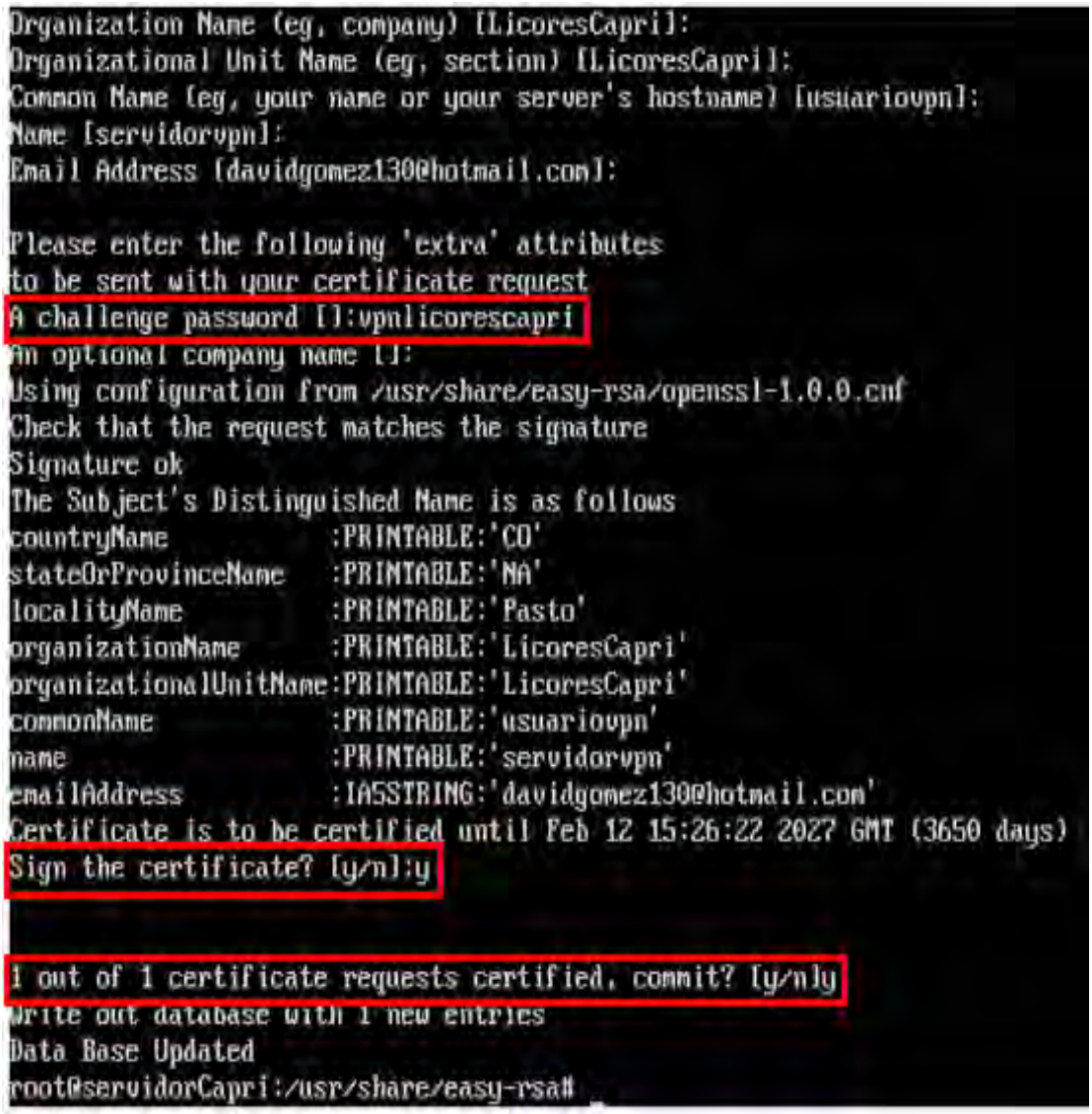
Es necesario crear también un certificado para el cliente, el cual servirá para autenticarse en el servidor. Por seguridad, se crea un certificado para cada cliente. Para ello se usa los comandos source vars y ./build-key usuariovpn, como en la Figura 227.

Figura 227. Certificados para clientes

```
root@servidorCapri:/usr/share/easy-rsa/keys# cd ../
root@servidorCapri:/usr/share/easy-rsa# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /usr/share/easy-rsa/ke
ys
root@servidorCapri:/usr/share/easy-rsa# ./build-key usuariovpn
Generating a 2048 bit RSA private key
.....................+++
...........+++
writing new private key to 'usuariovpn.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Al igual que en el anterior certificado se escoge una contraseña y se firma el certificado, lo demás debe quedar por defecto, ver Figura 228.

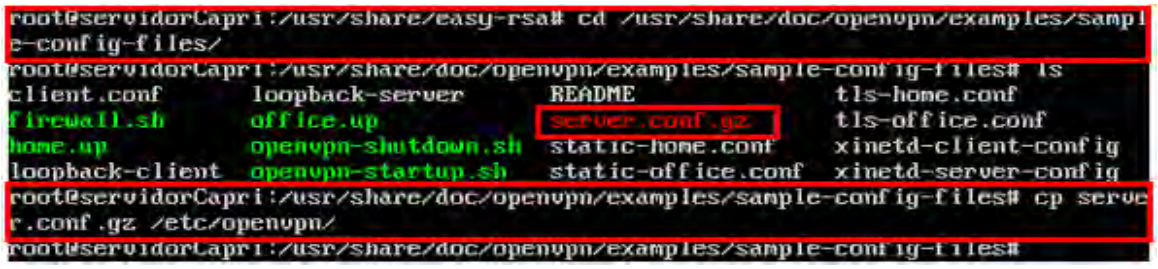
Figura 228. Firma de certificados de cliente



Hasta aquí, ya se han generado los certificados de autenticación tanto del servidor como de los clientes. Ahora, se debe configurar el servidor para la creación de la VPN.

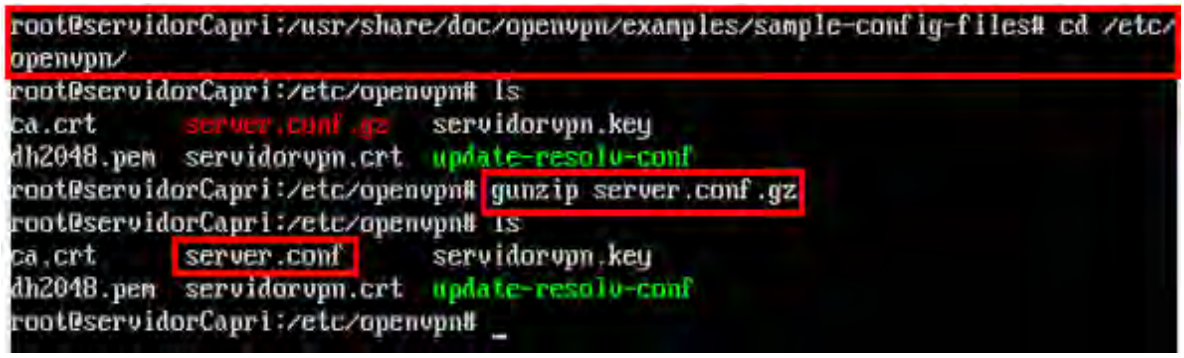
Para configurar el servidor VPN se copia el ejemplo de archivo de configuración llamado server.conf.gz desde la ruta /usr/share/doc/example/openvpn/simple-config-files hacia el directorio /etc/openvpn, tal como se muestra en la Figura 229.

Figura 229. Copiar archivo de configuración server.conf



Una vez realizada la copia, dirigirse al directorio en donde se copió el archivo y descomprimirlo con el comando gunzip, ver Figura 230.

Figura 230. Extraer archivo de configuración server.conf

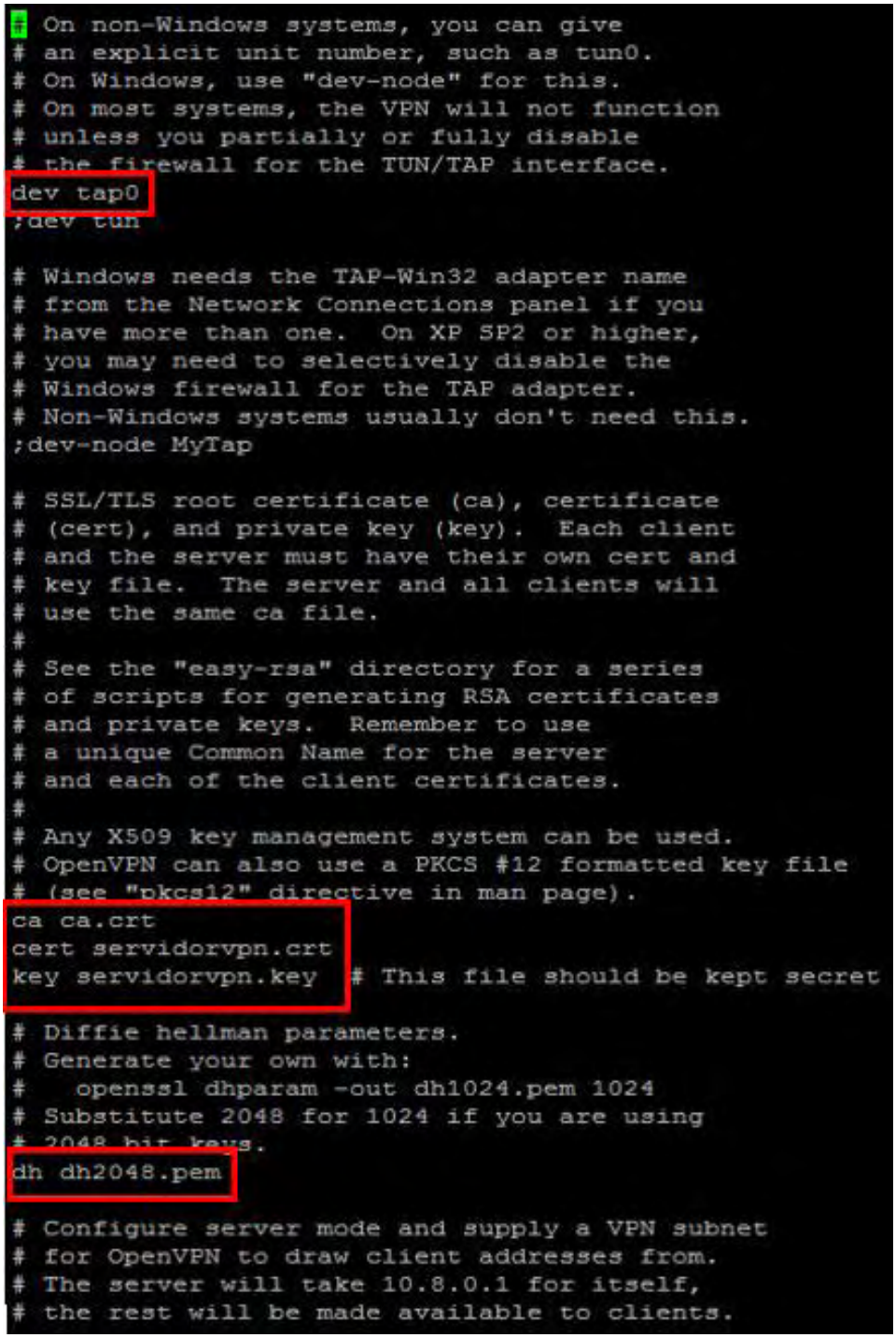


Para editar el archivo se hace uso del comando nano –c server.conf como lo muestra la Figura 231.

Figura 231. Editar archivo de configuración server.conf

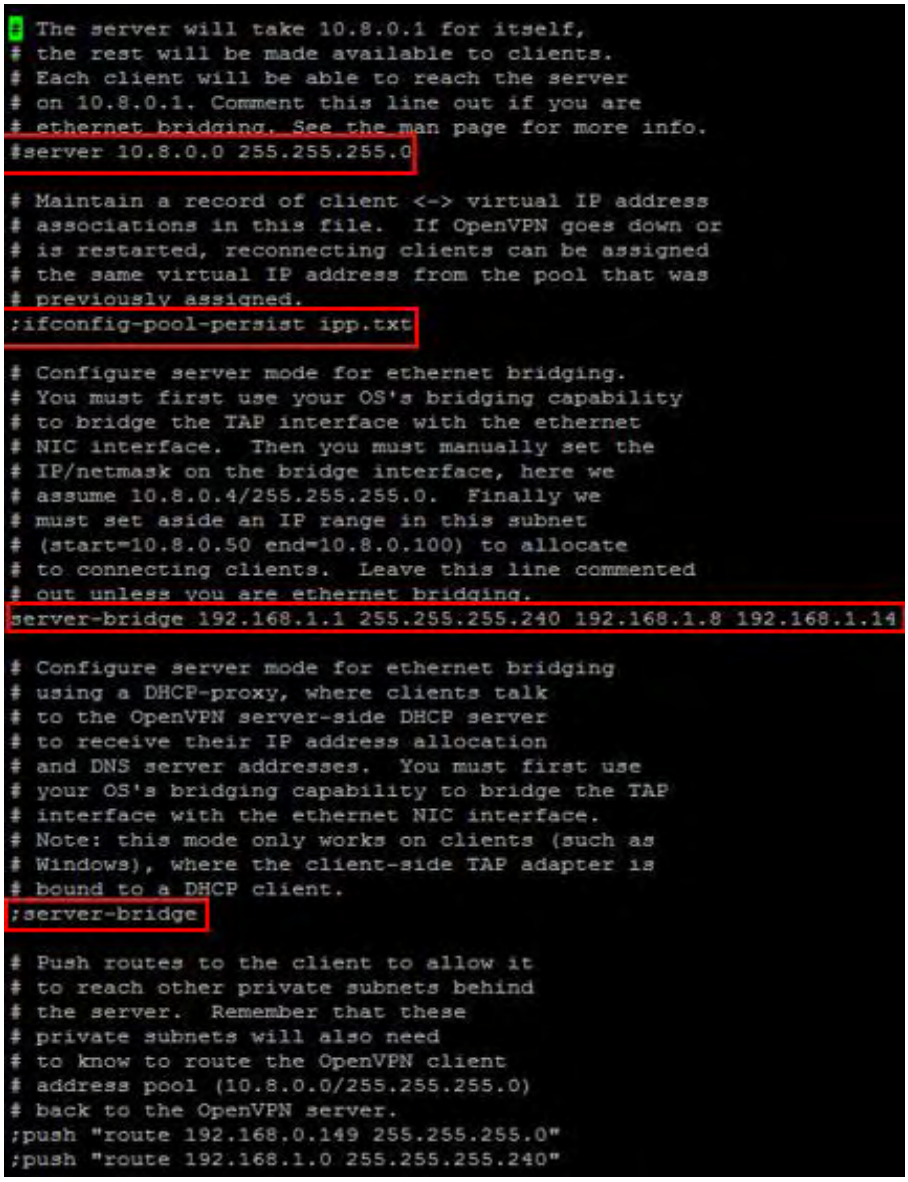
La configuración de este archivo es muy importante, aquí se deben añadir reglas de seguridad, de direccionamiento IP de la VPN, el método de encriptamiento de las llaves, los certificados a utilizar en el servidor, entre otros. En la Figura 232, Figura 233, Figura 234 y Figura 235, se muestra la configuración realizada para la creación de la VPN de la empresa.

Figura 232. Archivo de configuración server.conf 1



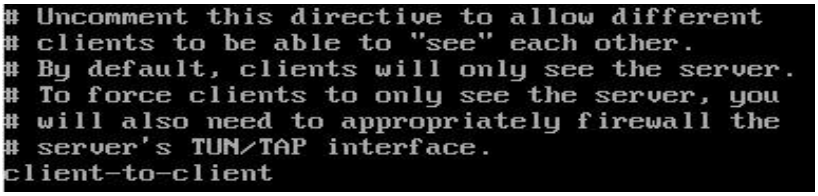
```
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap0
;dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert servidorvpn.crt
key servidorvpn.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh2048.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
```

Figura 233. Archivo de configuración server.conf 2



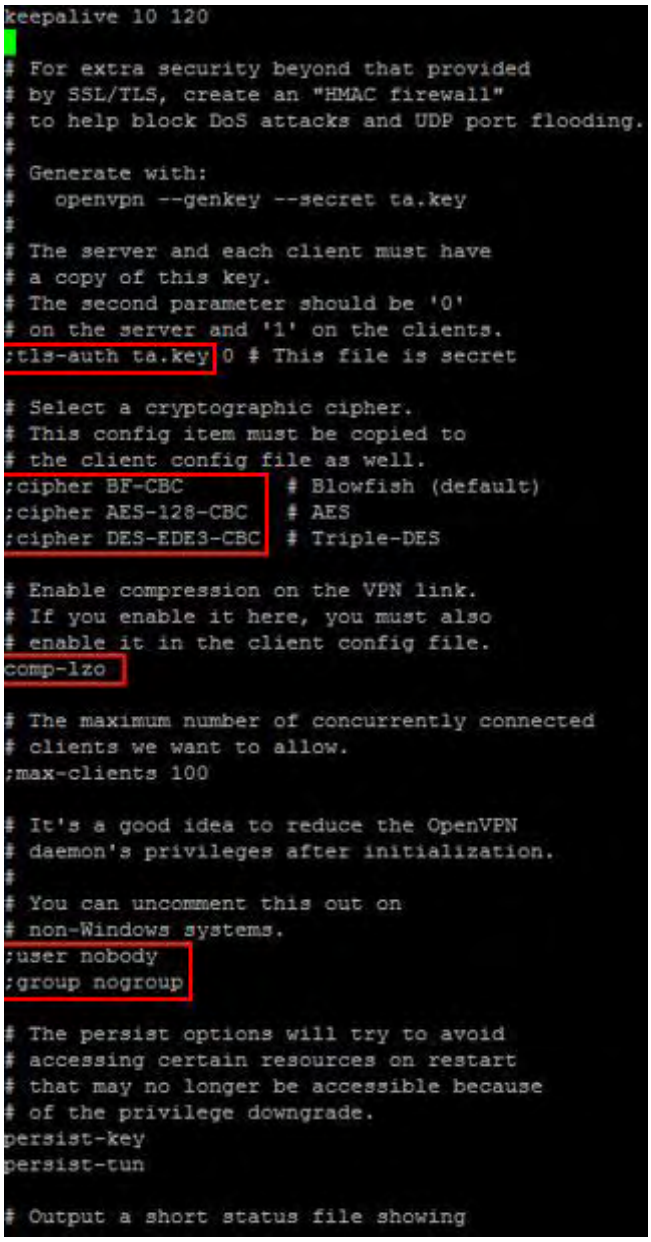
```
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
#server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
;ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
server-bridge 192.168.1.1 255.255.255.240 192.168.1.8 192.168.1.14

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.0.149 255.255.255.0"
;push "route 192.168.1.0 255.255.255.240"
```

Figura 234. Archivo de configuración server.conf 3



```
# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client
```

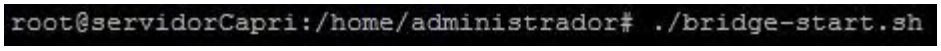
Figura 235. Archivo de configuración server.conf 4.



```
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
```

Una vez editados los parámetros de configuración del servidor se debe ejecutar los scripts que se crearon en la primera parte e iniciar el servicio de OpenVPN. Es muy importante tener en cuenta el orden de estos comandos ya que de esto depende la implementación del puente de manera correcta. Primero se ejecuta el script bridge-start.sh como en la Figura 236.

Figura 236. Ejecutar script bridge-start.sh



Ahora se debe iniciar el servidor VPN con el comando service openvpn start, ver Figura 237.

Figura 237. Iniciar servicio openvpn

En caso de necesitar detener el servicio se debe detener primero el servidor VPN de la siguiente manera, ver Figura 238.

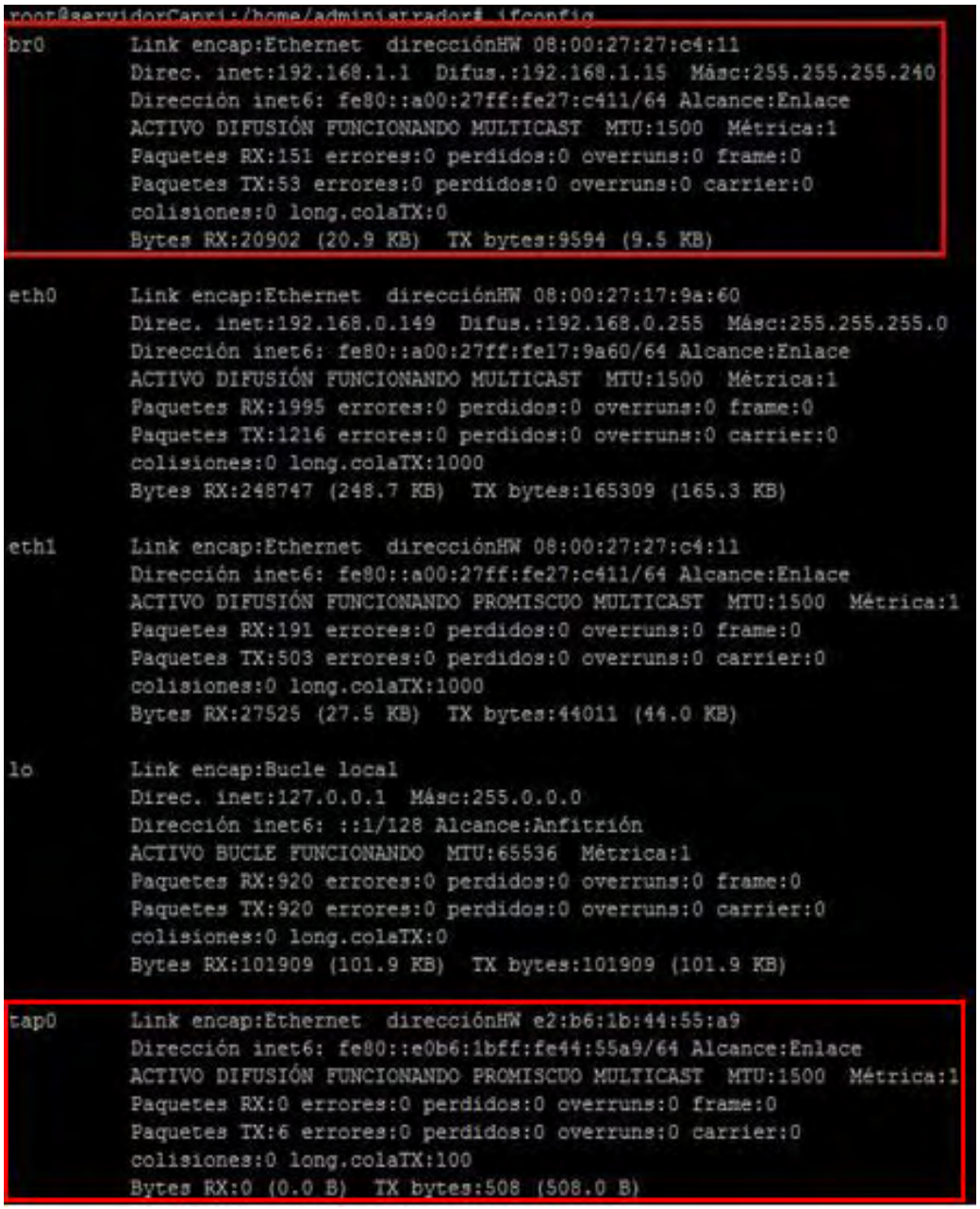
Figura 238. Detener servicio openvpn

Y finalmente, se ejecuta el script bridge-stop para detener el servicio de puente, como lo indica la Figura 239.

Figura 239. Ejecutar script bridge-stop.sh

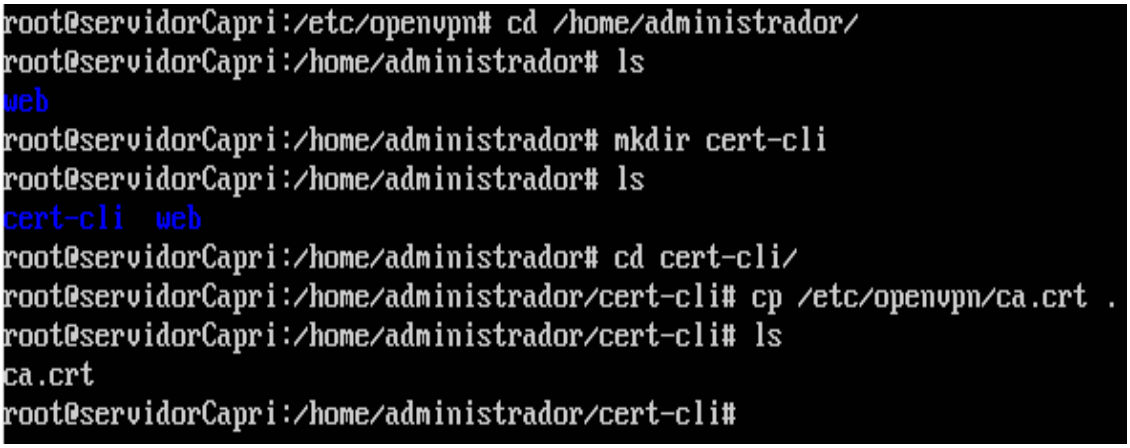
Una vez iniciado el servicio, se debe verificar la creación del puente para proporcionar el direccionamiento IP del servidor DHCP mediante el comando ifconfig, como se muestra en la Figura 240.

Figura 240. Configuración de las tarjetas de red del servidor



Para configurar el cliente se debe copiar los certificados y las claves creadas en los pasos anteriores, para facilitar este proceso se crea un directorio llamado cert-cli en donde se copiarán los certificados como lo muestra la Figura 241.

Figura 241. Crear directorio de certificados para el cliente



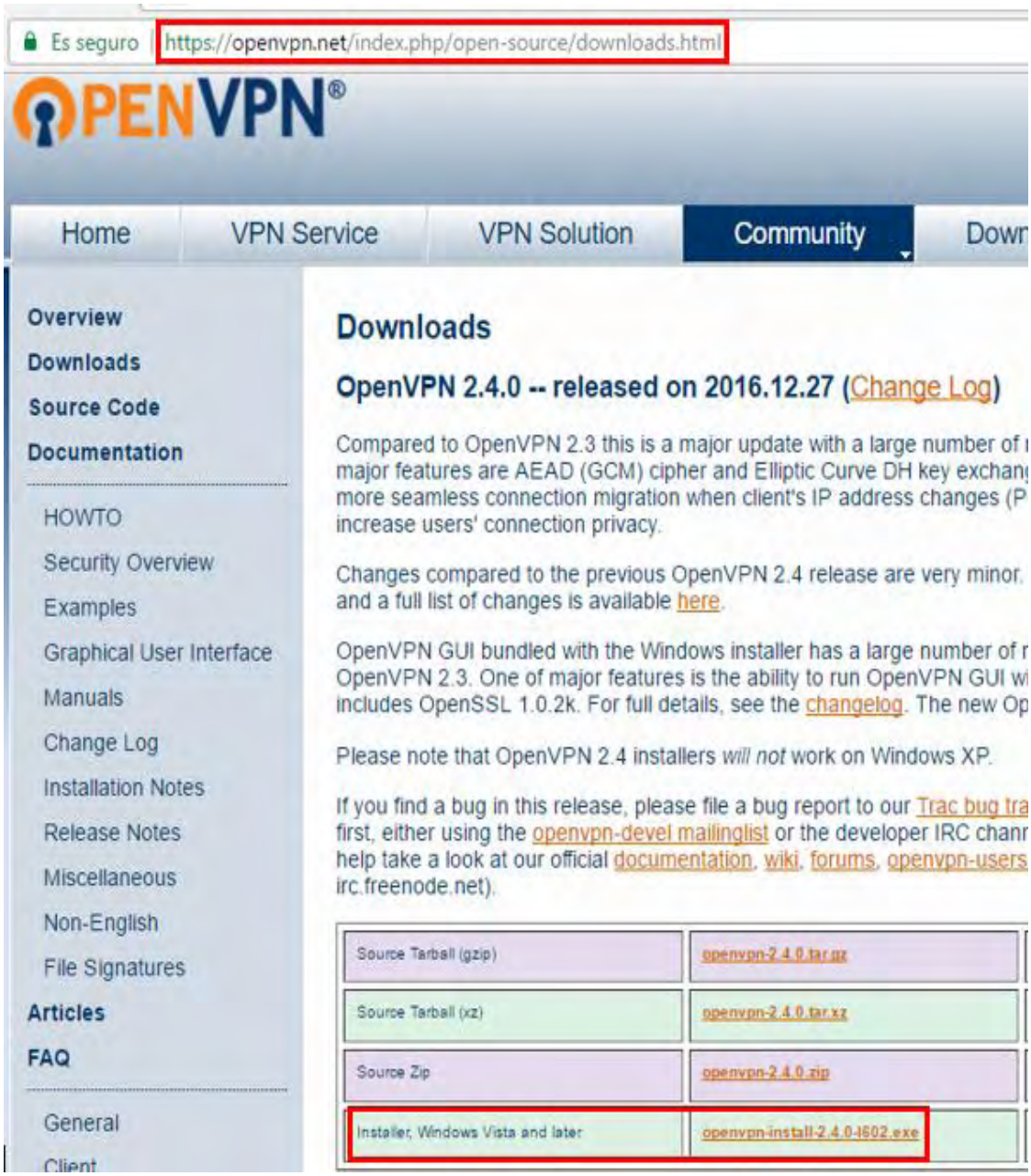
Repetir este proceso para los otros certificados y claves, ver Figura 242.

Figura 242. Copiar certificados de cliente al directorio cert-cli

Ahora se debe transferir el directorio cert-cli al cliente por alguno de los diferentes medios de transferencia como una memoria USB.

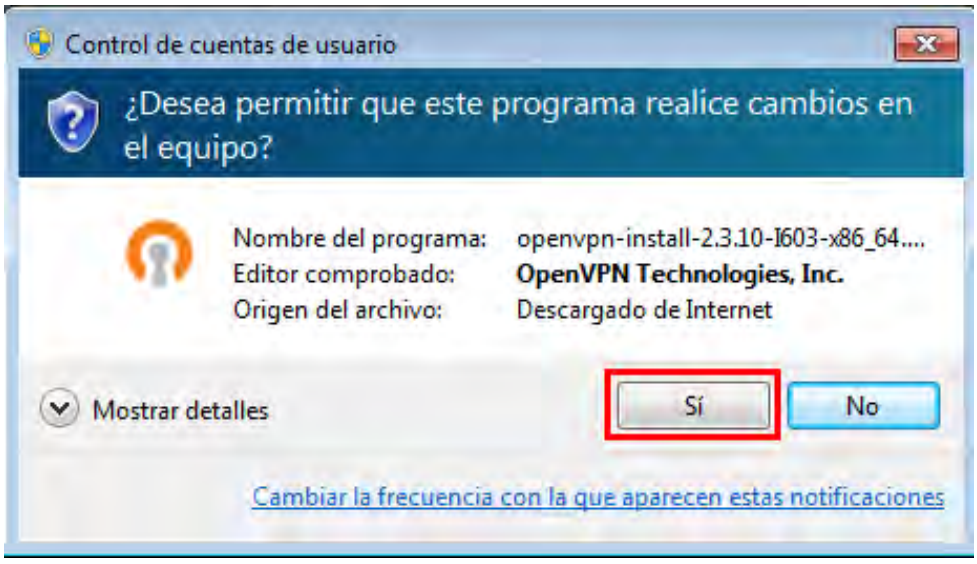
Para empezar a hacer uso de la red virtual privada, desde una maquina cliente Windows se debe descargar la aplicación OpenVPN de su página principal en la sección de Descargas y escoger la versión correspondiente al sistema operativo de la máquina, como se indica en la Figura 243.

Figura 243. Sección de descargas de la página oficial de la aplicación OpenVNP



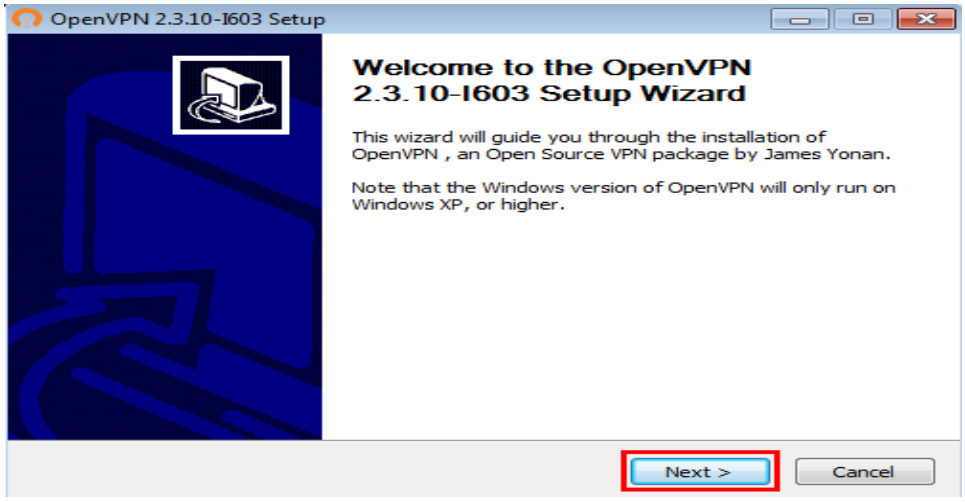
Una vez descargado, se debe ejecutar el instalador y aceptar que el programa se instale en la ventana de control de cuentas de usuario, como se muestra en la Figura 244.

Figura 244. Control de cuentas de usuario



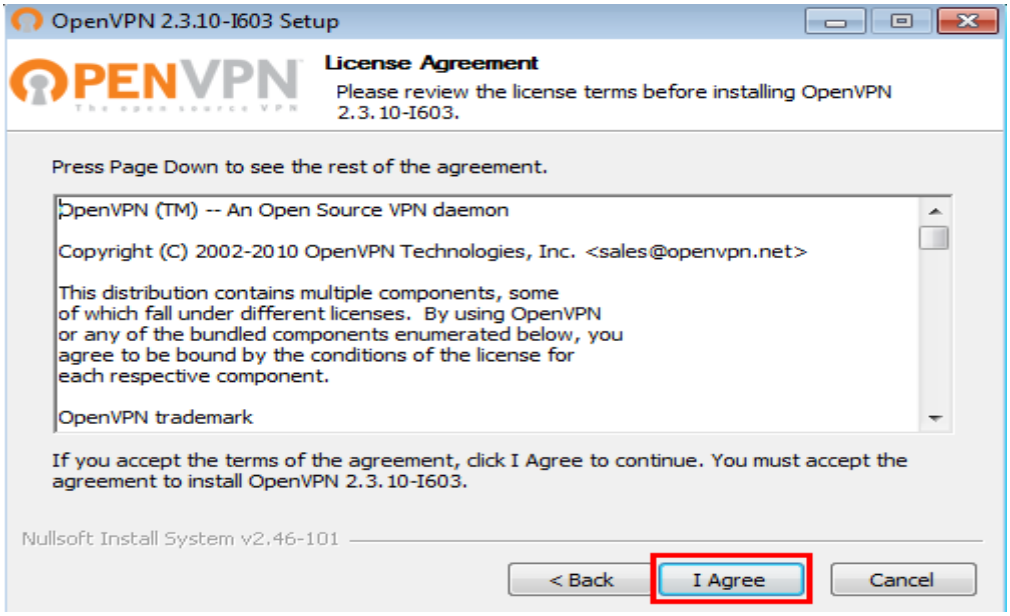
Se abrirá un asistente de instalación y se debe escoger la opción Next, ver la Figura 245.

Figura 245. Asistente de instalación OpenVPN.



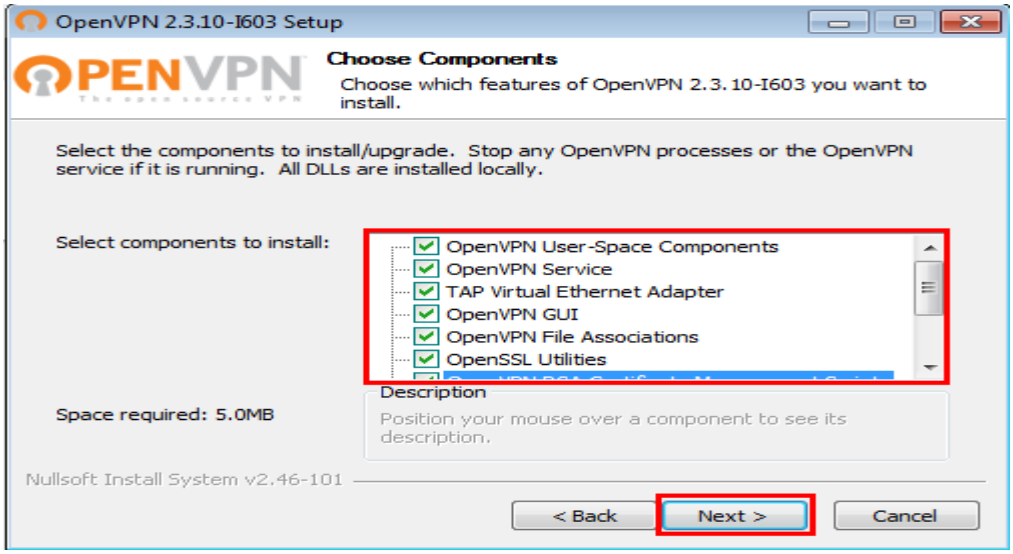
Aceptar los términos del contrato en la opción I Agree, ver Figura 246.

Figura 246. Acuerdo de licencia de la aplicación OpenVPN



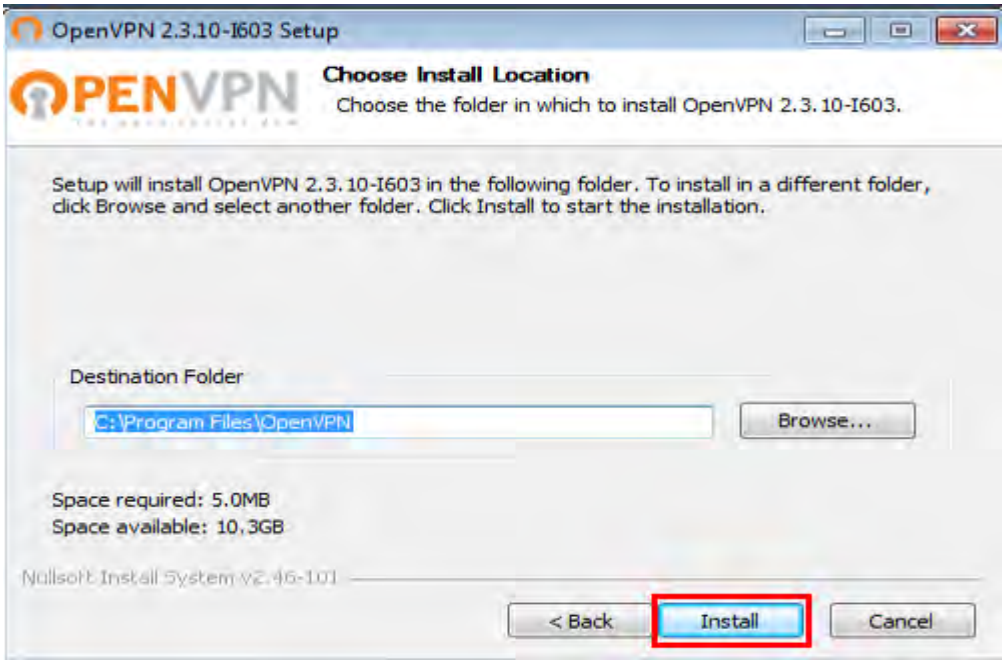
Seleccionar todas las opciones de componentes a instalar y hacer clic en Next, ver Figura 247.

Figura 247. Listado de componentes de la aplicación OpenVPN



Hacer clic en Install y esperar que finalice la instalación, ver Figura 248.

Figura 248. Ruta de instalación de la aplicación OpenVPN

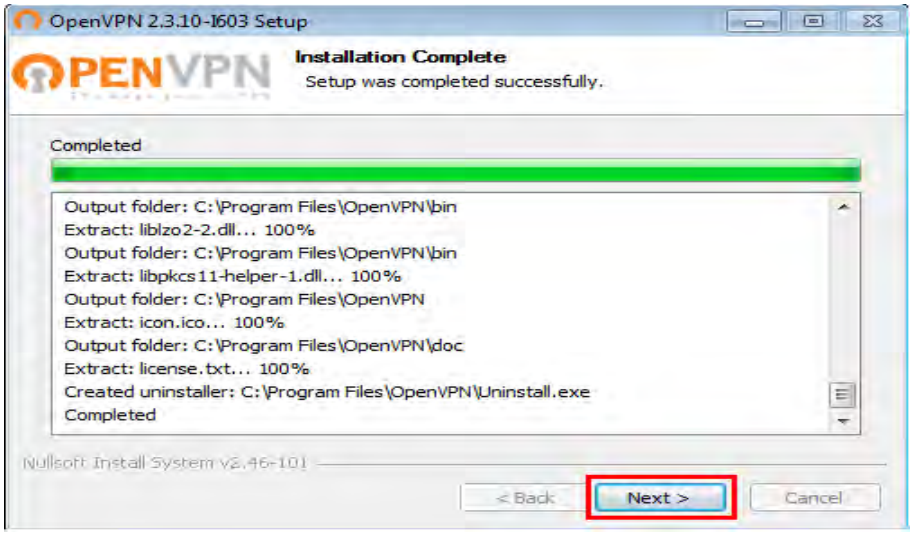


Escoger la opción Instalar, ver Figura 249.

Figura 249. Alerta de seguridad de Windows

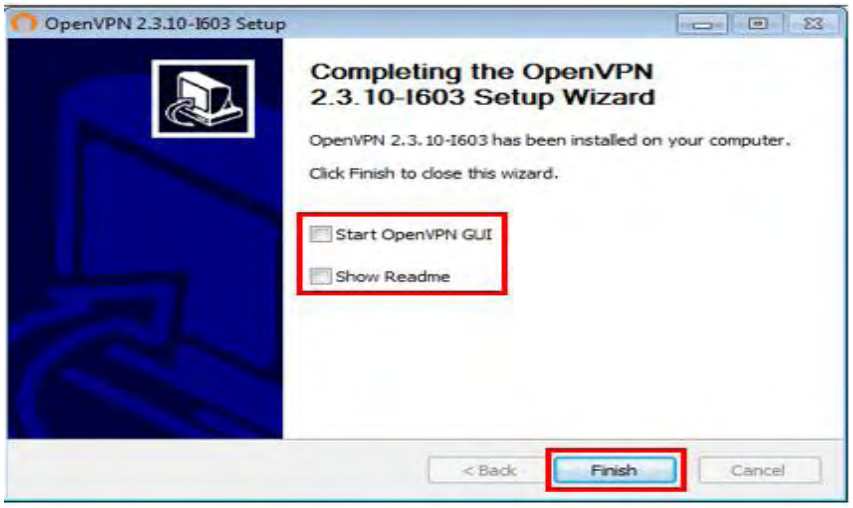
Una vez finalizada la instalación hacer clic en Next, ver Figura 250.

Figura 250. Instalación de la aplicación OpenVPN



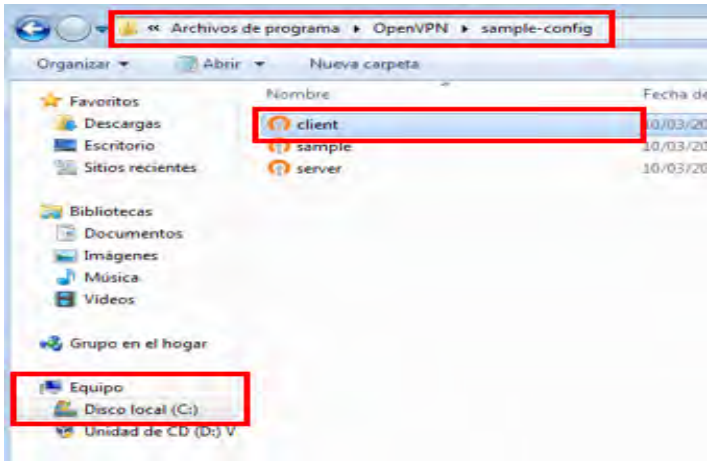
Desmarcar las dos casillas y hacer clic en Finish, ver Figura 251.

Figura 251. Finalizar instalación de la aplicación OpenVPN



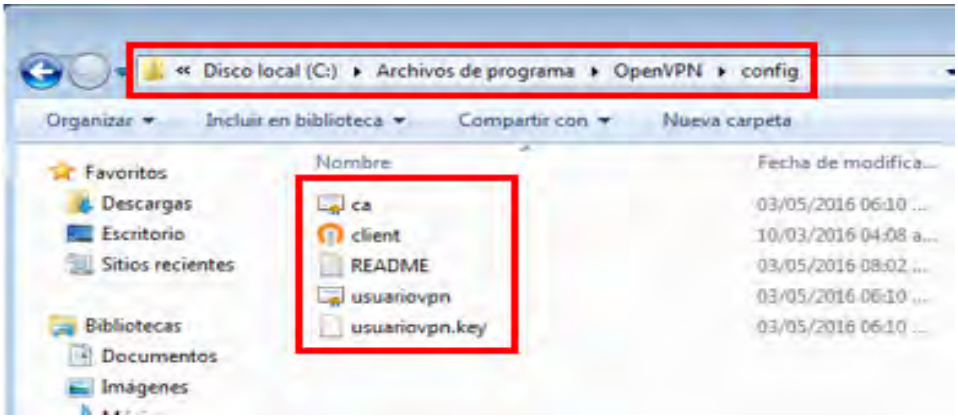
Una vez finalizada la instalación, se debe ubicar en el directorio en donde se instaló OpenVPN y copiar el archivo client de la ruta /Equipo/Disco Local C/Archivos de programa/OpenVPN/simple-config, como se muestra en la Figura 252.

Figura 252. Ejemplos de archivos de configuración para la aplicación OpenVPN



Como se aprecia, se debe pegar el archivo en la ruta /Equipo/Disco Local C/Archivos de programa/OpenVPN/config junto con los certificados copiados del servidor que se encuentran en el directorio cert-cli. Ver Figura 253.

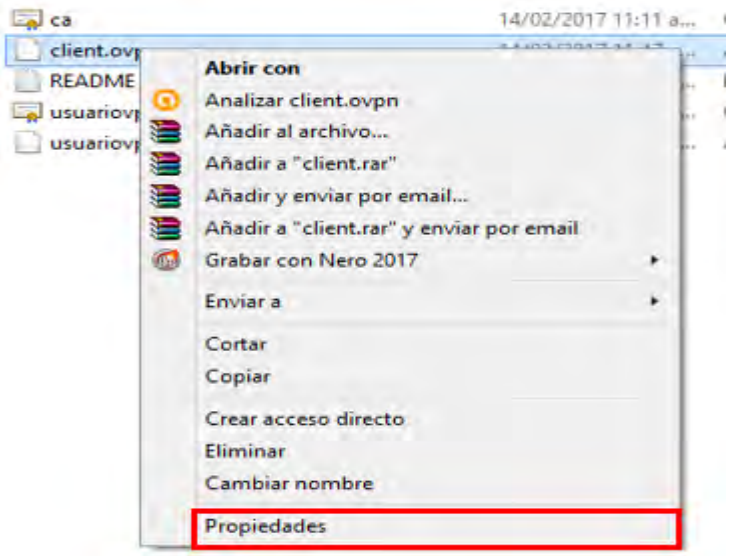
Figura 253. Directorio de configuración de OpenVPN



Antes de editar el archivo client, hay que concederle los permisos necesarios para poder escribir y guardar sobre él. Esto se logra de la siguiente manera:

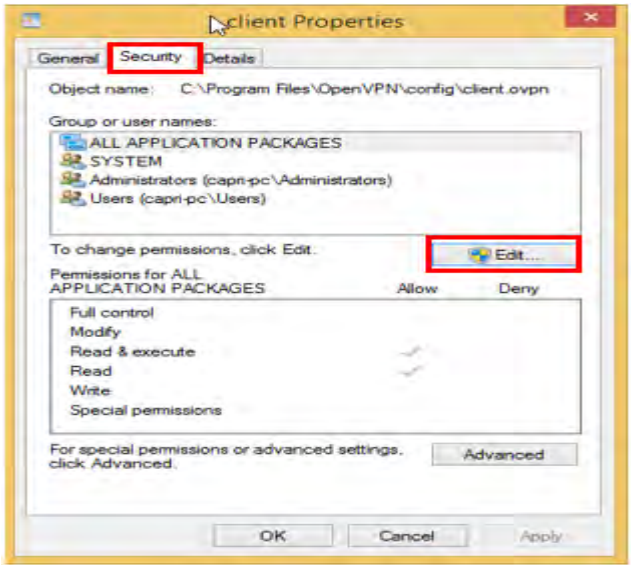
Presionar clic derecho sobre el archivo client y escoger la opción Propiedades, ver Figura 254.

Figura 254. Menú del archivo client.ovpn



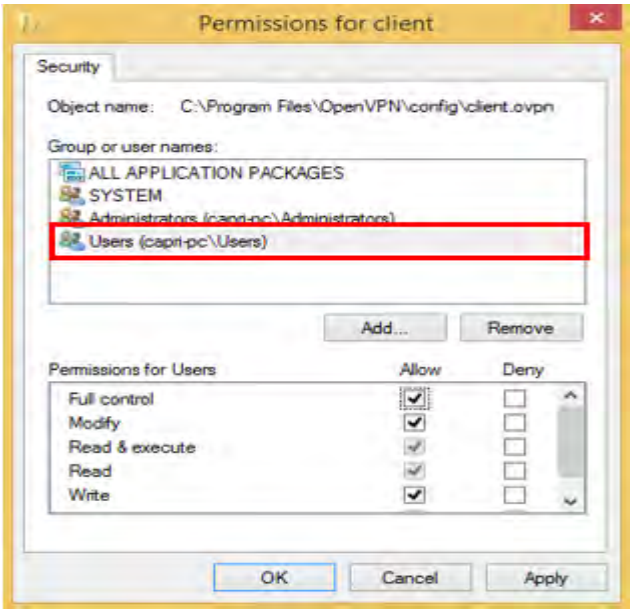
Dentro de esta ventana dirigirse a la pestaña Seguridad y hacer clic en el botón Editar, ver Figura 255.

Figura 255. Propiedades archivo client.ovpn



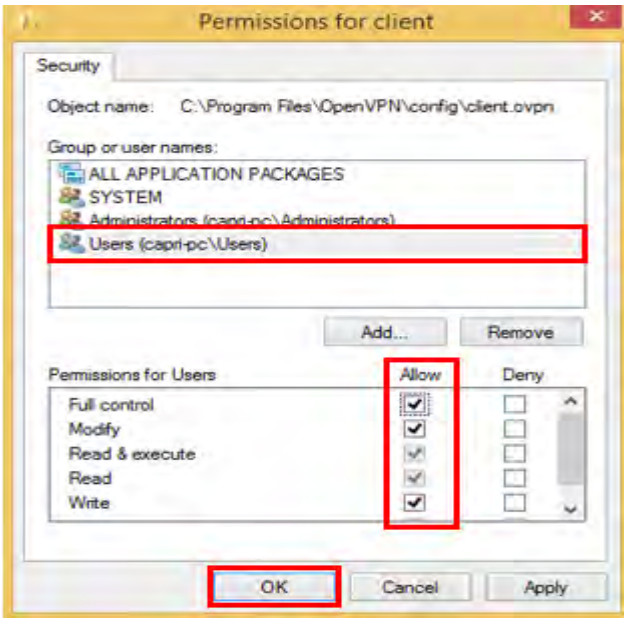
Se abre una nueva ventana y se debe escoger la opción Usuarios, ver Figura 256.

Figura 256. Configuración de permisos de usuario



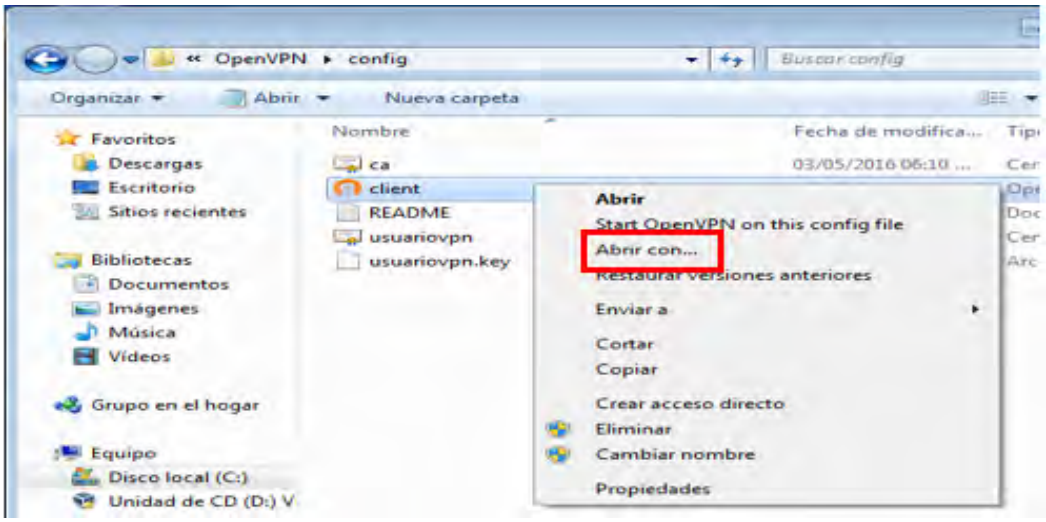
Sobre este usuario marcar la opción Control total de la columna Permitir como se muestra en la imagen. Luego hacer clic sobre el botón Aceptar, ver Figura 257.

Figura 257. Modificar permisos de usuario



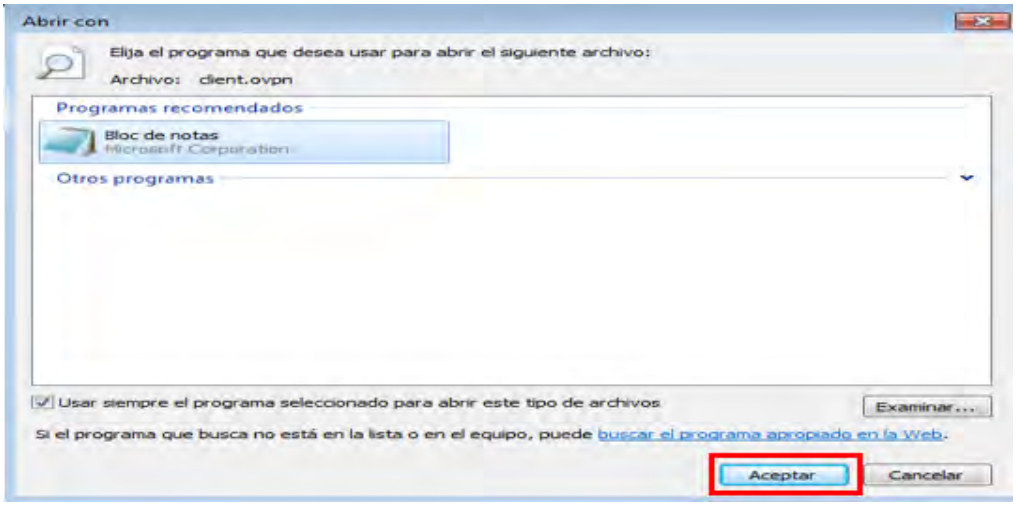
Editar el archivo client con un editor de texto, para introducir los datos donde se encuentra el servidor, las claves de cliente y la autoridad de certificación, ver Figura 258.

Figura 258. Editar archivo de configuración client.ovpn



Elegir un editor de texto de su preferencia y presionar el botón Aceptar, ver Figura 259.

Figura 259. Listado editores de texto



Dentro del archivo de configuración se debe configurar algunos parámetros como el puente a crear, la dirección IP del servidor al cual se va a conectar, los certificados que utilizará para autenticarse en el servidor, entre otros.

Buscar las siguientes líneas y modificarlas como lo indican la Figura 260, Figura 261, Figura 262 y Figura 263.

Figura 260. Configuración cliente OpenVPN 1

```
# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap0
;dev tun
```

Figura 261. Configuración cliente OpenVPN 2

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.149 1194
;remote my-server-2 1194
```

Figura 262. Configuración cliente OpenVPN 3

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert usuariovpn2.crt
key usuariovpn2.key
```

Figura 263. Configuración cliente OpenVPN 4

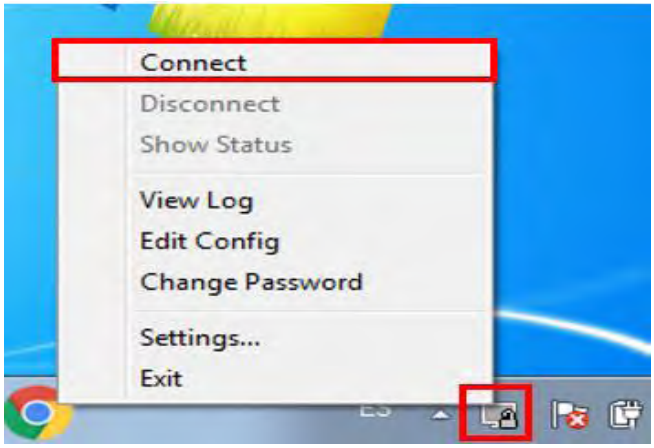
```
# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
# Note that 2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
;cipher AES-256-CBC

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

Una vez se haya realizado la configuración del archivo client.ovpn, se debe iniciar la aplicación OpenVPN GUI, haciendo doble clic sobre el icono que se muestra en la Figura 264

Figura 264. Iniciar aplicación OpenVPN

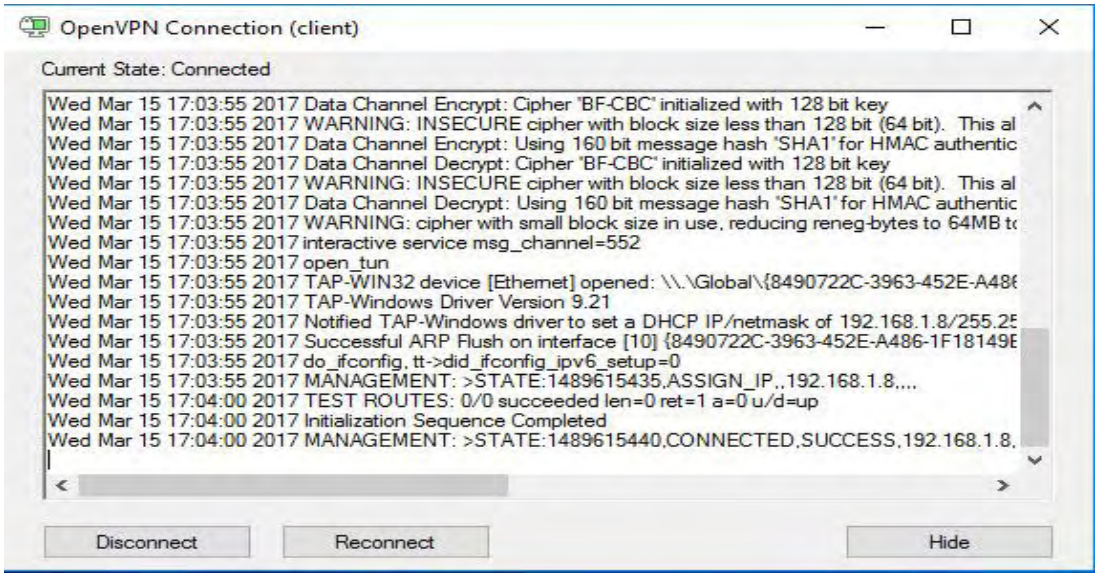
Dirigirse a la barra de tareas en la parte inferior derecha y hacer clic derecho sobre el icono de OpenVPN y escoger la opción Connect, ver Figura 265.

Figura 265. Unirse a la red privada virtual VPN



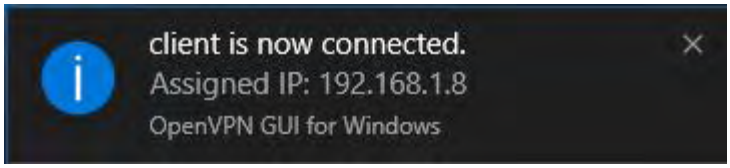
Esperar unos segundos a que cargue la configuración y los certificados de la aplicación, como se muestra en la Figura 266.

Figura 266. Establecer conexión con el servidor



Por último, el cliente aparecerá conectado y se le asignará una dirección IP, como lo indica la Figura 267.

Figura 267. Usuario autenticado y conectado a la red virtual privada



4.19 CONFIGURACIÓN DEL SERVICIO DE RED STREAMING Y CHAT

Antes de la instalación de la herramienta Openfire es necesario instalar el kit de desarrollo java , y ejecutar los siguientes pasos:

Se debe añadir lo repositorios para la posterior instalación de openjdk como se muestra en la Figura 268.

Figura 268. Añadir repositorios de openjdk

```
root@servidorCapri:/home/administrador# add-apt-repository ppa:openjdk-r/ppa
```

También es necesario actualizar los repositorios del servidor mediante el comando apt-get update, ver Figura 269.

Figura 269. Actualización de repositorios del sistema operativo

```
root@servidorCapri:/home/administrador# apt-get update
```

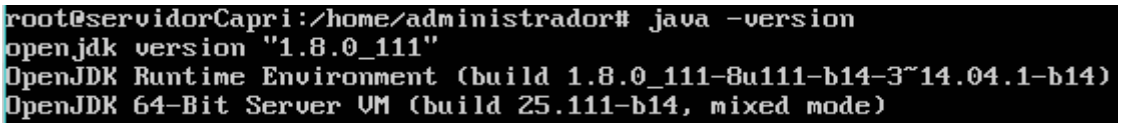
Ahora se debe instalar la herramienta openjdk con el comando mostrado en la Figura 270.

Figura 270. Instalar aplicación openjdk

```
root@servidorCapri:/home/administrador# apt-get install openjdk-8-jre_
```

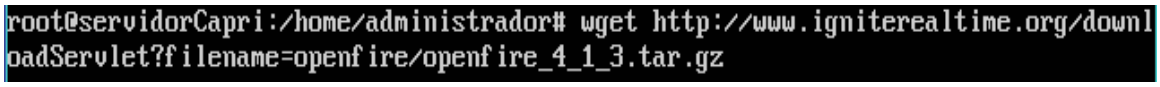
Se puede verificar la versión de Java con la que ahora cuenta el servidor ejecutando lo siguiente, ver Figura 271.

Figura 271. Verificar la versión de java



Una vez realizados estos pasos se procede a instalar la herramienta Openfire mediante el comando wget como se indica en la Figura 272.

Figura 272. Descargar aplicación Openfire



Se renombra el archivo descargado con el nombre de su preferencia con el fin de facilitar su ubicación, en este caso se nombra como openfire_4_1_3.tar.gz, esto se realiza mediante el comando mv tal como se indica en la Figura 273.

Figura 273. Renombrar archivo

El siguiente paso es descomprimir el archivo que se acaba de renombrar mediante el comando tar mostrado en la Figura 274.

Figura 274. Descomprimir la aplicación Openfire

Se comprueba la extracción del archivo con el comando ls y se observa el directorio openfire, ver Figura 275.

Figura 275. Listado de directorios y archivos del directorio administrador

Acceder a los archivos de configuración en la ruta /opt/openfire/conf/, como se observa en la Figura 276.

Figura 276. Listado de directorios y archivos en el directorio conf

```
root@servidorCapri:/home/administrador# cd /opt/openfire/conf/
root@servidorCapri:/opt/openfire/conf# ls
crowd.properties  openfire.xml  security.xml
```

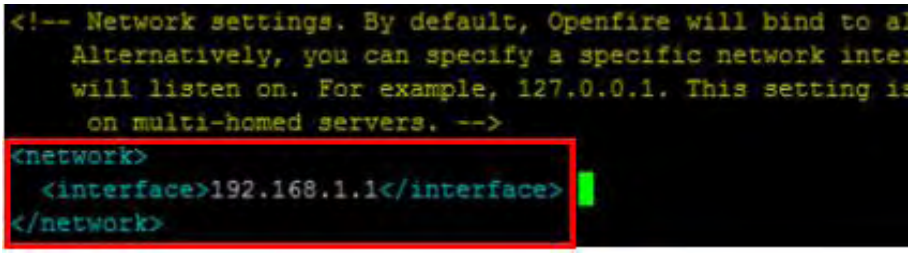
Y se edita el archivo openfire.xml con el comando nano tal como se muestra en la Figura 277.

Figura 277. Editar archivo de configuración openfire.xml

```
root@servidorCapri:/opt/openfire/conf# nano openfire.xml _
```

Se debe modificar la dirección IP con la del servidor por el cual va a funcionar Openfire, ver Figura 278.

Figura 278. Interfaz de red para Openfire



Se ejecutan los siguientes comandos para que el servicio de Openfire se inicie automáticamente al iniciar el sistema, ver Figura 279.

Figura 279. Iniciar servicio de Openfire con el sistema

```
root@servidorCapri:/home/administrador# ln -s /opt/openfire/bin/openfire /etc/init.d/
root@servidorCapri:/home/administrador# chmod +x /etc/init.d/openfire
root@servidorCapri:/home/administrador# cd /opt/openfire/
root@servidorCapri:/opt/openfire# update-rc.d openfire defaults
 Adding system startup for /etc/init.d/openfire ...
   /etc/rc0.d/K20openfire -> ../init.d/openfire
   /etc/rc1.d/K20openfire -> ../init.d/openfire
   /etc/rc6.d/K20openfire -> ../init.d/openfire
   /etc/rc2.d/S20openfire -> ../init.d/openfire
   /etc/rc3.d/S20openfire -> ../init.d/openfire
   /etc/rc4.d/S20openfire -> ../init.d/openfire
   /etc/rc5.d/S20openfire -> ../init.d/openfire
root@servidorCapri:/opt/openfire# nohoop ls >ls.log 2>&1 &
[1] 2249
```

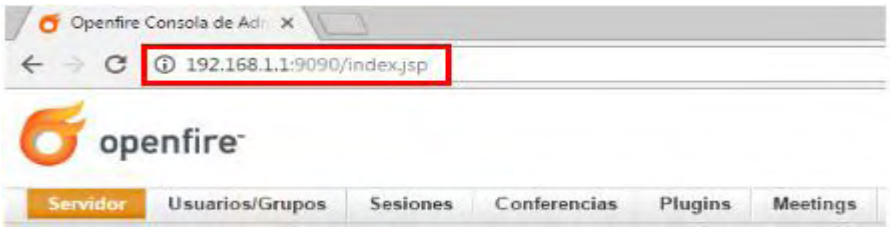
Finalmente, se inicia el servicio de Openfire mediante el comando indicado en la Figura 280.

Figura 280. Iniciar el servicio Openfire

```
root@servidorCapri:/opt/openfire/conf# /opt/openfire/bin/openfire start
```

Una vez iniciado el servicio ya es posible ingresar desde un navegador de cualquiera de las maquinas Windows de la red especificando la dirección IP o el nombre del dominio seguido del puerto 9090 que es el puerto por defecto para Openfire, como se observa en la Figura 281.

Figura 281. Ingresar a la consola de administración de Openfire



Como parte inicial de la configuración se muestra un asistente de configuración en el cual se elige el idioma a utilizar y se presiona el botón continuar, ver Figura 282.

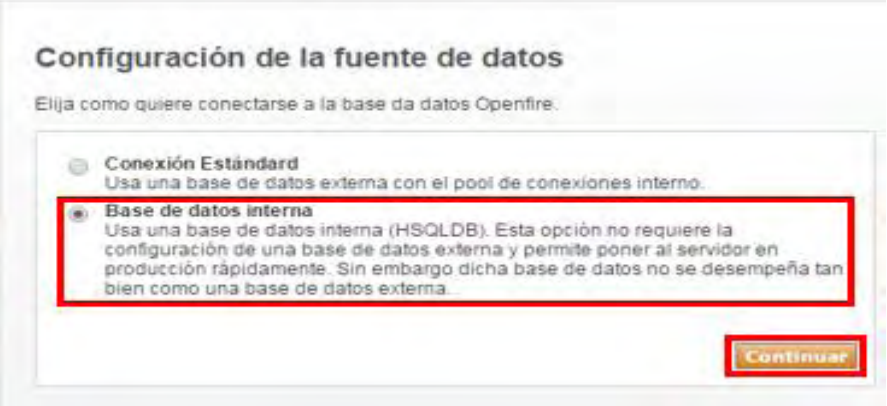
Figura 282. Configuración inicial de Openfire 1

En la siguiente ventana se configura el nombre del servidor y los puertos de conexión lo cual se recomienda dejar por defecto y presionar el botón continuar, ver Figura 283.

Figura 283. Configuración inicial de Openfire 2

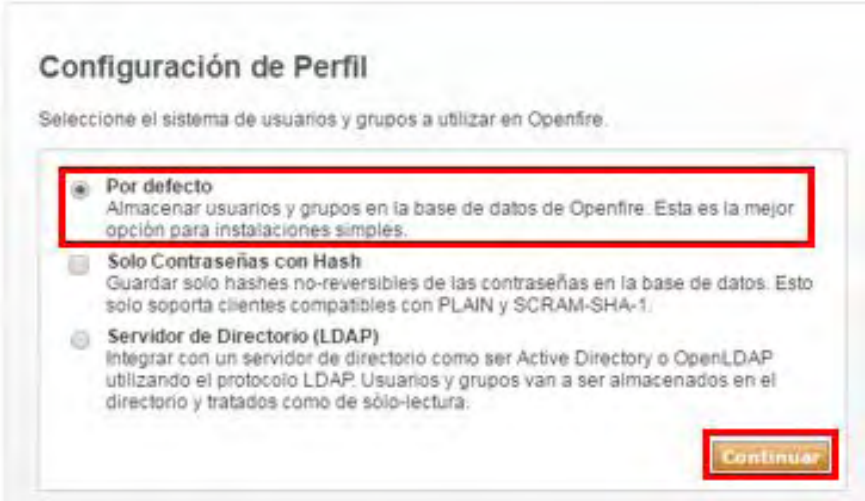
Seleccionar la opción Base de datos interna y hacer clic en continuar, ver Figura 284.

Figura 284. Configuración inicial de Openfire 3



Seleccionar la opción Por defecto y presionar el botón continuar, ver Figura 285.

Figura 285. Configuración inicial de Openfire 4



Se debe ingresar una cuenta de correo electrónico valida y una contraseña para la cuenta de administrador, como lo muestra la Figura 286 y presionar el botón continuar:

Figura 286. Configuración inicial de Openfire 5

Una vez completada la configuración inicial del servicio Openfire, se mostrará una ventana como la de la Figura 287, en donde se marca la opción Conectarse a la consola de administración.

Figura 287. Configuración inicial de Openfire 6

Se muestra una ventana para la autenticación de usuarios como la de la Figura 288, en donde se ingresa con el nombre de usuario admin y la contraseña definida en los pasos anteriores:

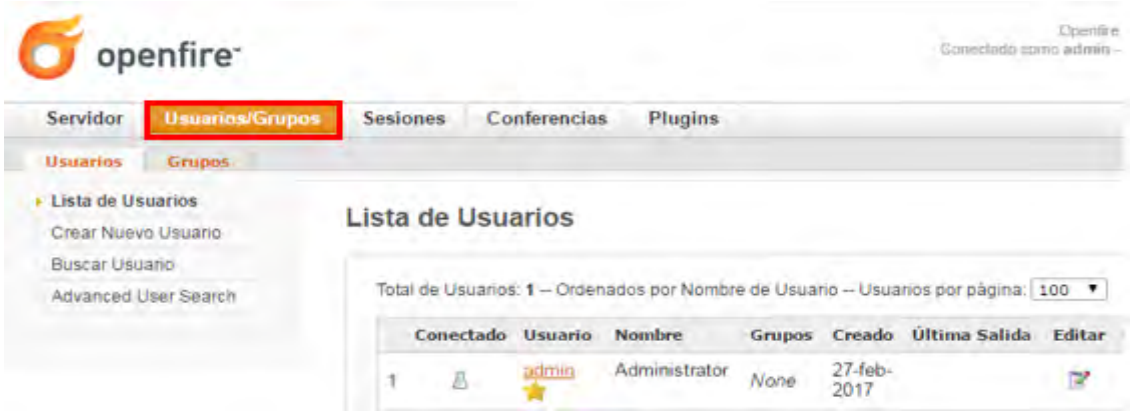
Figura 288. Autenticación de usuario consola de administración de Openfire

Al ingresar a la consola de administración se muestra la siguiente ventana, ver Figura 289.

Figura 289. Consola de administración de Openfire

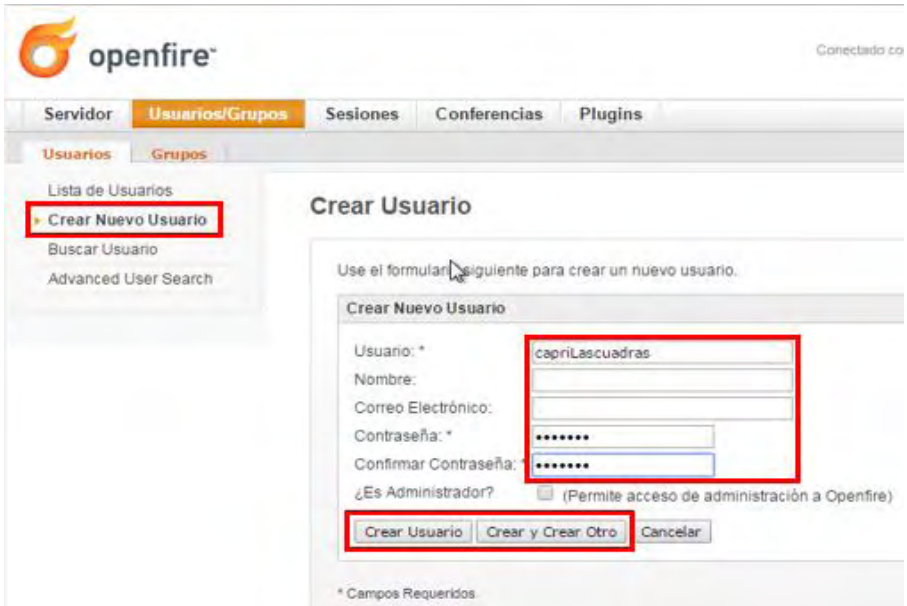
Luego, debe dirigirse a la pestaña Usuarios/Grupos para el ingreso de los nuevos usuarios como lo muestra la Figura 290.

Figura 290. Sección Usuarios/Grupos



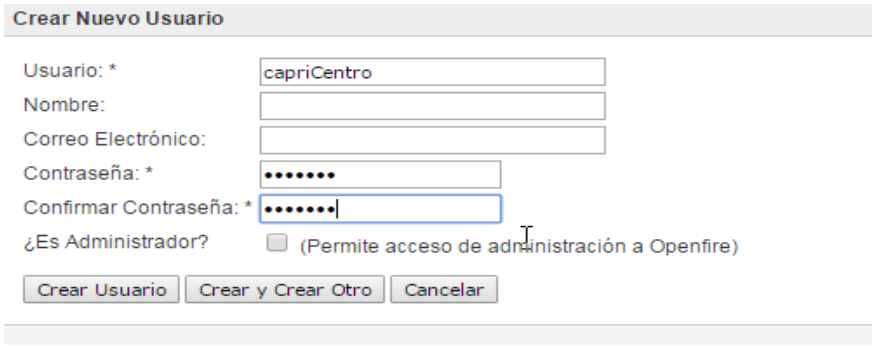
Aquí se ingresan los usuarios que sean necesarios y que podrán hacer uso de los servicios de chat y streaming mas adelante. Para añadir al usuario debe escoger un nombre de usuario y una contraseña, posteriormente se crea el usuario en el botón Crear o si lo desea en el botón Crear y crear otro para seguir añadiendo usuarios, como se observa en la Figura 291.

Figura 291. Crear nuevo usuario



Como se puede observar en la Figura 292, se ha creado otro usuario adicional para realizar la interacción entre usuarios y servidor:

Figura 292. Crear nuevo usuario 2



Cuando haya finalizado la creación de usuarios se mostrará la siguiente lista con el administrador y los usuarios registrados anteriormente. Como se puede observar en la Figura 293, los usuarios pueden ser eliminados o editar la información que se ingresó al momento de su creación.

Figura 293. Lista de usuarios de Openfire

Ya ha finalizado la configuración del servidor para prestar el servicio de chat a los usuarios que se crearon. Ahora es necesario descargar el programa pidgin mediante el cual van a interactuar los clientes. Este programa se lo puede descargar de la página oficial la cual se puede observar en la Figura 294.

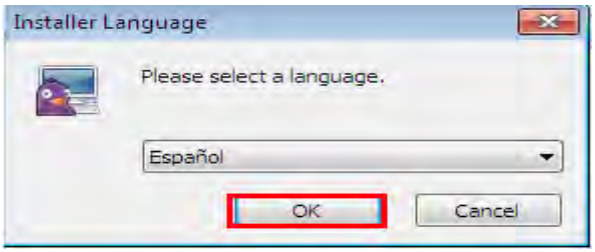
Figura 294. Página oficial de pidgin

Nota: Es recomendable descargar el instalador offline como se muestra en la Figura 295 para evitar inconvenientes al momento de la instalación.

Figura 295. Instalador offline del programa pidgin

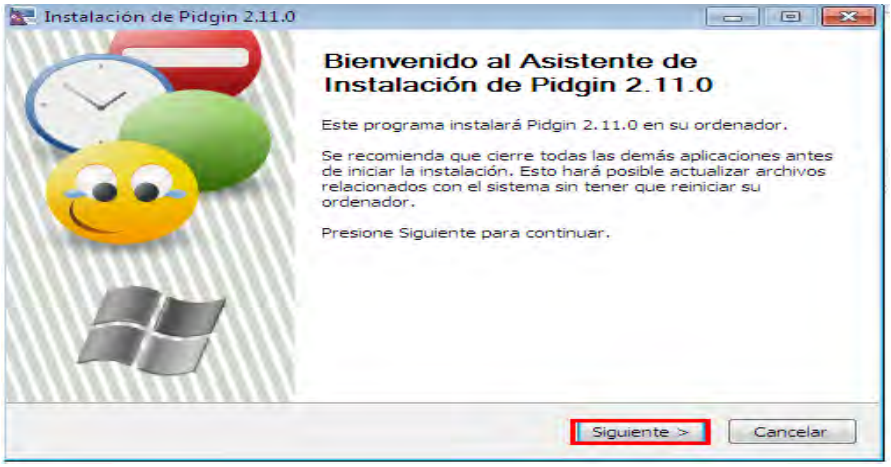
Una vez realizada la descarga se debe inicializar el instalador, el cual muestra un asistente de instalación, en el cual se elige el idioma de instalación y presionar el botón OK, ver Figura 296.

Figura 296. Asistente de instalación pidgin 1



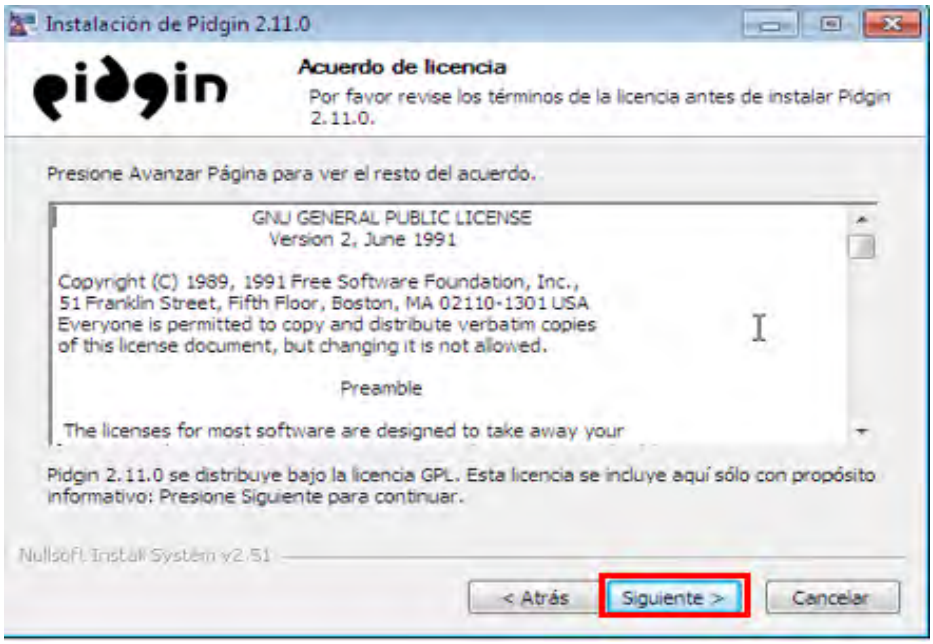
Se muestra una ventana de bienvenida en la cual se presiona el botón Siguiente, ver Figura 297.

Figura 297. Asistente de instalación pidgin 2



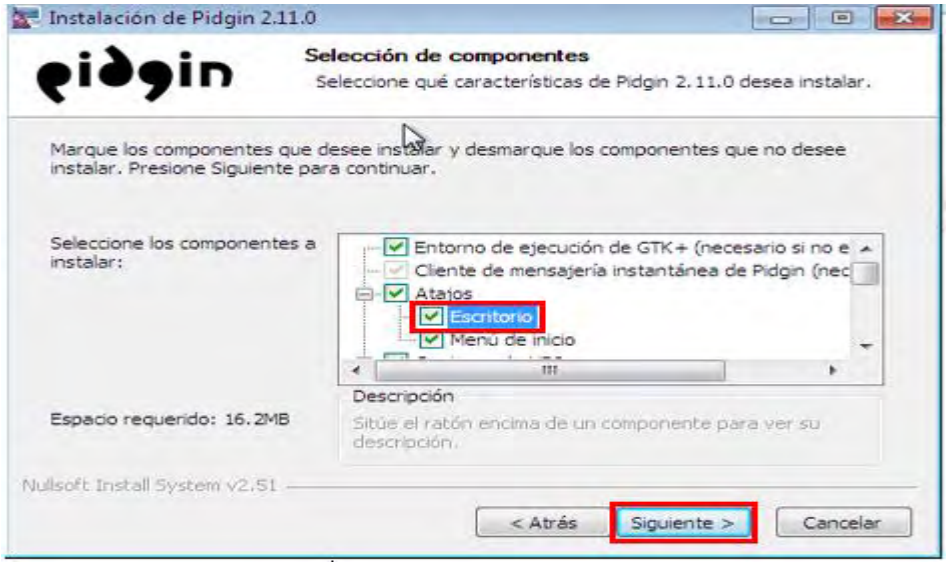
En esta sección se lee el acuerdo de licencia y luego se presiona Siguiente, ver Figura 298.

Figura 298. Asistente de instalación pidgin 3



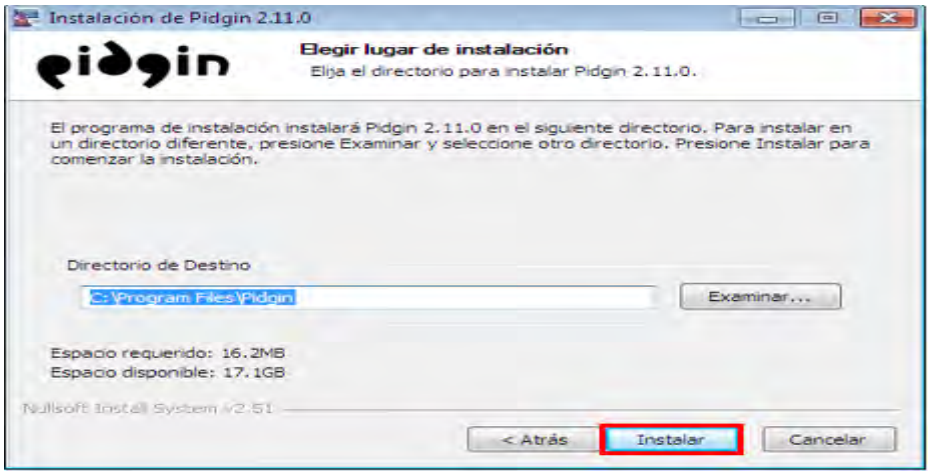
Seleccionar la opción de icono en escritorio si se desea y hacer clic en Siguiente, ver Figura 299.

Figura 299. Asistente de instalación pidgin 4



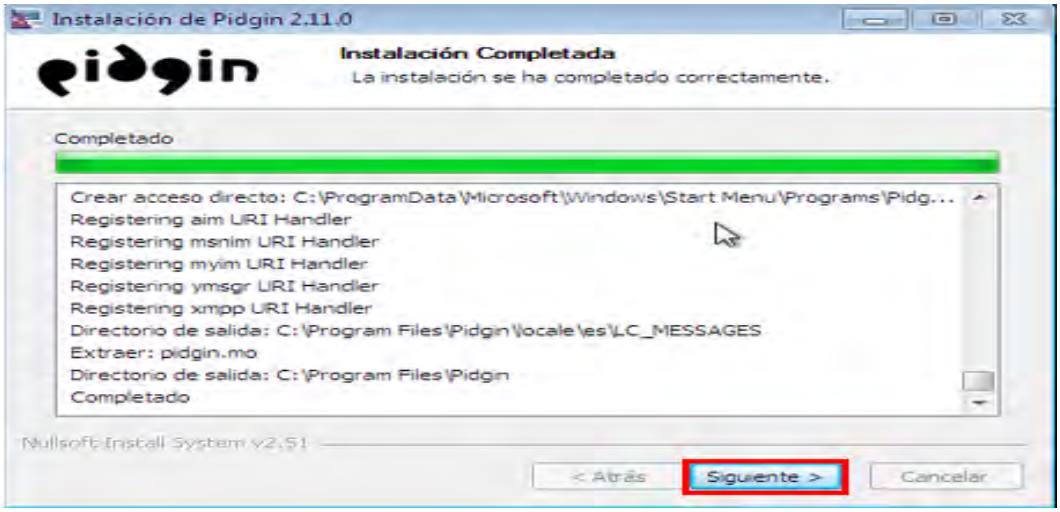
Se escoge la ruta de instalación del programa la cual se recomienda dejar por defecto y hacer clic en Instalar, ver Figura 300.

Figura 300. Asistente de instalación pidgin 5



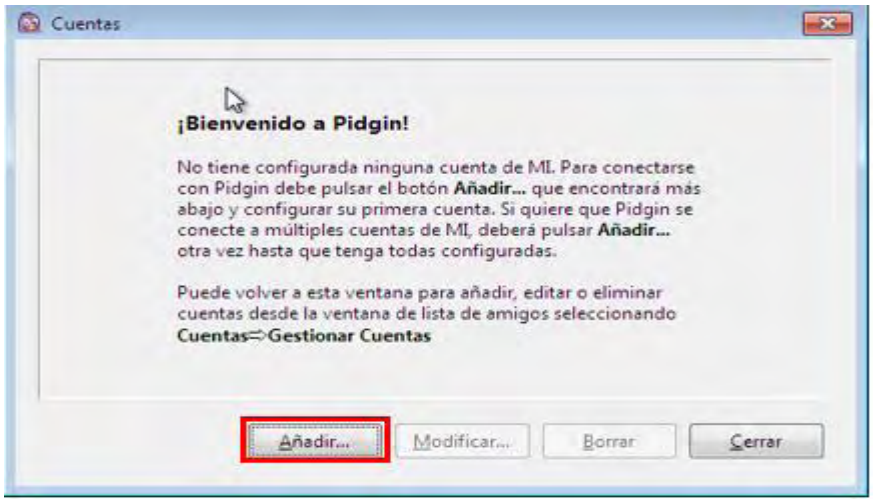
Al finalizar la instalación hacer clic en Siguiente, ver Figura 301.

Figura 301. Asistente de instalación pidgin 6



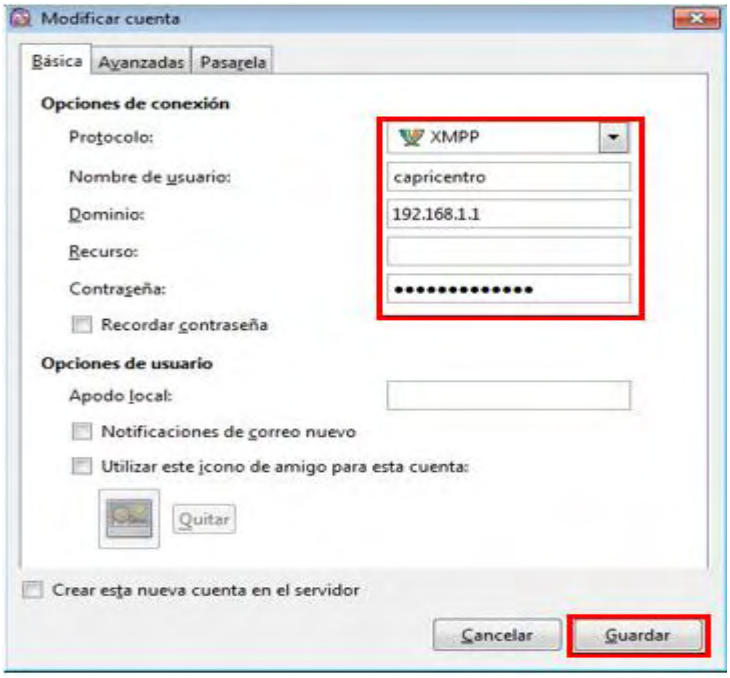
Abrir el programa Pidgin y se debe dar clic en el botón Añadir, ver Figura 302.

Figura 302. Añadir nueva cuenta pidgin



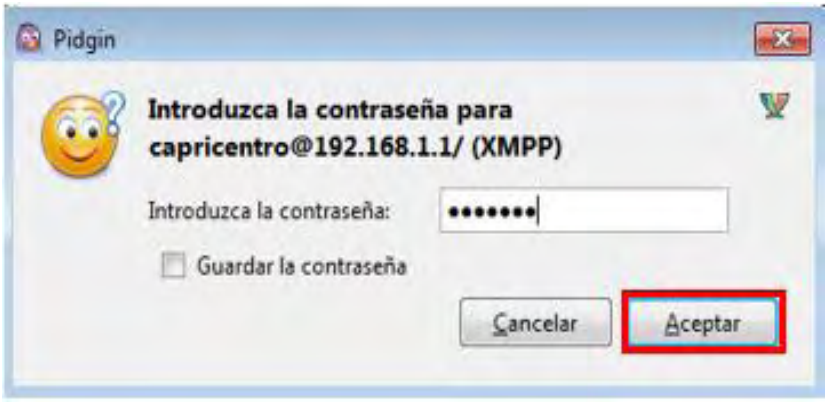
Se abre la ventana que se muestra en la Figura 303, en donde se debe especificar el protocolo, nombre de usuario, el dominio o la dirección IP del servidor y la contraseña de usuario para iniciar la sesión.

Figura 303. Ingresar información de nueva cuenta



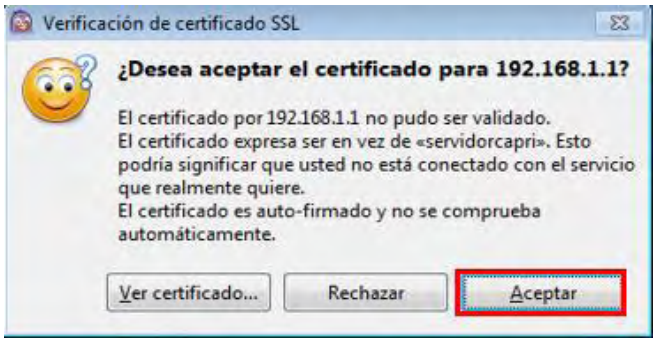
Introducir la contraseña nuevamente para ese usuario, ver Figura 304.

Figura 304. Confirmar contraseña de usuario



También se debe aceptar el certificado presionando el botón Aceptar, ver Figura 305.

Figura 305. Firmar certificados

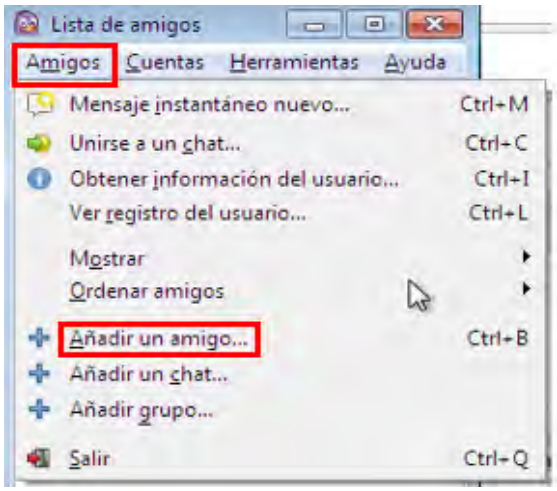


Al finalizar la creación de la cuenta se muestra una ventana como la de la Figura 306, la cual muestra los usuarios creados en la aplicación.

Figura 306. Listado de cuentas pidgin

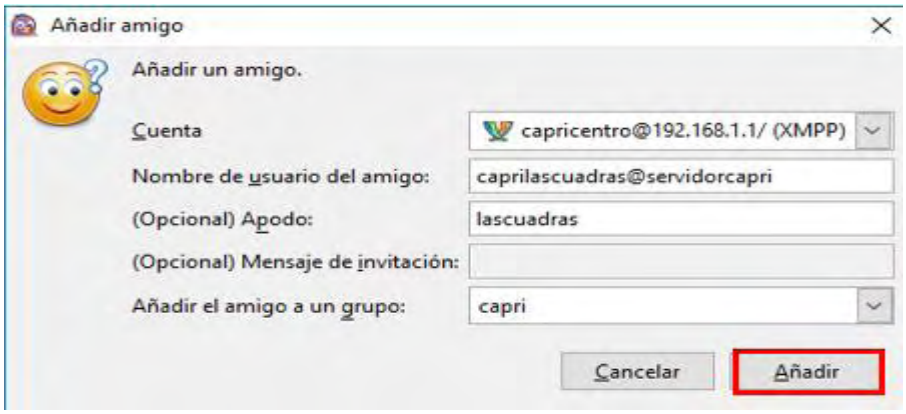
Una vez que se haya ingresado a la cuenta, se debe dirigir a la pestaña Amigos y escoger la opción Añadir un amigo, tal como lo muestra la Figura 307.

Figura 307. Lista de amigos pidgin



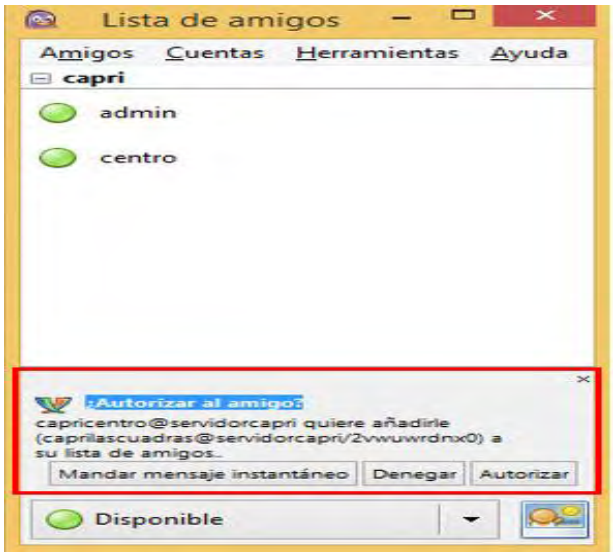
Se debe seleccionar la cuenta por la cual se va a conectar, el usuario al cual se va a agregar, un apodo para identificarlo fácilmente en la lista de amigos y se crea un grupo al cual se conectarán los usuarios, ver Figura 308.

Figura 308. Añadir amigo pidgin



Se ha ingresado desde otra máquina Windows con el usuario caprilascuadras el cual ha recibido la solicitud de amistad del usuario capricentro como se aprecia en la Figura 309.

Figura 309. Solicitud de amistad pidgin



De la misma manera, se ha ingresado con el usuario admin y se han agregado las diferentes máquinas Windows que harán parte del chat como lo muestran la Figura 310 y la Figura 311.

Figura 310. Lista de amigos usuario admin

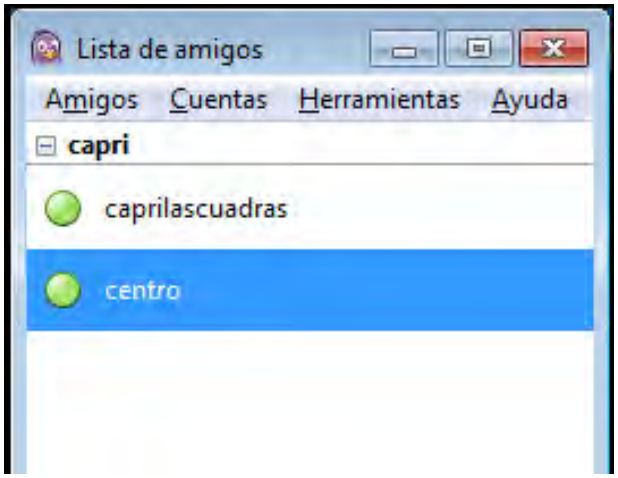
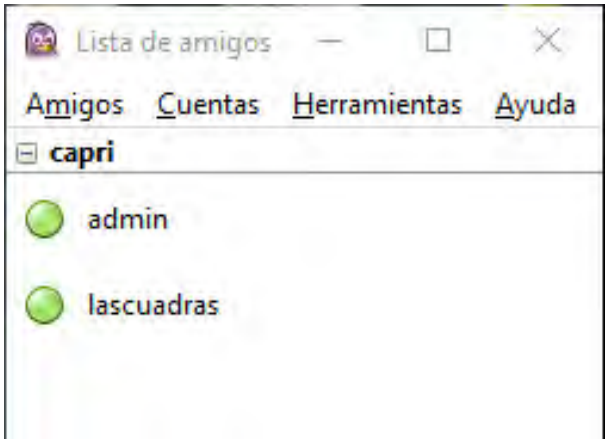


Figura 311. Lista de amigos usuario capricentro



Como se puede observar en la Figura 312 y la Figura 313, se envían mensajes de prueba entre los usuarios y el administrador.

Figura 312. Prueba de chat 1

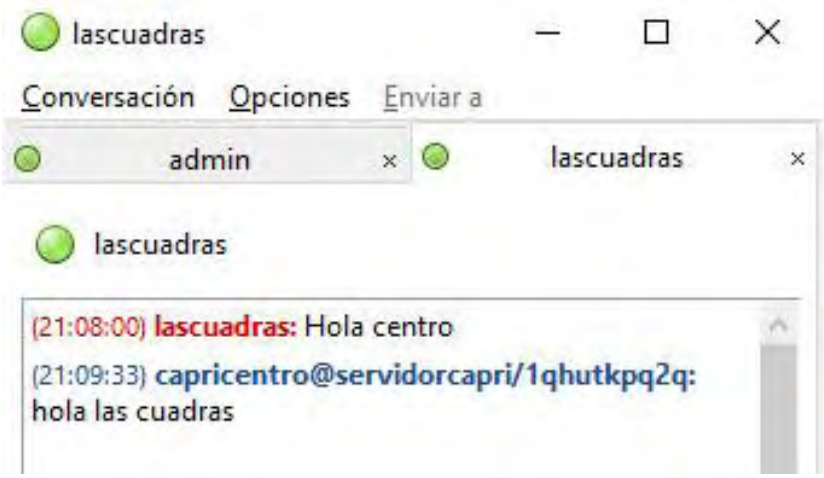
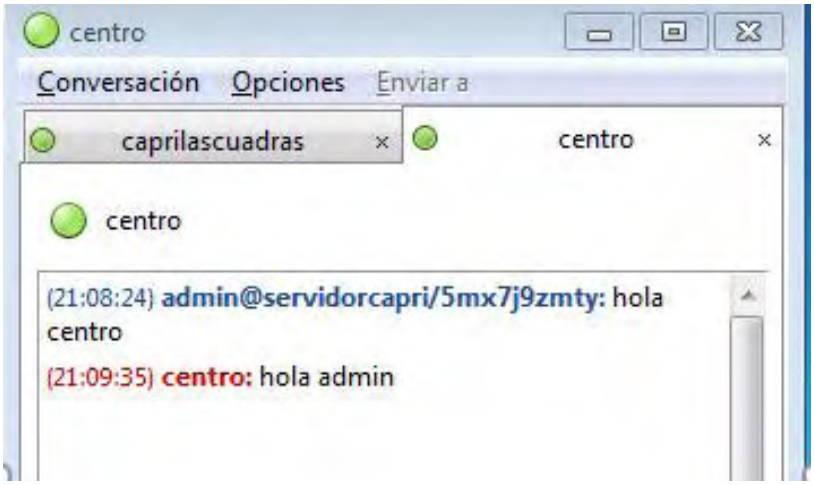
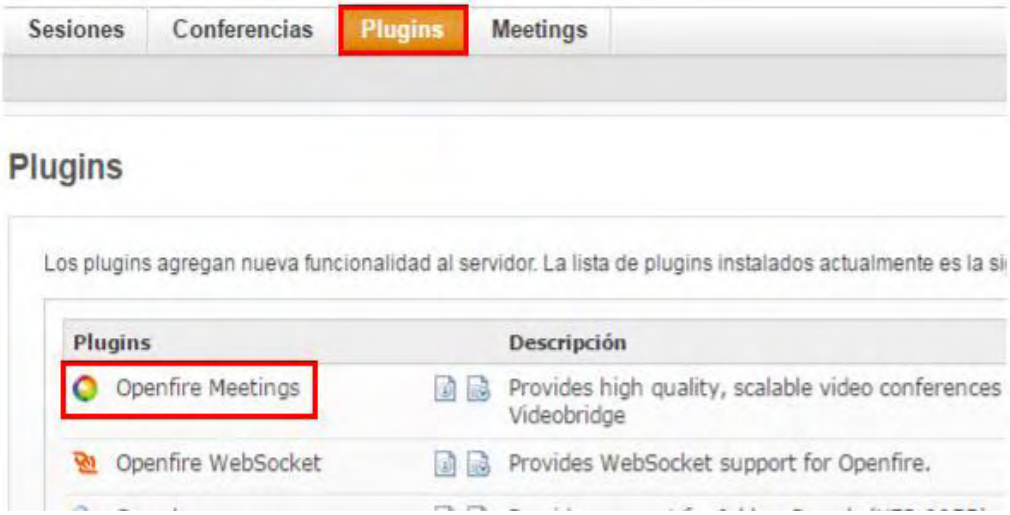


Figura 313. Prueba de chat 2



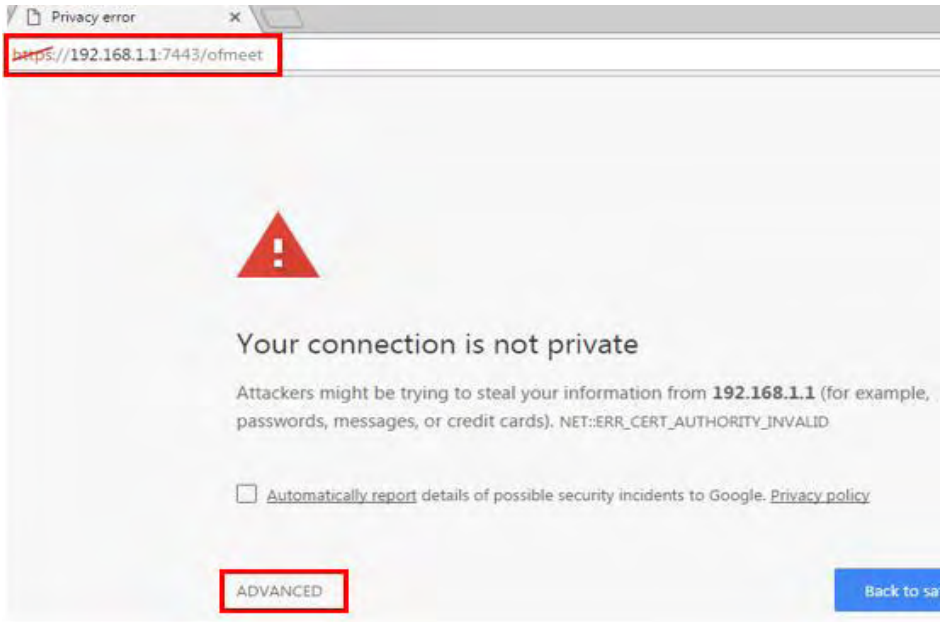
Para la configuración del servicio de Streaming es necesario instalar el complemento o plugin Openfire Meetings en el servidor como se muestra en la pestaña Plugins de la Figura 314.

Figura 314. Plugin Openfire Meetings



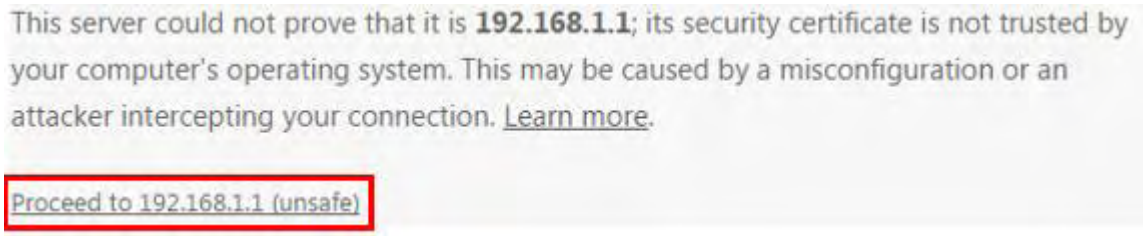
Una vez instalado el complemento debe dirigirse a la dirección URL https://192.168.1.1:7443/ofmeet en la cual aparece un mensaje de advertencia y se presiona el enlace Advanced(Avanzado), ver Figura 315.

Figura 315. Ingresar al servicio de streaming Openfire



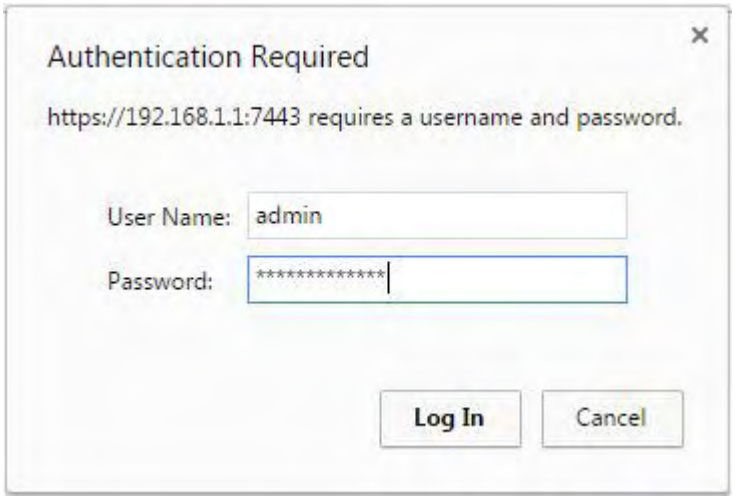
Se muestra un nuevo mensaje y un enlace para acceder al servicio de streaming en el cual se hace clic, ver Figura 316.

Figura 316. Advertencia de seguridad



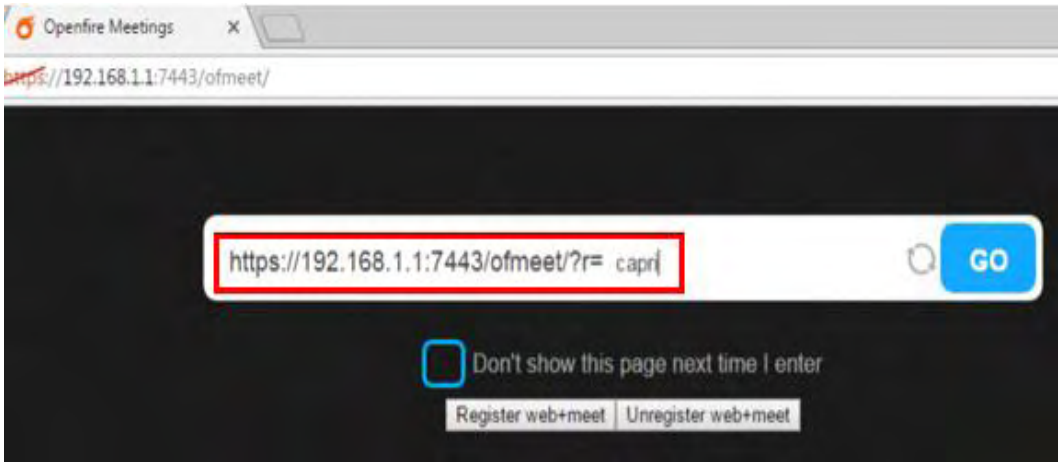
Luego, aparece la ventana de autenticación de usuarios en la cual se ingresa un nombre de usuario y contraseña de usuario válido creados anteriormente en la consola de administración de Openfire, como se aprecia en la Figura 317.

Figura 317. Autenticación de usuarios streaming



Una vez realizada la autenticación, se muestra una página en la cual se crean los links para las salas en la cual participaran los usuarios del streaming. Se debe elegir un nombre para la sala en este caso se la llama capri y presionar el botón Go. Los usuarios que deseen ingresar a esta sala deberán ingresar la dirección que se muestra a continuación en la Figura 318.

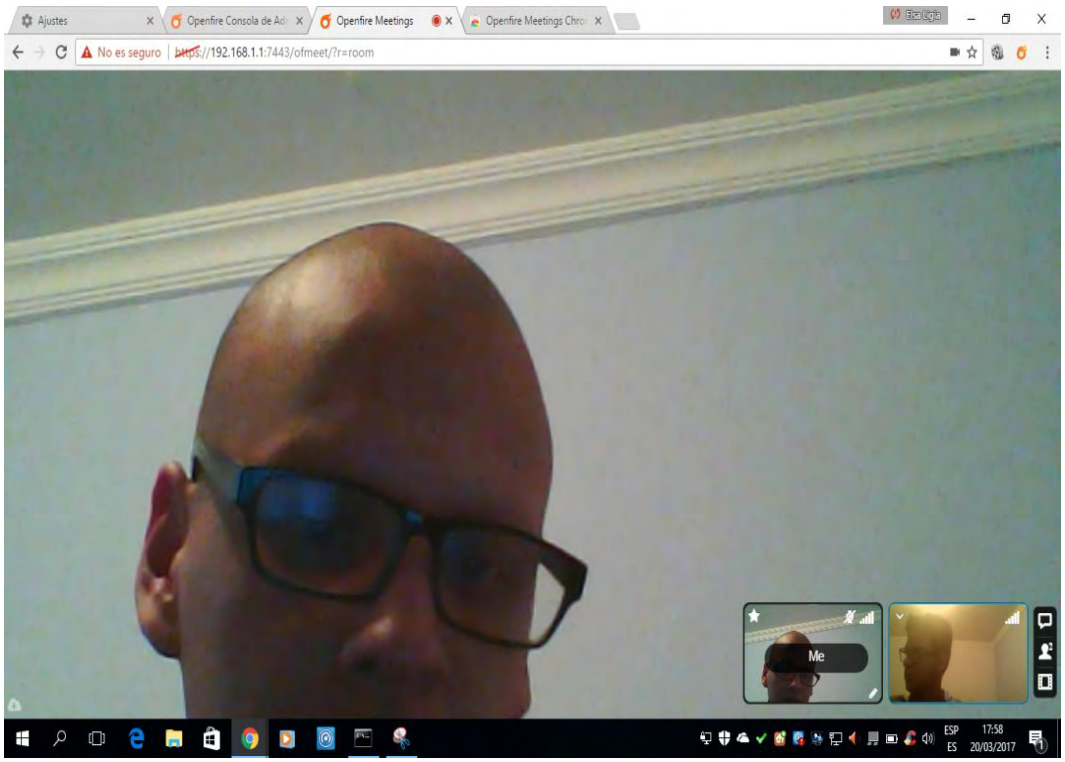
Figura 318. Crear salas de streaming



Finalmente se inicia la sesión de video streaming entre los usuarios autenticados que se hayan unido a dicha sesión como lo muestran la Figura 319 y la Figura 320.

Figura 319. Sesión de video streaming

Figura 320. Sesión de video streaming 2



4.20 CONFIGURACIÓN DEL SERVIDOR DE APLICACIONES TOMCAT

Apache Tomcat es una aplicación web de código fuente libre, el cual es utilizado para desarrollar aplicaciones en java, así como servlets que son programas, que corren del lado del servidor y corren automáticamente a la respuesta de entradas de un usuario

La instalación de esta aplicación se la realiza de forma manual con el fin de instalar la versión más nueva la cual es tomcat-9.0.0.M19, antes de proceder con la instalación se debe tener en cuenta que la herramienta de desarrollo de java (JDK), desde la versión 7 en adelante debe estar instalada en el servidor, para este caso la instalación de la herramienta JDK en su versión 8 fue hecha en una sección previa en la instalación del servicio de chat.

Una vez se confirma que JAVA este instalado se procede a descargar la versión más nueva de la aplicación tomcat con el comando wget y la dirección donde se ubica el archivo con formato tar-gz ubicado en la página oficial de la aplicación como se aprecia en la Figura 321.

Figura 321. Descarga de la aplicación Tomcat

```
root@servidorCapri:/home/administrador# wget http://apache.uniminuto.edu/tomcat/tomcat-9/v9.0.0.M19/
bin/apache-tomcat-9.0.0.0.M19.tar.gz_
```

A continuación, se extrae el paquete y se lo mueve a la carpeta /usr/local/, con el comando tar –xvf, y el comando mv descritos en la Figura 322.

Figura 322. Descomprimir archivo de tomcat y ubicación de ruta

```
root@servidorCapri:/home/administrador# tar -xvf apache-tomcat-9.0.0.M19.tar.gz
root@servidorCapri:/home/administrador# mv apache-tomcat-9.0.0.M19 /usr/local/
```

Después, para el acceso de usuarios a la administración de la aplicación se debe editar el archivo tomcat-users.xml, ubicado en la ruta /usr/local/apache-tomcat-9.0.0.m19/conf/, con el comando nano, como se ve en la Figura 323.

Figura 323. Edición archivo tomcat-users.xml.

```
root@servidorCapri:/home/administrador# nano /usr/local/apache-tomcat-9.0.0.M19/conf/tomcat-users.xml
```

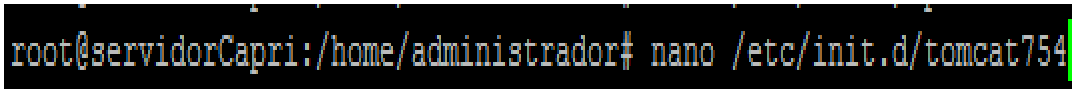
Dentro del archivo se deben añadir las siguientes líneas descritas en el cuadro rojo para añadir los roles de administración y el usuario administrador con la contraseña del mismo nombre para el acceso a la aplicación, como se ve en la Figura 324.

Figura 324. Creación de roles y nombres de usuario Tomcat

```
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<role rolename="manager-gui"/>
<role rolename="admin-gui"/>
<user username="administrador" password="administrador" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

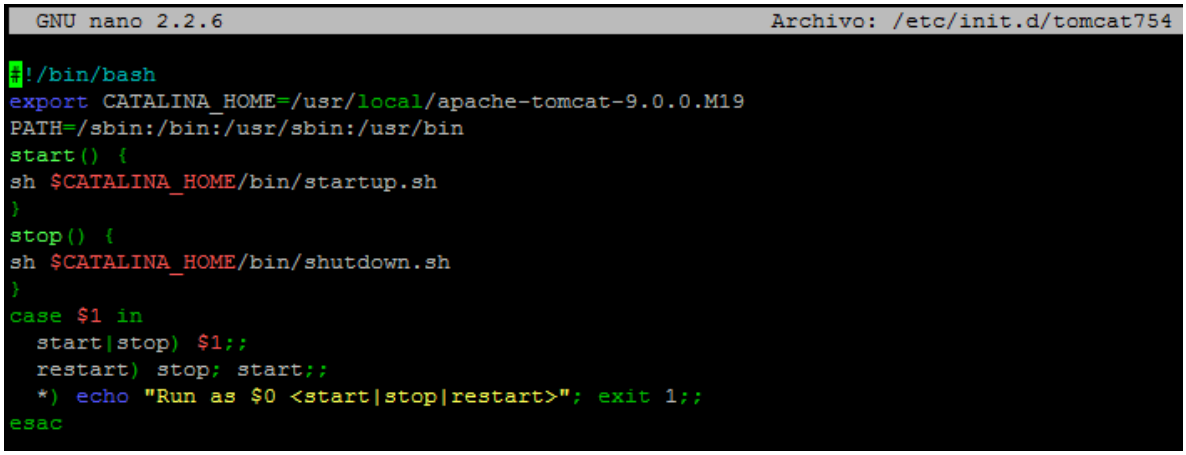
Posteriormente, se crea un nuevo archivo nombrado tomcat754 en la ruta /etc/init.d/, para la activación del servicio en el arranque del servidor, con el comando nano, apreciado en la Figura 325.

Figura 325. Creación archivo tomcat754



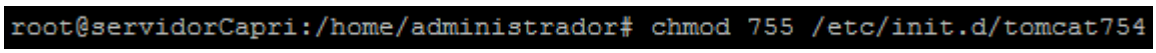
Una vez se comienza a configurar el archivo, se añade el código descrito en la Figura 326, este archivo crea el servicio llamado tomcat754.

Figura 326. Código archivo tomcat754



Se deben guardar los cambios en el archivo y se deben cambiar los permisos de este, con el comando chmod 755, para su ejecución como se ve en la Figura 327.

Figura 327. Permisos de ejecución archivo tomcat754



También se debe realizar una actualización en el archivo update-rc.d, con el fin de que el servicio tomcat754 se incluya en la listas de servicios activados desde el inicio del sistema, como se ve en la Figura 328.

Figura 328. Añadir servicio tomcat754 default update-rc.d

```
root@servidorCapri:/home/administrador# update-rc.d tomcat754 defaults
```

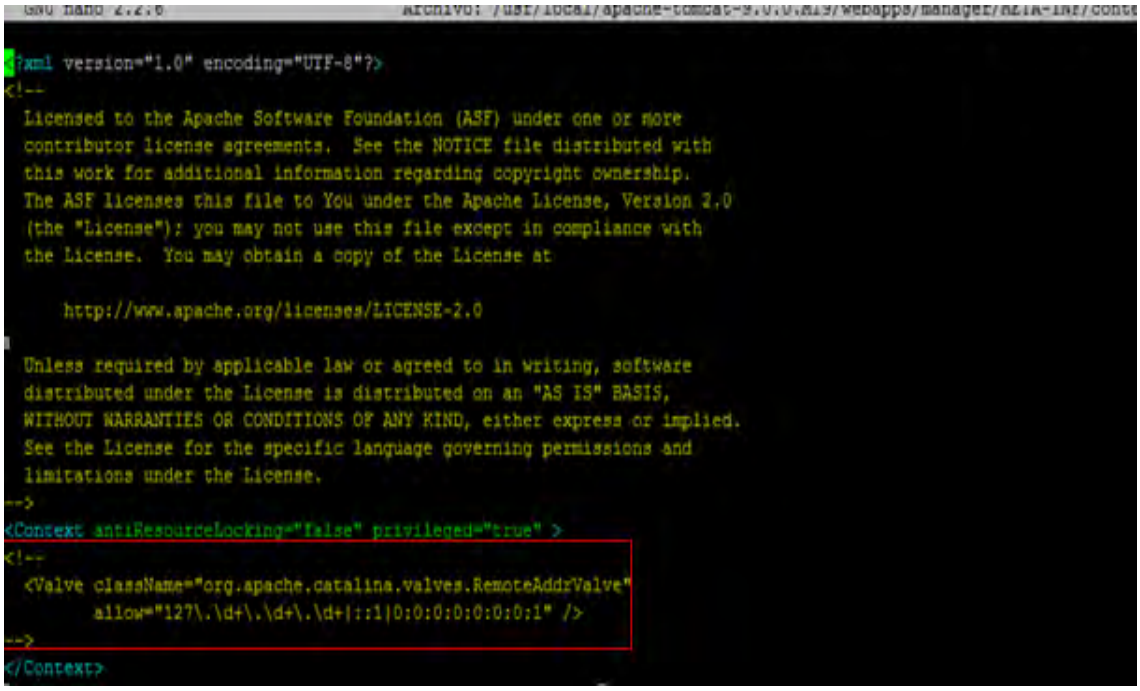
Posteriormente, se debe editar con el comando nano, el archivo context.xml para que la aplicación permita dar acceso al usuario configurado, en la ruta /usr/local/apache-tomcat-9.0.0.0.M19/webapps/manager/META-INF/, descrito en la Figura 329.

Figura 329. Edición del archivo context.xml.

```
root@servidorCapri:/home/administrador# nano /usr/local/apache-tomcat-9.0.0.M19/webapps/manager/META-INF/context.xml
```

Dentro del archivo, se debe comentar los campos que se muestran en la figura con formato HTML (<!-- -->), para comentar las líneas que se muestran en la Figura 330.

Figura 330. Comentarios en las líneas del archivo context.xml.



Se debe guardar el archivo una vez modificado, y a continuación de sebe iniciar el servicio instalado. Ver Figura 331.

Figura 331. Inicio servicio tomcat754

```
root@servidorCapri:/home/administrador# /etc/init.d/tomcat754 start
```

En un navegador cliente conectado a la red se debe escribir la dirección local con el puerto 8080 para que se muestre la interfaz principal de gestión de la aplicación. Donde se pueden saber los estados de todas las aplicaciones que se quieran instalar en la empresa, la aplicación para su gestión, y una administración de todos los hosts que se requieran virtualizar por medio de la aplicación. Ver Figura 332, Figura 333, y Figura 334.

Figura 332. Página principal Tomcat

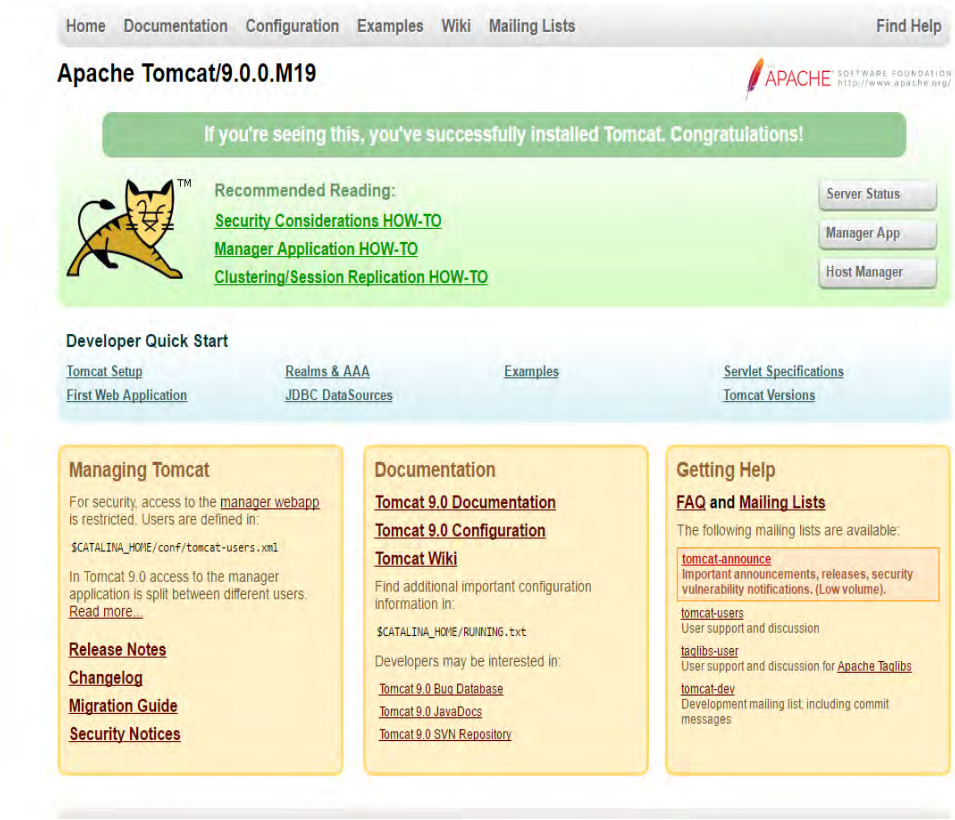
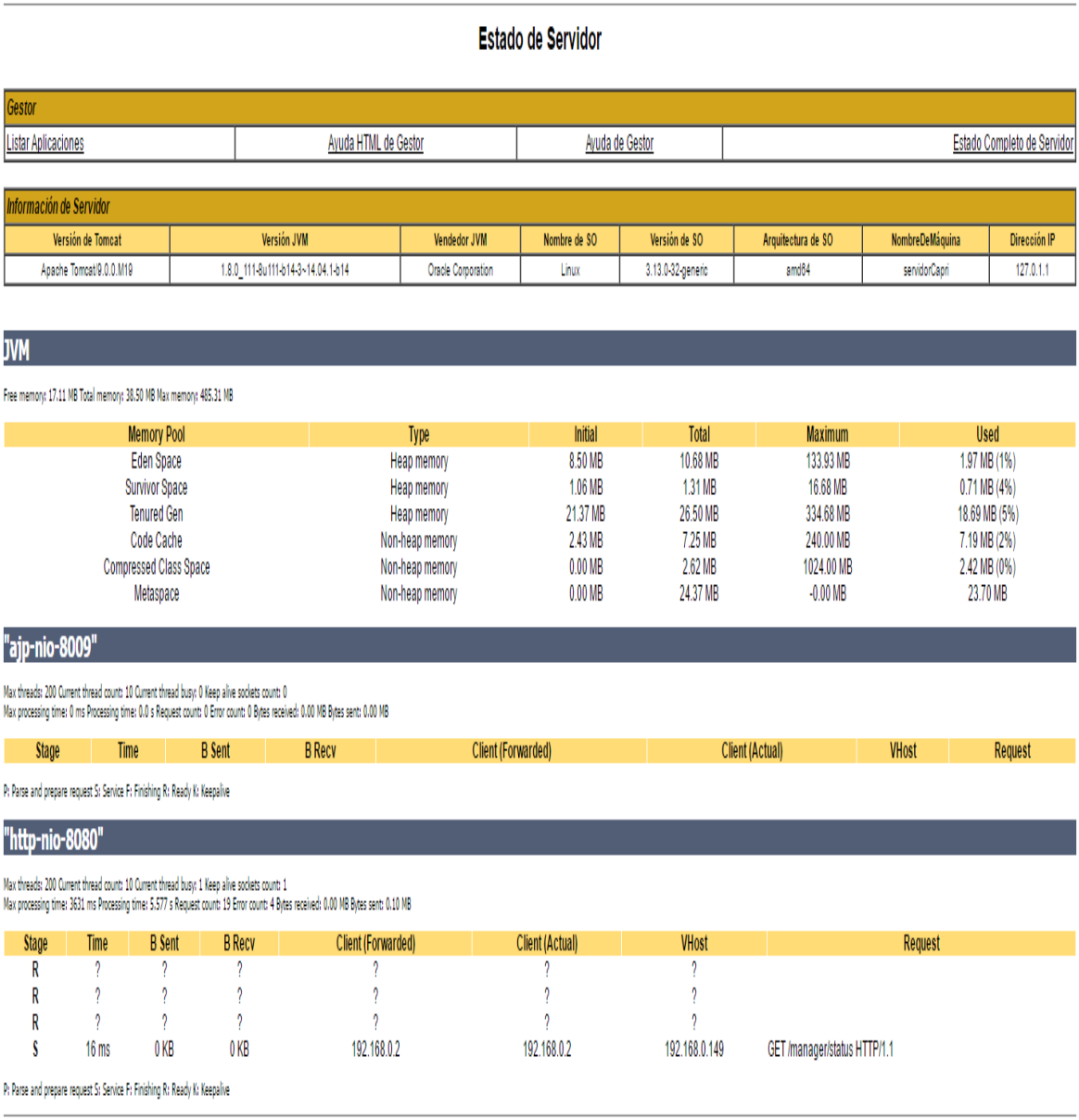


Figura 333. Estado de servidor Tomcat



Estado de Servidor

Gestor			
Listar Aplicaciones	Ayuda HTML de Gestor	Ayuda de Gestor	Estado Completo de Servidor

Información de Servidor							
Versión de Tomcat	Versión JVM	Vendedor JVM	Nombre de SO	Versión de SO	Arquitectura de SO	NombreDeMáquina	Dirección IP
Apache Tomcat/9.0.0.M19	1.8.0_111-8u111-b14-3~14.04.1-b14	Oracle Corporation	Linux	3.13.0-32-generic	amd64	servidorCapri	127.0.1.1

JVM

Free memory: 17.11 MB Total memory: 38.50 MB Max memory: 465.31 MB

Memory Pool	Type	Initial	Total	Maximum	Used
Eden Space	Heap memory	8.50 MB	10.68 MB	133.93 MB	1.97 MB (1%)
Survivor Space	Heap memory	1.06 MB	1.31 MB	16.68 MB	0.71 MB (4%)
Tenured Gen	Heap memory	21.37 MB	26.50 MB	334.68 MB	18.69 MB (5%)
Code Cache	Non-heap memory	2.43 MB	7.25 MB	240.00 MB	7.19 MB (2%)
Compressed Class Space	Non-heap memory	0.00 MB	2.62 MB	1024.00 MB	2.42 MB (0%)
Metaspace	Non-heap memory	0.00 MB	24.37 MB	-0.00 MB	23.70 MB

"ajp-nio-8009"

Max threads: 200 Current thread count: 10 Current thread busy: 0 Keep alive sockets count: 0
Max processing time: 0 ms Processing time: 0.0 s Request count: 0 Error count: 0 Bytes received: 0.00 MB Bytes sent: 0.00 MB

Stage	Time	B Sent	B Recv	Client (Forwarded)	Client (Actual)	VHost	Request

P: Parse and prepare request S: Service F: Finishing R: Ready K: Keepalive

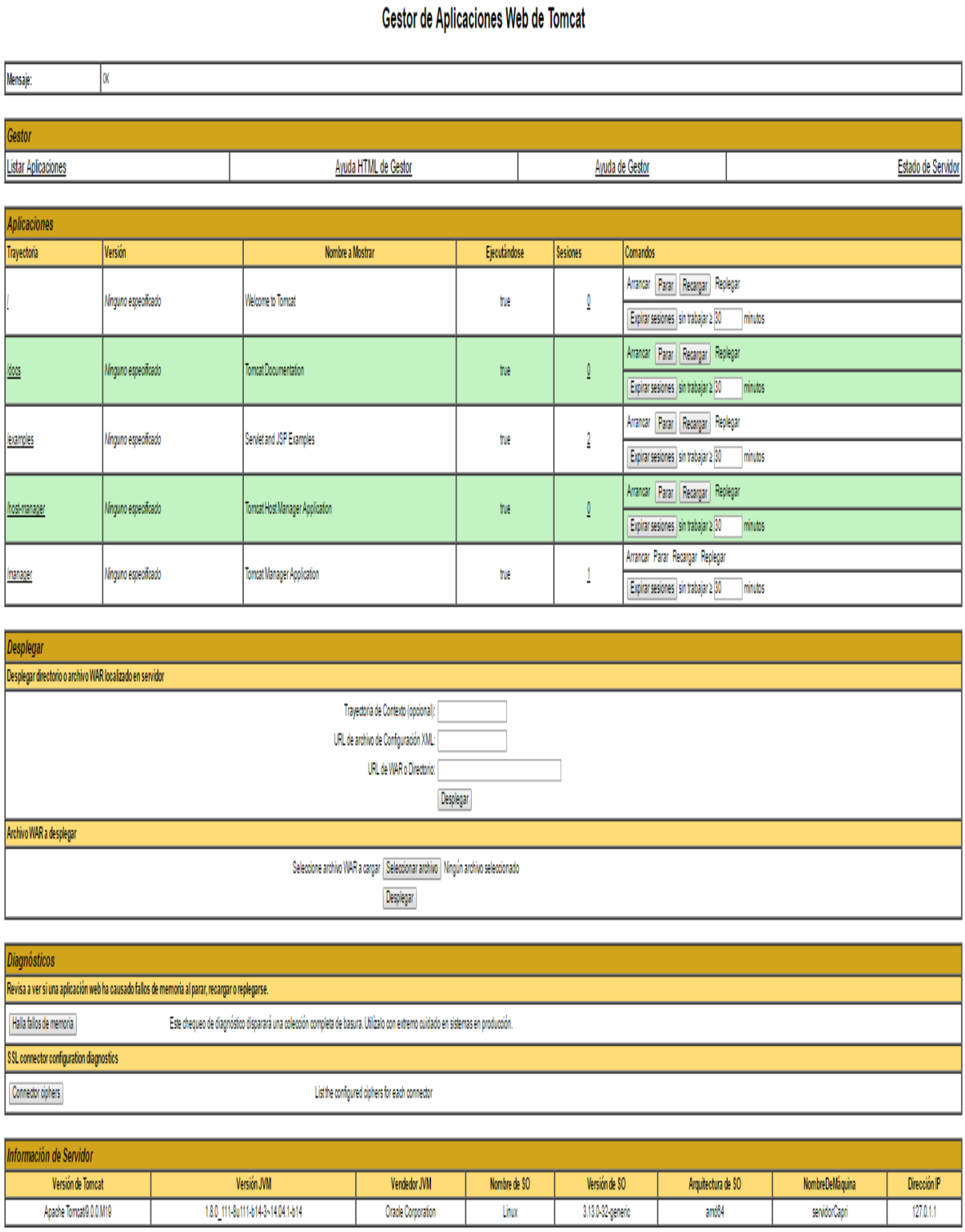
"http-nio-8080"

Max threads: 200 Current thread count: 10 Current thread busy: 1 Keep alive sockets count: 1
Max processing time: 3621 ms Processing time: 5.577 s Request count: 19 Error count: 4 Bytes received: 0.00 MB Bytes sent: 0.10 MB

Stage	Time	B Sent	B Recv	Client (Forwarded)	Client (Actual)	VHost	Request
R	?	?	?	?	?	?	
R	?	?	?	?	?	?	
R	?	?	?	?	?	?	
S	16 ms	0 KB	0 KB	192.168.0.2	192.168.0.2	192.168.0.149	GET /manager/status HTTP/1.1

P: Parse and prepare request S: Service F: Finishing R: Ready K: Keepalive

Figura 334. Gestor de aplicaciones web Tomcat



Gestor de Aplicaciones Web de Tomcat

Mensaje:	OK

Gestor			
Listar Aplicaciones	Ayuda HTML de Gestor	Ayuda de Gestor	Estado de Servidor

Aplicaciones

Trayectoria	Versión	Nombre a Mostrar	Ejecutándose	Sesiones	Comandos
/	Ninguno especificado	Welcome to Tomcat	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
/docs	Ninguno especificado	Tomcat Documentation	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
/examples	Ninguno especificado	Servlet and JSP Examples	true	2	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
/host-manager	Ninguno especificado	Tomcat Host Manager Application	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
/manager	Ninguno especificado	Tomcat Manager Application	true	1	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos

Desplegar

Desplegar directorio o archivo WAR localizado en servidor

Trayectoria de Contexto (opcional):
URL de archivo de Configuración XML:
URL de WAR o Directorio:
Desplegar

Archivo WAR a desplegar

Seleccione archivo WAR a cargar Seleccionar archivo Ningún archivo seleccionado
Desplegar

Diagnósticos

Revisa a ver si una aplicación web ha causado fallos de memoria al parar, recargar o replegarse.

Halla fallos de memoria — Este chequeo de diagnóstico disparará una colección completa de basura. Utilízalo con extremo cuidado en sistemas en producción.

SSL connector configuration diagnostics

Connector ciphers — List the configured ciphers for each connector

Información de Servidor

Versión de Tomcat	Versión JVM	Vendedor JVM	Nombre de SO	Versión de SO	Arquitectura de SO	NombreDeMáquina	Dirección IP
Apache Tomcat/8.0.0.M19	1.8.0_111-8u111-b14-3~14.04.1-b14	Oracle Corporation	Linux	3.13.0-32-generic	amd64	servidorCapri	127.0.1.1

4.21 CONFIGURACIÓN DEL SISTEMA DE MONITOREO DE RED NAGIOS

Para realizar la instalación y configuración del sistema de monitoreo de red Nagios es necesario descargar la aplicación y sus complementos desde los links que se muestran en la Figura 335 y la Figura 336.

Figura 335. Descargar la aplicación Nagios

```
root@servidorCapri:/home/administrador# wget https://sourceforge.net/projects/na
gios/files/nagios-4.x/nagios-4.3.1/nagios-4.3.1.tar.gz_
```

Figura 336. Descargar complementos para la aplicación Nagios

```
root@servidorCapri:/home/administrador# wget https://nagios-plugins.org/download
/nagios-plugins-2.1.4.tar.gz
```

Es muy importante también, instalar el servicio de Apache y algunas librerías más que serán necesarias para el correcto funcionamiento del sistema.

En este caso el servicio de Apache ya fue instalado y configurado en el servidor de manera detallada anteriormente en el desarrollo de este documento, como se observa en la sección de configuración de Apache, por lo tanto, no es necesario realizar la instalación nuevamente así que se procede a instalar las librerías que hacen falta como lo indican la Figura 337, Figura 338 y la Figura 339.

Figura 337. Complementos del servidor web Apache

```
root@servidorCapri:/home/administrador# apt-get install libapache2-mod-php5_
```

Figura 338. Complementos del servidor web Apache 2

```
root@servidorCapri:/home/administrador# apt-get install build-essential
```

Figura 339. Complementos del servidor web Apache 3

```
root@servidorCapri:/home/administrador# apt-get install libgd2-xpm-dev_
```

Una vez instaladas las librerías, se debe crear un nuevo usuario llamado nagios para este caso, y se lo añade a un nuevo grupo el cual se ha nombrado como nagcmd. Posteriormente se añaden al grupo tanto el nuevo usuario creado como el usuario de Apache el cual es necesario para el funcionamiento de la aplicación. Este procedimiento se observa en la Figura 340.

Figura 340. Crear usuarios y grupos de Nagios

```
root@servidorCapri:/home/administrador# useradd nagios
root@servidorCapri:/home/administrador# groupadd nagcmd
root@servidorCapri:/home/administrador# usermod -a -G nagcmd nagios
root@servidorCapri:/home/administrador# usermod -a -G nagcmd www-data
```

Ahora se debe ubicar en el directorio en el cual se descargó Nagios y se debe descomprimir el archivo como lo indica la Figura 341.

Figura 341. Descomprimir la aplicación Nagios

```
root@servidorCapri:/home/administrador# tar -zxvf nagios-4.3.1.tar.gz
```

Una vez se haya extraído el archivo se accede a ese directorio mediante el comando cd /Nagios-4.3.1/. Dentro de este directorio se debe ejecutar el comando que se muestra en la Figura 342, para su configuración, en el cual se especifican los usuarios, el grupo y el directorio necesario de Apache:

Figura 342. Ejecutar configuración de Nagios

```
root@servidorCapri:/home/administrador/nagios-4.3.1# ./configure --with-nagios-g
roup=nagios --with-command-group=nagcmd --with-httpd_conf=/etc/apache2/sites-ena
bled/
```

Después de ejecutar el comando anterior, se muestra un resumen de la configuración con la cual funcionara la aplicación Nagios en el servidor, ver Figura 343.

Figura 343. Resumen de configuración de Nagios

Luego, se debe compilar el código fuente e instalar algunos archivos necesarios para el sistema como se muestra en la Figura 344, Figura 345, Figura 346, Figura 347 y Figura 348.

Figura 344. Compilar código fuente de Nagios

Figura 345. Compilar código fuente de Nagios 2

Figura 346. Compilar código fuente de Nagios 3

Figura 347. Compilar código fuente de Nagios 4

```
root@servidorCapri:/home/administrador/nagios-4.3.1# make install-commandmode_
```

Figura 348. Compilar código fuente de Nagios 5

```
root@servidorCapri:/home/administrador/nagios-4.3.1# make install-webconf_
```

Ya está instalado el sistema de monitoreo Nagios en el servidor y ahora se procede a su configuración. Para esto se edita el archivo contacts.cfg con el comando nano y se modifican las líneas que se muestra a continuación en la Figura 349 y la Figura 350.

Figura 349. Editar el archivo contacts.cfg

```
root@servidorCapri:/home/administrador/nagios-4.3.1# nano /usr/local/nagios/etc/
objects/contacts.cfg
```

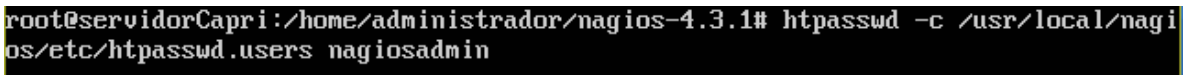
Figura 350. Información de contactos de Nagios

```
  GNU nano 2.2.6 Archivo: .../local/nagios/etc/objects/contacts.cfg Modificado

# CONTACTS
#
###############################################################################
###############################################################################

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-co$
# template which is defined elsewhere.

define contact{
        contact_name                    nagiosadmin             ; Short name of$
        use                             generic-contact         ; Inherit defau$
        alias                           Nagios Admin            ; Full name of $

        email                           davidgomez130@hotmail.com _ <<***** CHA$
        }
```

Ahora es necesario configurar la interfaz web para Nagios así que se debe crear un usuario y contraseña para acceder al sistema. Antes de realizar este paso, es importante realizar la instalación de apache2-utils que se ha instalado previamente en este documento en la sección de autenticación de apache.

Una vez realizado este paso se procede a crear el usuario y la contraseña de acceso como se muestra en la Figura 351.

Figura 351. Crear usuario y contraseña de acceso a Nagios



Para que las configuraciones anteriores tengan efecto se habilita el archivo de configuración mediante el comando a2enmod cgi, ver Figura 352.

Figura 352. Habilitar archivo de configuración cgi

Y también se debe reiniciar el servicio de Apache ejecutando el comando /etc/init.d/apache2 restart como lo muestra la Figura 353.

Figura 353. Reiniciar el servicio apache para Nagios

Tal como se hizo con el código fuente de Nagios, se debe descomprimir, configurar y compilar el código fuente de los plugins que se necesitan para el sistema. Para descomprimir se utiliza el comando de la Figura 354.

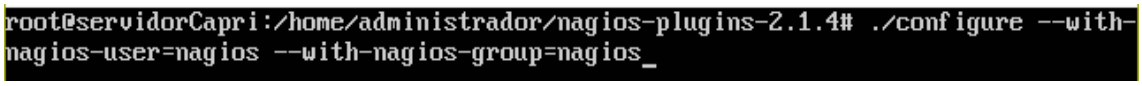
Figura 354. Descomprimir plugins de Nagios

Se accede al directorio que se acaba de descomprimir, ver Figura 355.

Figura 355. Acceder al directorio nagios-plugins-2.1.4.

También se ejecuta la configuración de estos plugins, especificando el usuario y el grupo al cual pertenecerá como lo indica la Figura 356.

Figura 356. Ejecutar configuración de plugins de Nagios



Finalmente se compila el código fuente y se instalan los archivos necesarios tal como lo muestran la Figura 357 y la Figura 358.

Figura 357. Compilar código fuente de los plugins de Nagios

Figura 358. Instalar plugins de Nagios

Para verificar que la configuración del sistema se ha realizado de manera correcta, se ejecuta el siguiente comando, ver Figura 359.

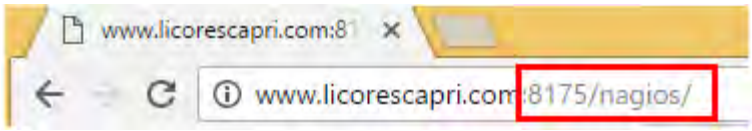
Figura 359. Comprobar configuración de Nagios

También es necesario crear el directorio checkresults en la ruta /usr/local/nagios/var/spool, como lo indica la Figura 360.

Figura 360. Crear directorio checkresults

Una vez realizado esto ya se puede acceder al administrador del sistema de monitoreo mediante un navegador web ingresando la dirección IP o el dominio de la empresa seguido del puerto de apache 8175 para este caso y finalmente el servicio al cual vamos a acceder que es nagios, tal como lo muestra la Figura 361.

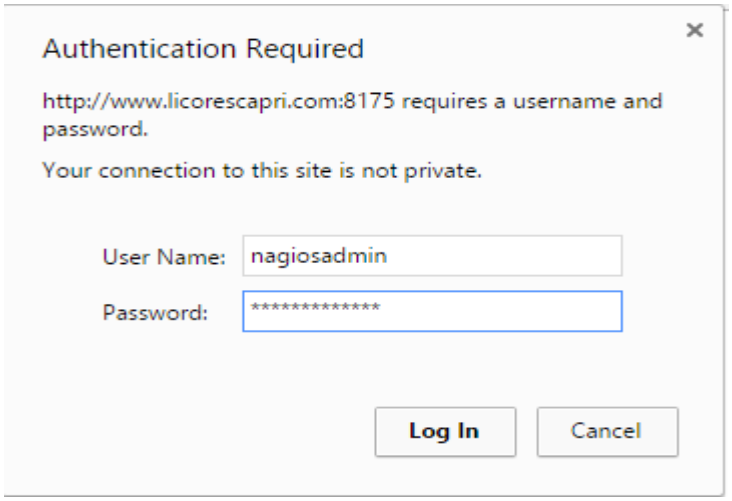
Figura 361. Ingresar a la consola de administración de Nagios



Nota: Recuerde que el puerto de escucha de Apache fue modificado en la configuración del servidor en la sección de Apache de este documento. Por lo tanto, debe ser especificado junto a la dirección URL en el navegador.

Como se puede apreciar en la Figura 362, el sistema solicitara la autenticación del usuario el cual fue creado en paso anteriores:

Figura 362. Autenticación de usuario de Nagios



Una vez el usuario se haya autenticado debe mostrarse la interfaz de administración de Nagios. También es importante fijarse el estado del servicio de la aplicación el cual debe aparecer con un visto como se muestra en la Figura 363.

Figura 363. Consola de administración de Nagios

En el caso de que el servicio no corra y se muestre con una X se debe ejecutar el siguiente comando, ver Figura 364.

Figura 364. Cambiar permisos de usuario

```
root@servidorCapri:/home/administrador# chown nagios:nagios /var/lib/nagios/ -R
```

Ahora se debe editar el archivo de configuración de Nagios para habilitar el monitoreo de máquinas Windows en el sistema, esto se hace con el comando que se muestra en la Figura 365.

Figura 365. Editar archivo de configuración nagios.cfg

```
root@servidorCapri:/home/administrador/nagios-4.3.1# nano /usr/local/nagios/etc/
nagios.cfg
```

Dentro del archivo se debe habilitar la siguiente opción como lo indica la Figura 366.

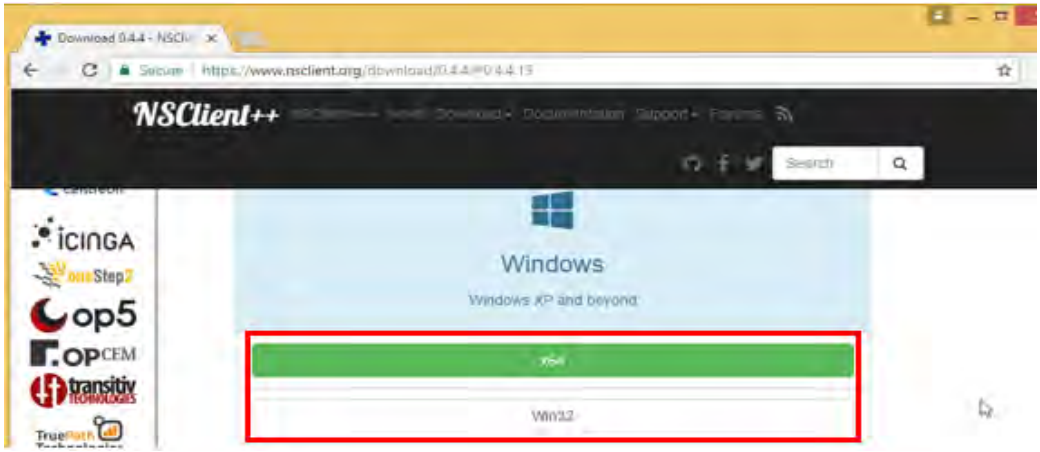
Figura 366. Archivo de configuración nagios.cfg

```
# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

Para añadir máquinas Windows al sistema de monitorización es necesario descargar el programa NSClient ++ en cada una de ellas. Es muy importante tener en cuenta la versión de Windows que se está ejecutando dado que hay una versión del programa para máquinas de 32 bits y otra para máquinas de 64 bits. Este programa se puede descargar de la página oficial como se muestra a continuación, ver Figura 367 y Figura 368.

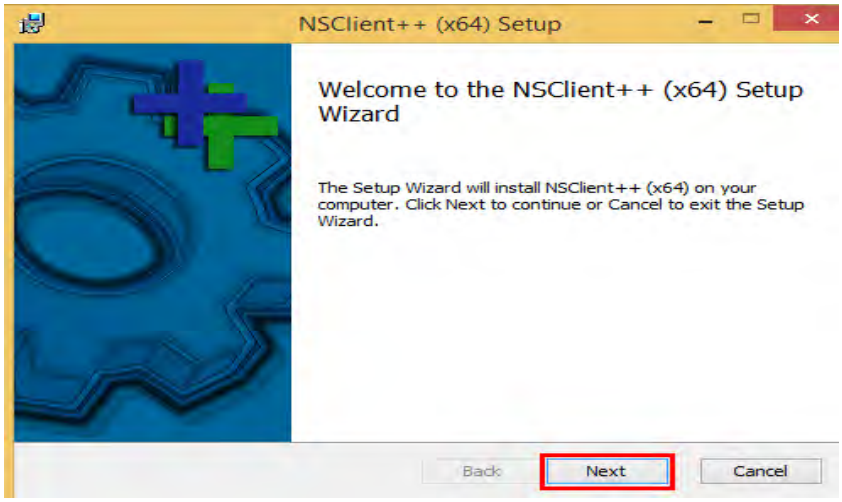
Figura 367. Página oficial de la aplicación NSClient++

Figura 368. Versiones de la aplicación



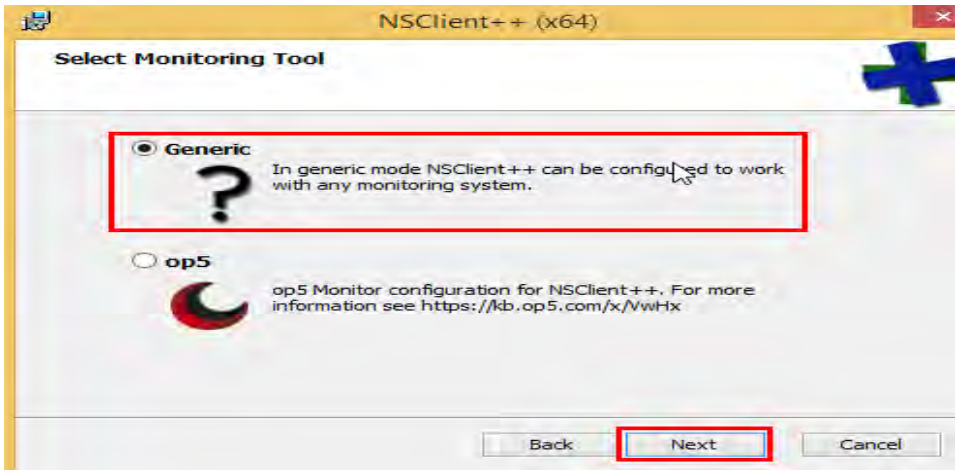
Una vez descargado el programa, se debe proceder con la instalación. Al ejecutar el instalador se muestra la siguiente ventana y se hace clic sobre Next, ver Figura 369.

Figura 369. Asistente de instalación NSClient++



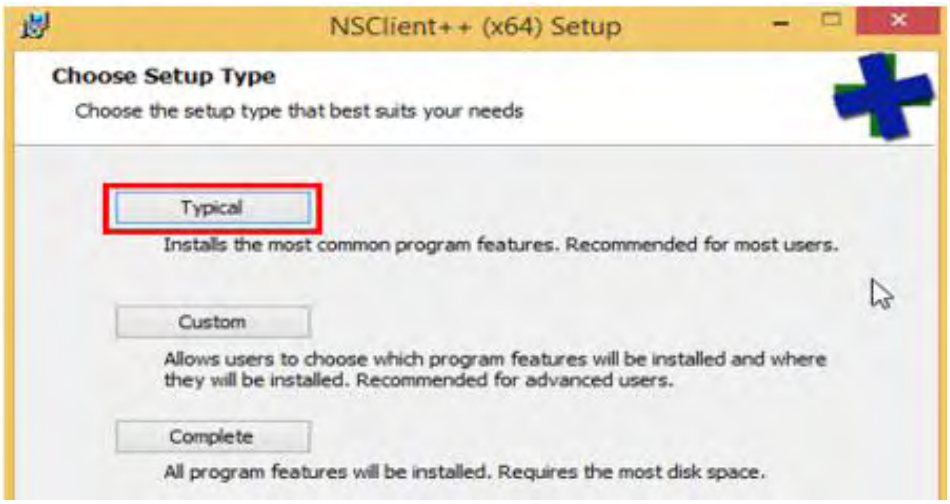
Seleccionar la opción Generic y presionar el botón Next, ver Figura 370.

Figura 370. Asistente de instalación NSClient++ 2



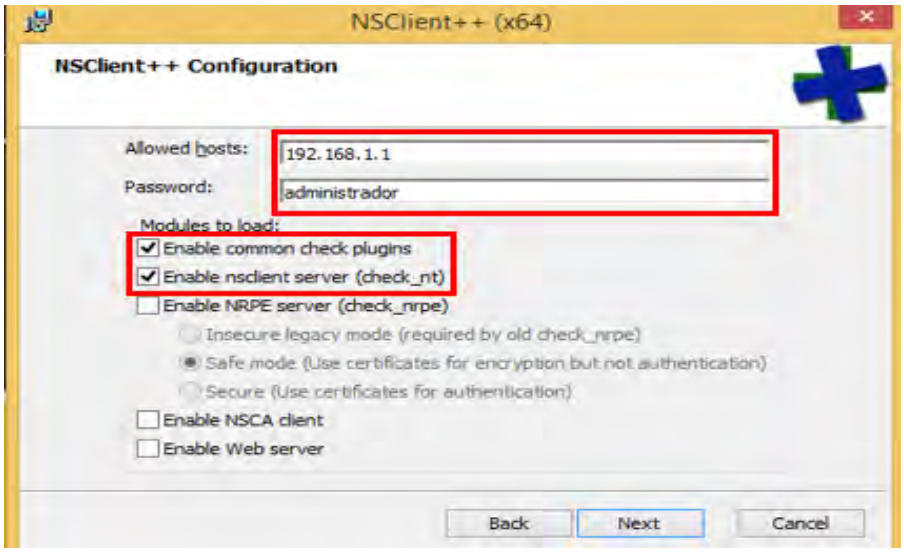
Seleccionar la opción Typical y presionar el botón Next, ver Figura 371.

Figura 371. Asistente de instalación NSClient++ 3



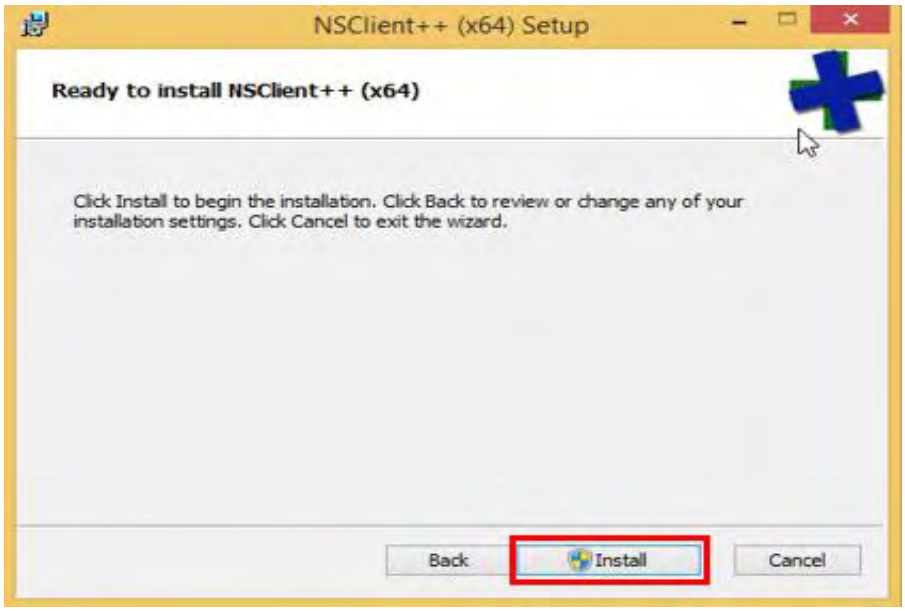
En esta sección, se debe especificar la dirección IP del servidor y la contraseña del usuario del servidor. Además, se marcan las casillas que se indican en la Figura 372.

Figura 372. Asistente de instalación NSClient++ 4



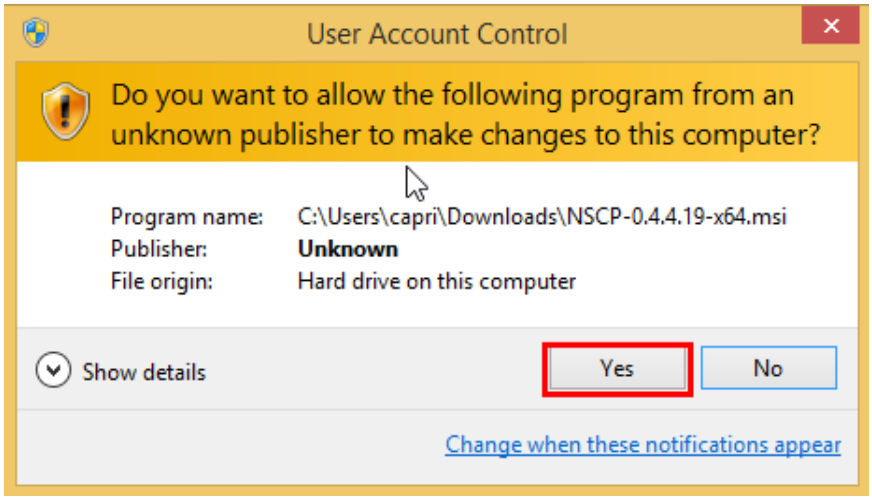
Presionar el botón Install para comenzar la instalación, ver Figura 373.

Figura 373. Asistente de instalación NSClient++ 5



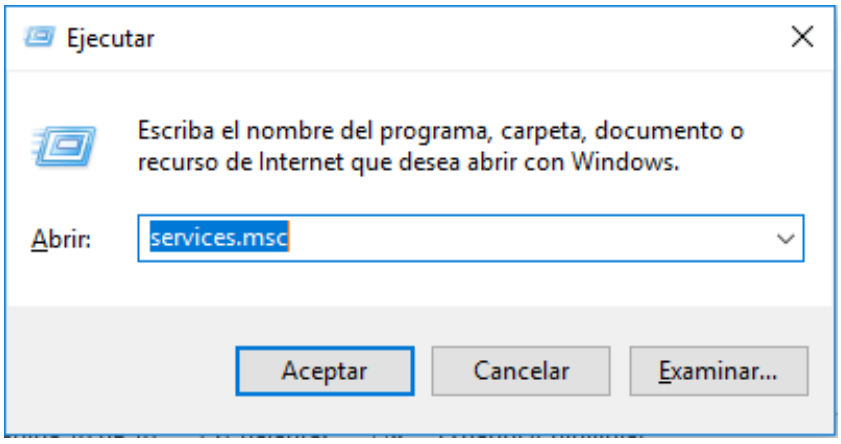
Se debe confirmar los permisos de usuario como se muestra en la Figura 374.

Figura 374. Alerta de control de usuarios



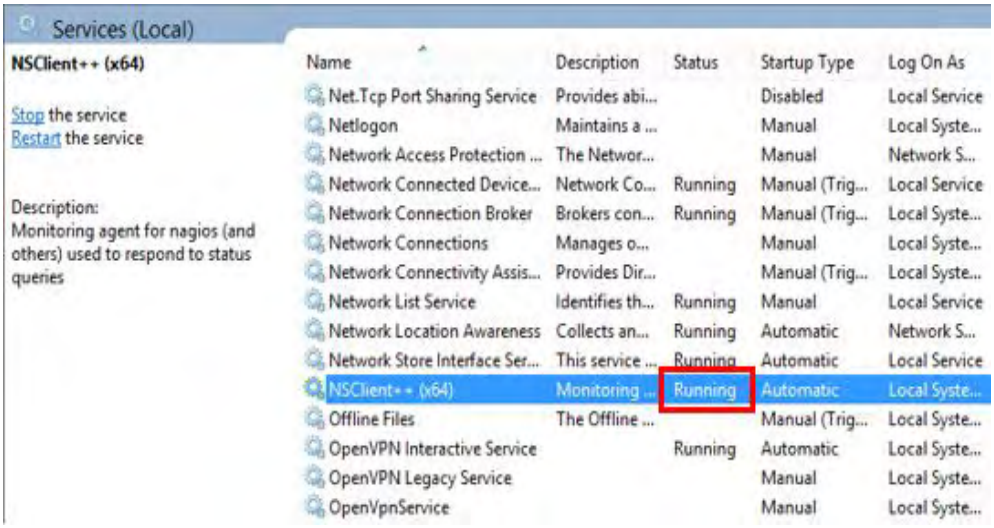
Cuando finalice la instalación, se debe presionar las teclas Windows +r y escribir el comando services.msc para acceder a los servicios de Windows, ver Figura 375.

Figura 375. Acceder a los servicios de Windows



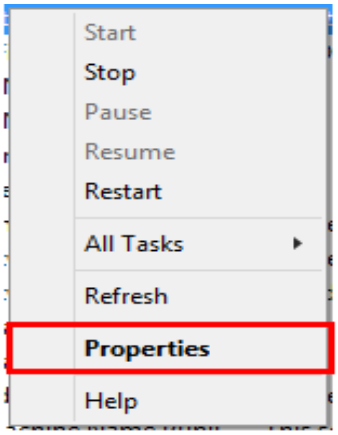
Se ubica el servicio NSClient ++ y se verifica que en su estado se encuentre corriendo, ver Figura 376.

Figura 376. Listado de servicios de Windows



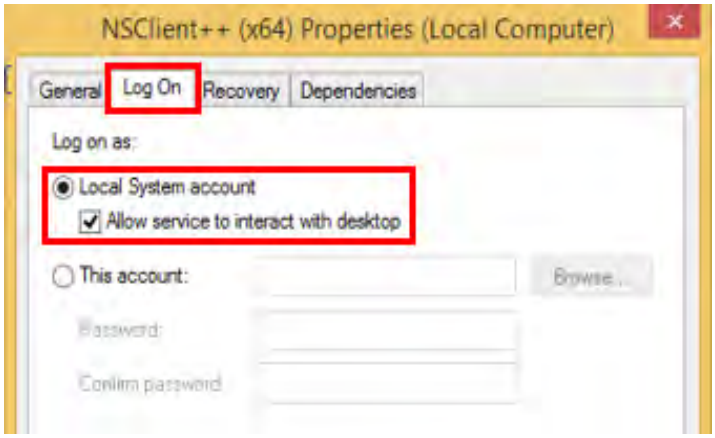
Ubicados sobre el servicio se hace clic derecho y se selecciona la opción Propiedades, ver Figura 377.

Figura 377. Menú servicio NSClient++



Se selecciona la pestaña Iniciar Sesión y se marca la casilla que se muestra a continuación, ver Figura 378.

Figura 378. Propiedades de NSClient++



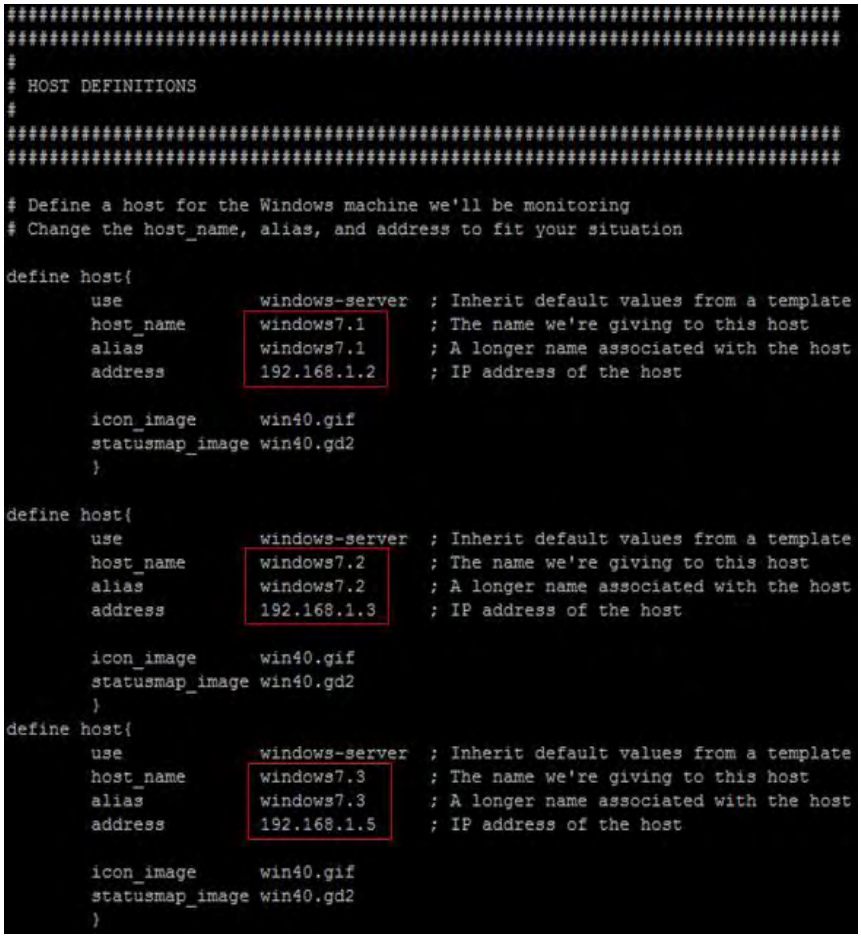
Nota: Este proceso debe realizarse en cada máquina que se desea monitorear en el sistema.

Ahora de vuelta en el servidor se debe ubicar en el directorio objects el cual se encuentra en la ruta /usr/local/nagios/etc/, como lo muestra la Figura 379.

Figura 379. Lista de archivos de configuración del directorio objects

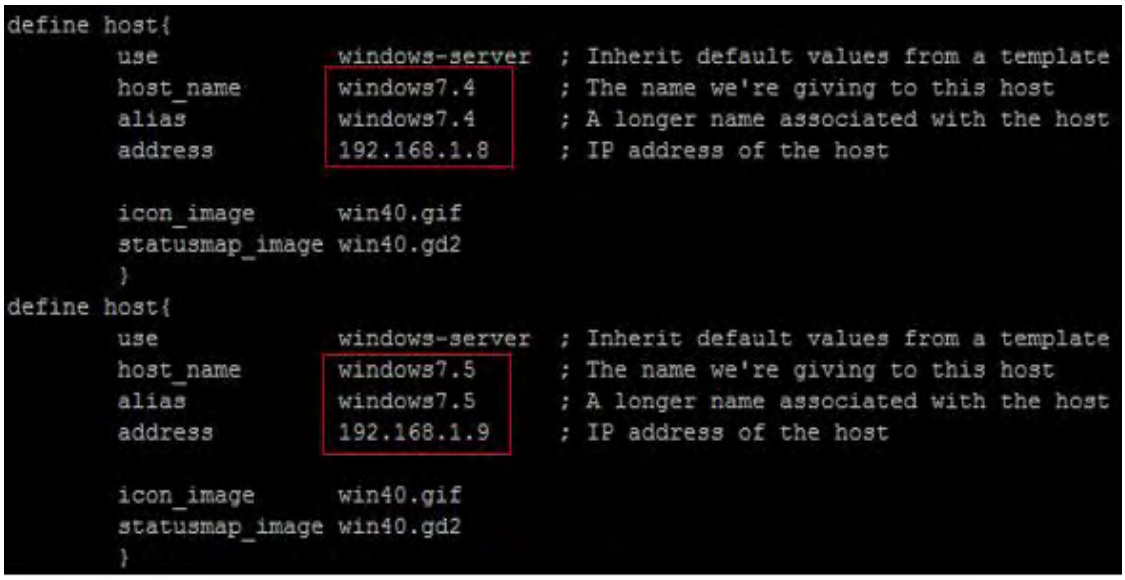
Editar el archivo windows.cfg mediante el comando nano windows.cfg y añadir los nombres de los equipos que se desea registrar y su dirección IP de la manera que lo indica la Figura 380, en este caso se asignan las direcciones asignadas por el DHCP a 5 equipos con el sistema operativo Windows 7, y 2 equipos Windows 8 los cuales hacen parte de las sucursales de la empresa,.

Figura 380. Archivo de configuración windows.cfg 1



En la Figura 381, se añaden los equipos 4 y 5 con sistema operativo Windows 7.

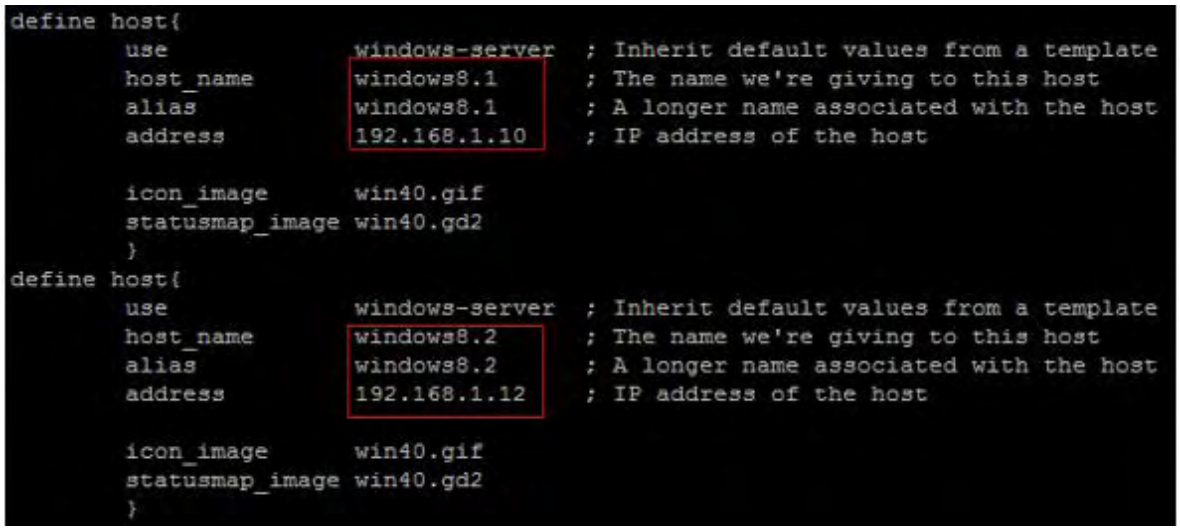
Figura 381. Archivo de configuración windows.cfg 2



```
define host{
        use             windows-server  ; Inherit default values from a template
        host_name       windows7.4      ; The name we're giving to this host
        alias           windows7.4      ; A longer name associated with the host
        address         192.168.1.8     ; IP address of the host

        icon_image      win40.gif
        statusmap_image win40.gd2
        }
define host{
        use             windows-server  ; Inherit default values from a template
        host_name       windows7.5      ; The name we're giving to this host
        alias           windows7.5      ; A longer name associated with the host
        address         192.168.1.9     ; IP address of the host

        icon_image      win40.gif
        statusmap_image win40.gd2
        }
```

En la Figura 382, se asignan las IP de los equipos 4 y 5, con sistema operativo Windows 8. Una vez realizada toda la configuración del archivo se debe guardarlo, para que los cambios surtan efecto.

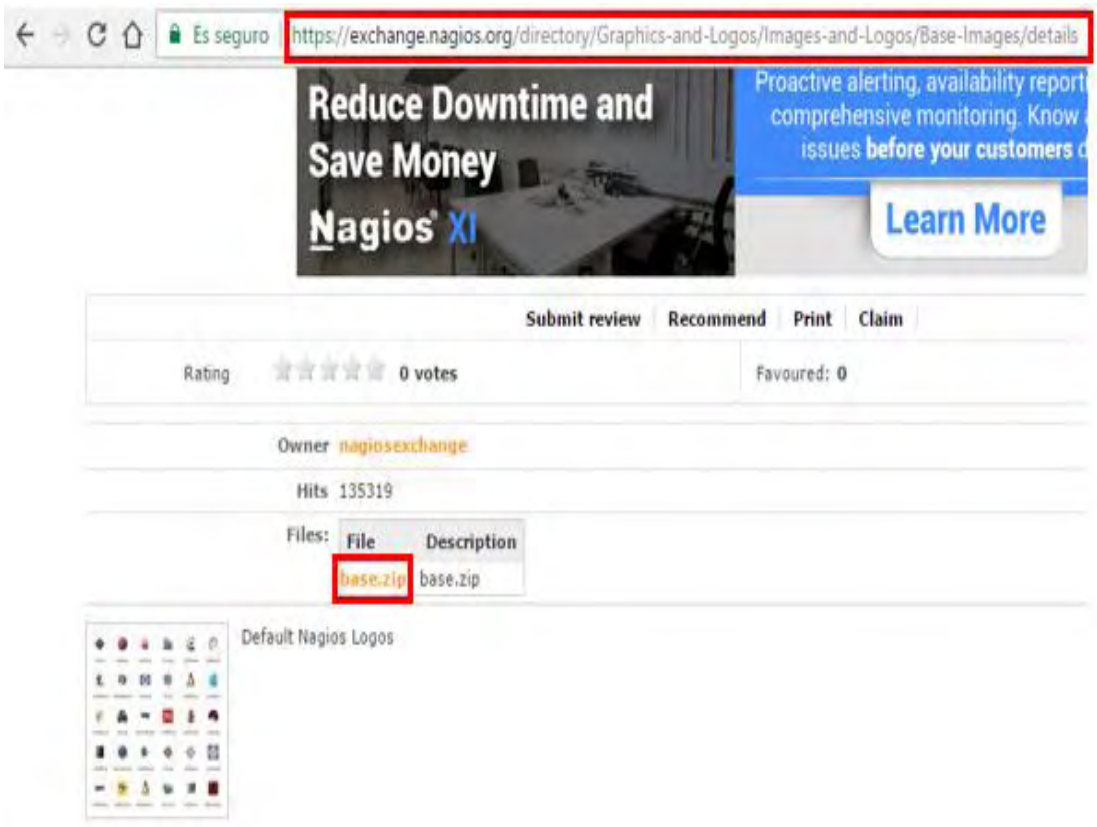
Figura 382. Archivo de configuración windows.cfg3



```
define host{
        use             windows-server  ; Inherit default values from a template
        host_name       windows8.1      ; The name we're giving to this host
        alias           windows8.1      ; A longer name associated with the host
        address         192.168.1.10    ; IP address of the host

        icon_image      win40.gif
        statusmap_image win40.gd2
        }
define host{
        use             windows-server  ; Inherit default values from a template
        host_name       windows8.2      ; The name we're giving to this host
        alias           windows8.2      ; A longer name associated with the host
        address         192.168.1.12    ; IP address of the host

        icon_image      win40.gif
        statusmap_image win40.gd2
        }
```

Como se puede observar en el cuadro anterior, es posible añadir iconos que identifican a cada una de las máquinas agregando las líneas icon_image, statusmap_image y el nombre del icono, esto con el fin de tener claridad de que objeto es el que se está monitoreando. Estos iconos se pueden descargar de la página que se muestra a continuación en la Figura 383, y se deben ubicar estos iconos en el directorio /usr/local/Nagios/share/images/logos.

Figura 383. Página de iconos para Nagios



En la Figura 384, se muestra el paquete de iconos que se descarga.

Figura 384. Iconos base para Nagios

En este mismo archivo de configuración, se debe definir un grupo para agregar las máquinas de Windows que se va a monitorear, se debe escribir el nombre de host de cada una de las maquinas separados por comas, así como lo indica la Figura 385.

Figura 385. Archivo de configuración windows.cfg 2

```
##############################################################################
##############################################################################
#
# HOST GROUP DEFINITIONS
#
##############################################################################
##############################################################################


# Define a hostgroup for Windows machines
# All hosts that use the windows-server template will automatically be a member of this group

define hostgroup{
        hostgroup_name  windows-servers ; The name of the hostgroup
        alias           Windows Servers ; Long name of the group
        }

define hostgroup{
        hostgroup_name  PCScapriwindows ; The name of the hostgroup
        alias           capriwindows    ; Long name of the group
        members         windows7.1, windows7.2, windows7.3, windows7.4, windows7.5, windows8.1, windows8.2
        }
```

También se debe ubicar la sección de servicios, que se monitorearán en este mismo archivo, para añadírselos a las máquinas Windows. Para esto se debe borrar o poner como comentario el nombre del host y añadir el nombre del grupo como se puede observar en la Figura 386, Figura 387, Figura 388, y la Figura 389.

Figura 386. Archivo de configuración windows.cfg 3

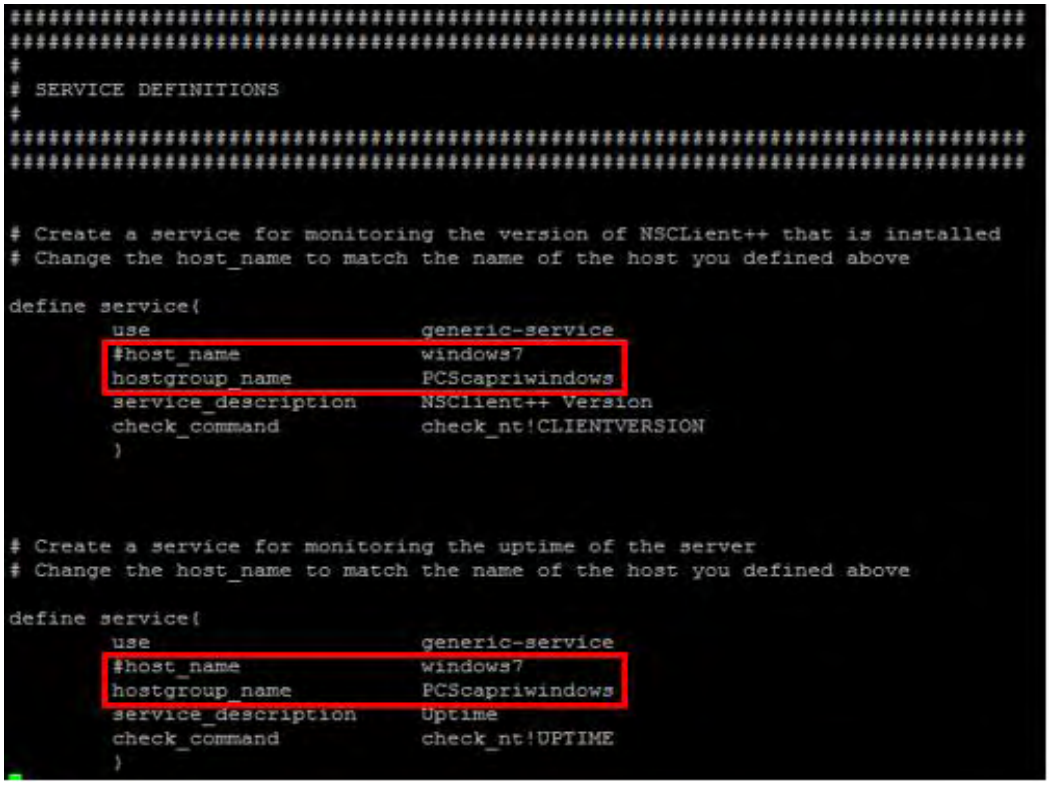


Figura 387. Archivo de configuración windows.cfg 4

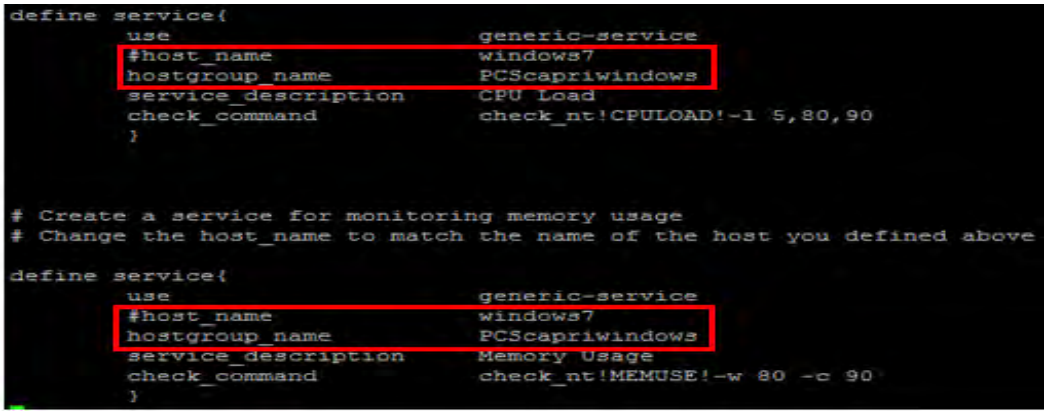


Figura 388. Archivo de configuración windows.cfg 5

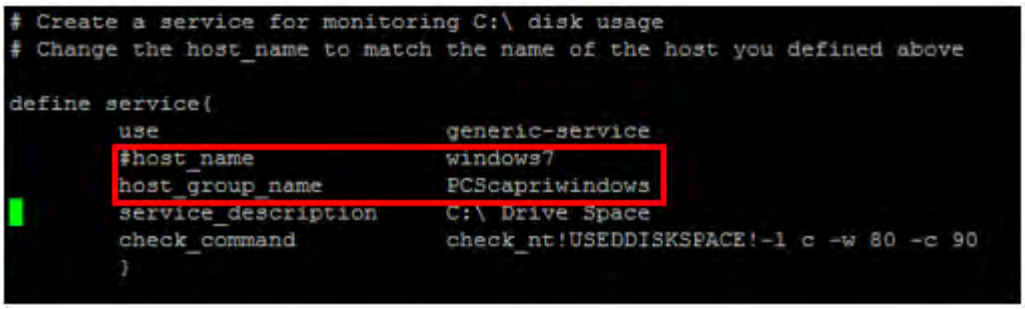
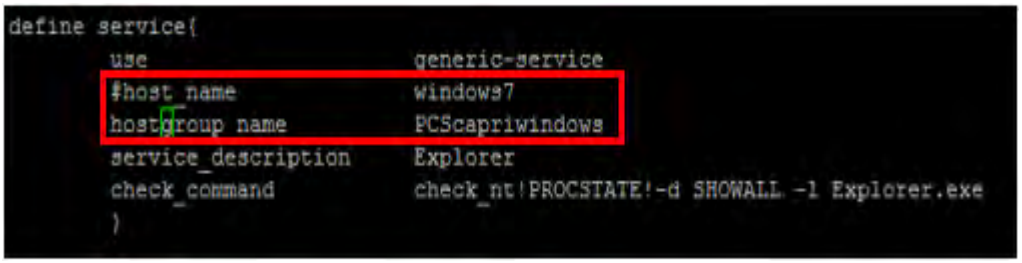
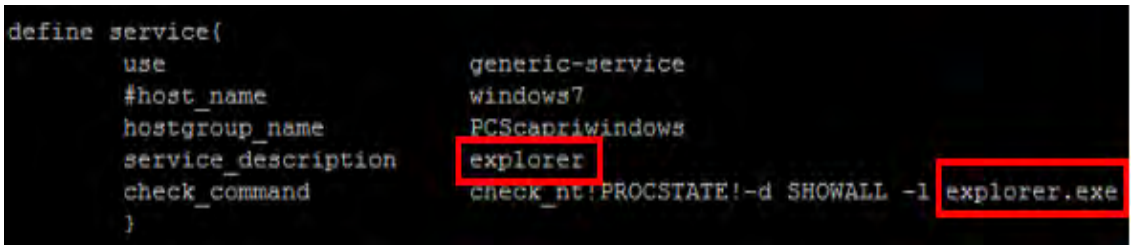


Figura 389. Archivo de configuración windows.cfg 6



En algunas ocasiones el servicio Explorer.exe suele presentar fallas al momento de ser monitoreado. Una de las posibles soluciones a este problema puede ser la modificación del cuadro anterior (Figura 390) en el cual se cambia el nombre del servicio de Explorer.exe a explorer.exe de la siguiente manera.

Figura 390. Archivo de configuración windows.cfg 7



Con los pasos anteriores ya se ha configurado las máquinas Windows que serán monitoreadas.

Ahora se deben configurar los comandos que se ejecutan para monitorear los servicios. Para esto, se debe editar el archivo commands.cfg como se muestra en la Figura 391.

Figura 391. Editar archivo de configuración commands.cfg

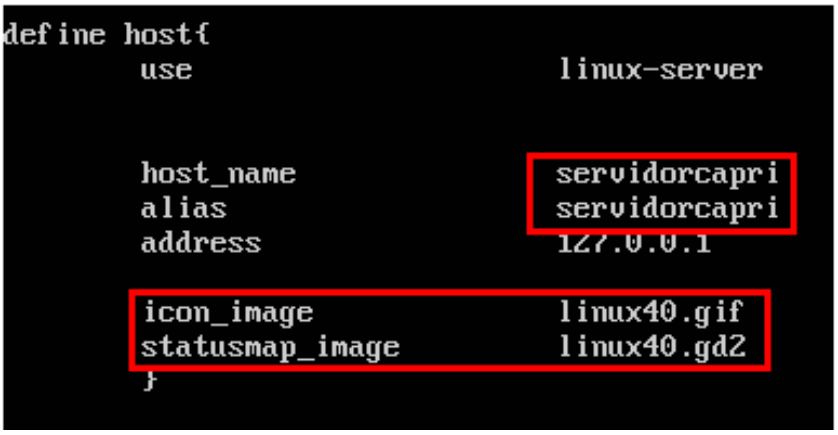
Se debe ubicar en la siguiente sección que se muestra en la Figura 392 y modificarla especificando la contraseña que se estableció en la instalación de NSClient ++ mediante el comando –s, seguido de la contraseña administrador para este caso.

Figura 392. Archivo de configuración commands.cfg

Al servidor también se le puede asignar un nombre y un icono para identificarlo en la red de la misma manera que se le asigno los iconos a las maquinas cliente. Para esto se debe modificar el archivo localhost.cfg, como lo indican la Figura 393 y la Figura 394.

Figura 393. Editar archivo de configuración localhost.cfg

Figura 394. Archivo de configuración localhost.cfg



Algo importante dentro de la configuración del servidor, es especificar los puertos por los cuales está recibiendo las peticiones de las maquinas clientes. En el caso de este servidor algunos puertos de escucha se han modificado por seguridad, como por ejemplo el puerto de Apache y el puerto de SSH. Esto causa que el sistema de monitorización de la red, tenga problemas para monitorear estos servicios al tener configurados los puertos por defecto para cada servicio.

Para dar solución a este problema se debe modificar el archivo localhost.cfg y dentro de este archivo se debe ubicar los servicios que se están monitoreando y a los cuales se les ha modificado el puerto por defecto, en este caso Apache y SSH como se observa en la Figura 395 y la Figura 396.

Figura 395. Archivo de configuración localhost.cfg 2

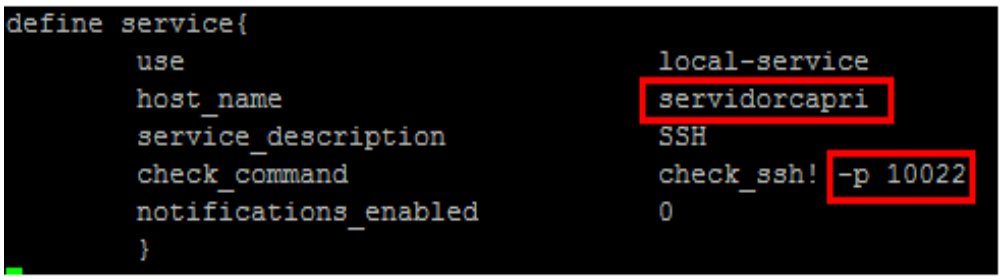
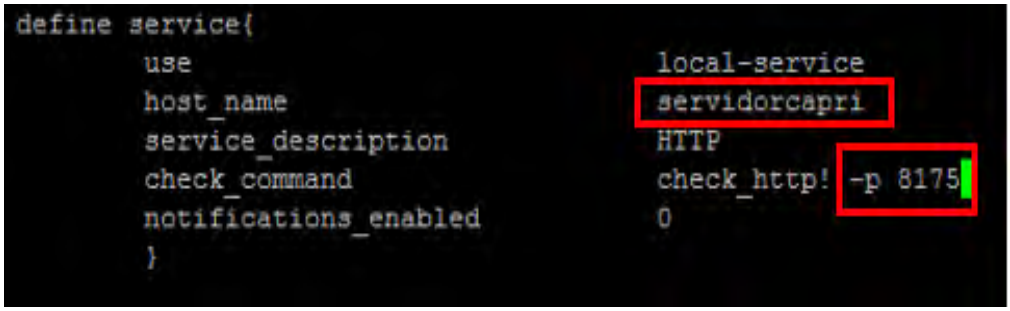


Figura 396. Archivo de configuración localhost.cfg 3



Como se observa en los anteriores cuadros, es muy importante también modificar el nombre del host, para que los servicios se apliquen a este servidor. Este nombre debe ser el mismo que se definió anteriormente en la Figura 397.

Una vez finalizada la configuración de los archivos, se vuelve a comprobar el estado de la configuración de Nagios mediante el comando /usr/local/nagios/bin/nagios –v /usr/local/nagios/etc/nagios.cfg mostrado anteriormente.

Finalmente, se reinicia nuevamente el servicio de Nagios, ver Figura 397.

Figura 397. Reiniciar servicio de Nagios

Ahora se abre nuevamente el navegador y accedemos con el usuario y contraseña como se explicó anteriormente. Debe aparecer la interfaz de administración de Nagios como se muestra en la Figura 398.

Figura 398. Interfaz de administración de Nagios

Luego debe dirigirse a la pestaña Hosts en el panel de navegación del lado izquierdo de la pantalla, ver Figura 399.

Figura 399. Menú principal de Nagios

Aquí deben aparecer una lista detallada del estado de los equipos conectados, como la última vez que se hizo la prueba de conexión, el tiempo que tomó en hacer todas las pruebas, así como los paquetes de datos perdidos, como resultado de la monitorización de la red, tal como se muestra en la Figura 400.

Figura 400. Lista de equipos monitorizados

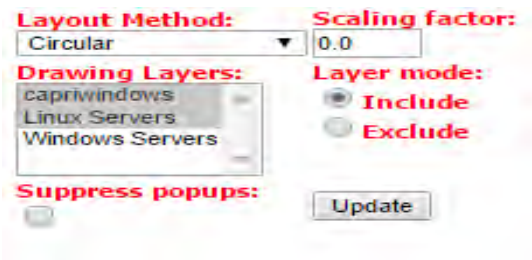
Host	Status	Last Check	Duration	Status Information
servidorcapri	UP	04-06-2017 10:21:52	13d 8h 20m 27s	ECO OK - Paquetes perdidos = 0%, RTA = 0.12 ms
windows7.1	UP	04-06-2017 10:23:06	0d 0h 21m 51s	ECO OK - Paquetes perdidos = 0%, RTA = 2.82 ms
windows7.2	UP	04-06-2017 10:23:42	0d 0h 23m 8s	ECO OK - Paquetes perdidos = 0%, RTA = 2.79 ms
windows7.3	UP	04-06-2017 10:24:20	0d 0h 21m 32s	ECO OK - Paquetes perdidos = 0%, RTA = 2.83 ms
windows7.4	UP	04-06-2017 10:24:57	0d 0h 21m 22s	ECO OK - Paquetes perdidos = 0%, RTA = 5.71 ms
windows7.5	UP	04-06-2017 10:25:35	0d 0h 22m 19s	ECO OK - Paquetes perdidos = 0%, RTA = 1.55 ms
windows8.1	UP	04-06-2017 10:25:29	0d 0h 0m 25s	ECO OK - Paquetes perdidos = 0%, RTA = 6.68 ms
windows8.2	UP	04-06-2017 10:21:46	0d 0h 20m 52s	ECO OK - Paquetes perdidos = 0%, RTA = 2.63 ms

También se puede dirigir a la pestaña (Legacy) para observar un mapa general de la red, ver Figura 401.

Figura 401. Menú principal de Nagios 2

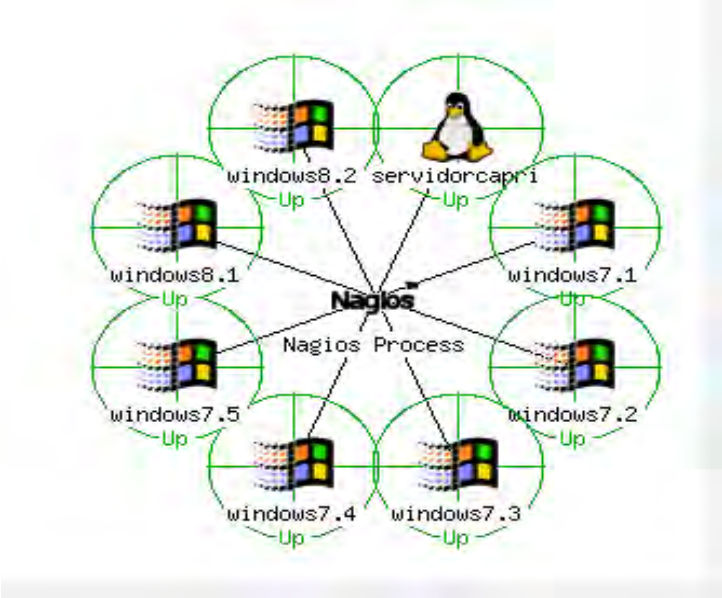
Se debe configurar las opciones que se muestran en el cuadro de la esquina superior derecha de la pantalla como se muestra a continuación, ver Figura 402.

Figura 402. Configurar parámetros del mapa de red



Una vez realizada esta configuración, puede observar el mapa de la red con los equipos conectados como se aprecia en la Figura 403.

Figura 403. Mapa de red de nagios

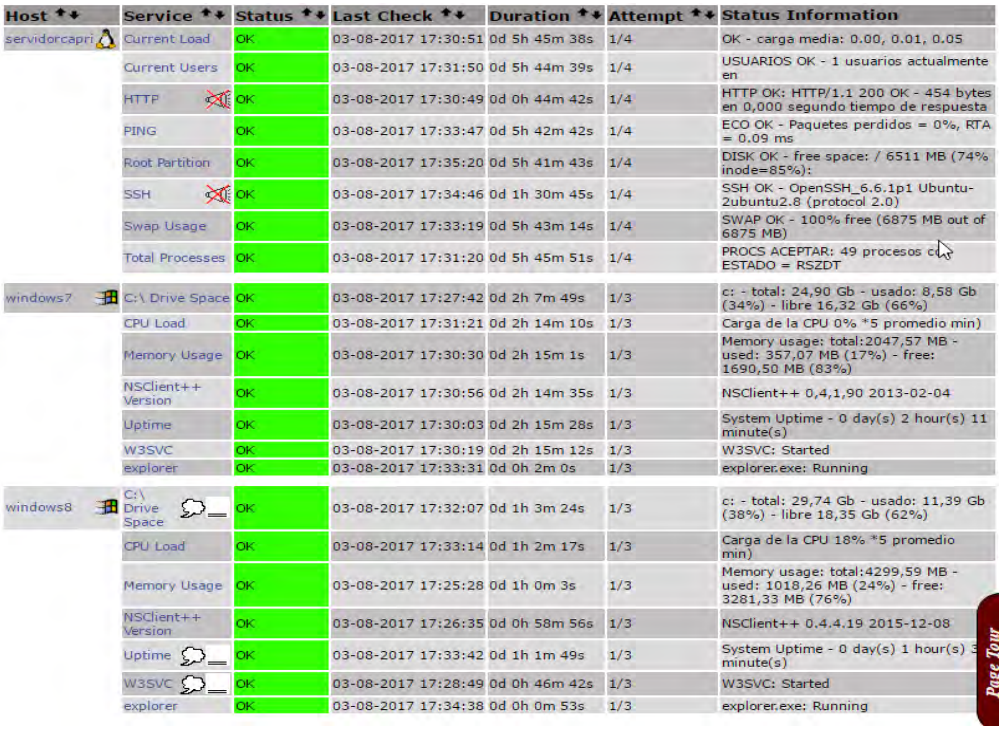


Con esto ya está configurado el sistema de monitorización de red con la herramienta Nagios. Para verificar el estado de todos los servicios configurados tanto del servidor y las máquinas clientes de Windows se dirige a la pestaña Services como lo indica la Figura 404.

Figura 404. Menú principal de Nagios 3

En esta pestaña se listan todos los servicios que se encuentran actualmente monitoreados mostrando con un color verde los servicios activos y con color rojo los servicios que tienen algún problema junto con la descripción del mismo, ver Figura 405.

Figura 405. Lista general de servicios



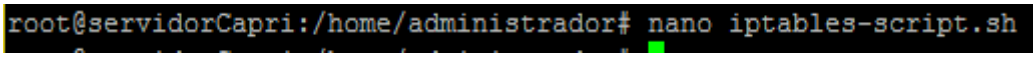
Host	Service	Status	Last Check	Duration	Attempt	Status Information
servidorcapri	Current Load	OK	03-08-2017 17:30:51	0d 5h 45m 38s	1/4	OK - carga media: 0.00, 0.01, 0.05
	Current Users	OK	03-08-2017 17:31:50	0d 5h 44m 39s	1/4	USUARIOS OK - 1 usuarios actualmente en
	HTTP	OK	03-08-2017 17:30:49	0d 0h 44m 42s	1/4	HTTP OK: HTTP/1.1 200 OK - 454 bytes en 0,000 segundo tiempo de respuesta
	PING	OK	03-08-2017 17:33:47	0d 5h 42m 42s	1/4	ECO OK - Paquetes perdidos = 0%, RTA = 0.09 ms
	Root Partition	OK	03-08-2017 17:35:20	0d 5h 41m 43s	1/4	DISK OK - free space: / 6511 MB (74% inode=85%):
	SSH	OK	03-08-2017 17:34:46	0d 1h 30m 45s	1/4	SSH OK - OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8 (protocol 2.0)
	Swap Usage	OK	03-08-2017 17:33:19	0d 5h 43m 14s	1/4	SWAP OK - 100% free (6875 MB out of 6875 MB)
	Total Processes	OK	03-08-2017 17:31:20	0d 5h 45m 51s	1/4	PROCS ACEPTAR: 49 procesos c ESTADO = RSZDT
windows7	C:\ Drive Space	OK	03-08-2017 17:27:42	0d 2h 7m 49s	1/3	c: - total: 24,90 Gb - usado: 8,58 Gb (34%) - libre 16,32 Gb (66%)
	CPU Load	OK	03-08-2017 17:31:21	0d 2h 14m 10s	1/3	Carga de la CPU 0% *5 promedio min)
	Memory Usage	OK	03-08-2017 17:30:30	0d 2h 15m 1s	1/3	Memory usage: total:2047,57 MB - used: 357,07 MB (17%) - free: 1690,50 MB (83%)
	NSClient++ Version	OK	03-08-2017 17:30:56	0d 2h 14m 35s	1/3	NSClient++ 0,4,1,90 2013-02-04
	Uptime	OK	03-08-2017 17:30:03	0d 2h 15m 28s	1/3	System Uptime - 0 day(s) 2 hour(s) 11 minute(s)
	W3SVC	OK	03-08-2017 17:30:19	0d 2h 15m 12s	1/3	W3SVC: Started
	explorer	OK	03-08-2017 17:33:31	0d 0h 2m 0s	1/3	explorer.exe: Running
windows8	C:\ Drive Space	OK	03-08-2017 17:32:07	0d 1h 3m 24s	1/3	c: - total: 29,74 Gb - usado: 11,39 Gb (38%) - libre 18,35 Gb (62%)
	CPU Load	OK	03-08-2017 17:33:14	0d 1h 2m 17s	1/3	Carga de la CPU 18% *5 promedio min)
	Memory Usage	OK	03-08-2017 17:25:28	0d 1h 0m 3s	1/3	Memory usage: total:4299,59 MB - used: 1018,26 MB (24%) - free: 3281,33 MB (76%)
	NSClient++ Version	OK	03-08-2017 17:26:35	0d 0h 58m 56s	1/3	NSClient++ 0.4.4.19 2015-12-08
	Uptime	OK	03-08-2017 17:33:42	0d 1h 1m 49s	1/3	System Uptime - 0 day(s) 1 hour(s) minute(s)
	W3SVC	OK	03-08-2017 17:28:49	0d 0h 46m 42s	1/3	W3SVC: Started
	explorer	OK	03-08-2017 17:34:38	0d 0h 0m 53s	1/3	explorer.exe: Running

Page Tour

4.22 CONFIGURACIÓN DE FIREWALL

Para la configuración del servicio de Firewall es necesario crear un archivo de tipo script en donde se establecen las reglas de seguridad de los puertos de escucha, para esto se crea con el editor nano el archivo iptables-script.sh en la carpeta principal del administrador como se ve en la Figura 406.

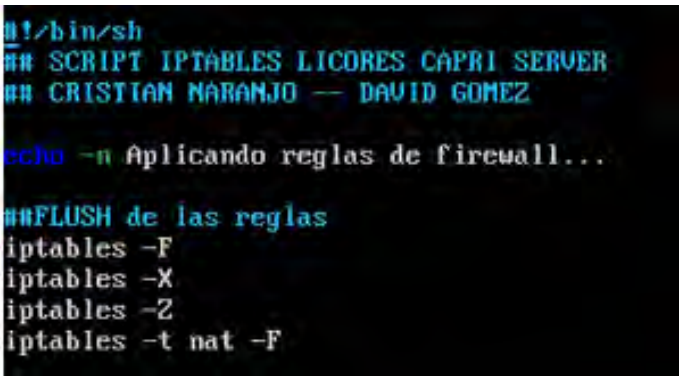
Figura 406. Editar archivo iptables-script.sh



Una vez dentro del archivo se deben especificar las reglas propias para la aplicación de iptables, en el cual se utilizan reglas de input, output, forward, prerouting y postrouting, y otros parámetros de configuración como se explica a continuación:

El primer paso que se realiza, es una limpieza de reglas de firewall que se ejecutaron anteriormente en el servidor, como se observa en la Figura 407, esto con el fin de que se apliquen únicamente las nuevas reglas establecidas y no generar conflictos con las aplicaciones y los puertos que se utilizan en el servidor.

Figura 407. Archivo de configuración iptables-script.sh 1



La siguiente sección a configurar, es la de políticas de acceso que se va a adoptar dentro del firewall. Esta configuración se puede establecer de dos maneras:
La primera es implementar una política de seguridad por defecto de permitir la entrada y salida de todos los paquetes y peticiones que pasen a través del firewall, a excepción de los que sean considerados peligrosos o potencialmente peligrosos por el administrador de la red.

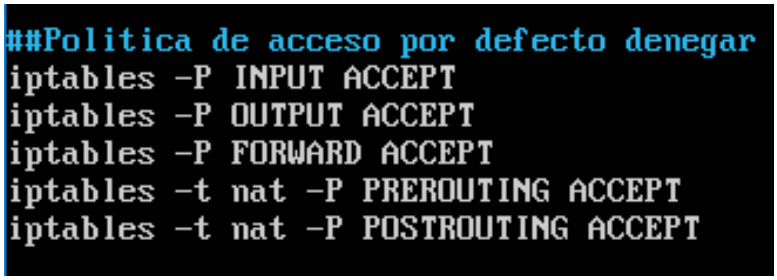
Utilizar esta opción resulta un poco más complejo, ya que requiere tener un amplio conocimiento de las aplicaciones, puertos y tipo de paquetes que se manejan en la red, para permitir el intercambio de información entre estos a través del firewall.

La segunda política de seguridad que se puede establecer, es la de denegar por defecto todas las peticiones y paquetes que lleguen al firewall, y únicamente permitir este intercambio con paquetes que provengan de remitentes conocidos, de esta manera se crea una protección mucho mayor al servidor y los equipos de la red ante posibles ataques informáticos.

Generalmente, se utiliza la segunda opción dado que es más segura y reduce en gran medida los conflictos y problemas con futuros servicios que se deseen

implementar. Para implementar estas políticas de seguridad se utilizan los comandos que se muestran en la Figura 408.

Figura 408. Archivo de configuración iptables-script.sh 2



Uno de los puertos importantes dentro de la red, es el puerto del servidor web el cual comúnmente trabaja por el puerto 80, motivo por el cual las peticiones y paquetes dirigidos a este puerto deben ser re direccionados hacia el nuevo puerto que se ha definido anteriormente para hacer uso de los servicios web de la empresa.

También, es importante especificar otros parámetros como permitir el acceso al firewall de los equipos de la red local y del mismo servidor. La configuración de los anteriores parámetros se observa en la Figura 409.

Figura 409. Archivo de configuración iptables-script.sh 3

Dentro de los servicios que presta el servidor existen algunos que hacen uso de una conexión remota para realizar sus tareas, como por ejemplo el servicio de FTP, SSH y OpenVPN. Para permitir el uso de estos servicios se debe configurar

el firewall como se muestra en la Figura 410, especificando los puertos mediante los cuales trabajan y permitiendo el acceso desde cualquier red.

Figura 410. Archivo de configuración iptables-script.sh 4

```
# Acceso al firewall desde FTP, SSH  y OpenVPN
#
# Acceso al puerto de SSH
iptables -A INPUT 0.0.0.0/0 -p -tcp --dport 10022 -j ACCEPT
# Acceso al puerto de FTP
iptables -A INPUT 0.0.0.0/0 -p -tcp --dport 21 -j ACCEPT
# Acceso al puerto de OpenVPN
iptables -A INPUT 0.0.0.0/0 -p -tcp --dport 1194 -j ACCEPT
```

Además, se debe permitir el acceso a internet de las aplicaciones que lo necesiten, así como también permitir la resolución de nombres de dominio locales y de internet. Esto se debe configurar como lo muestra la Figura 411.

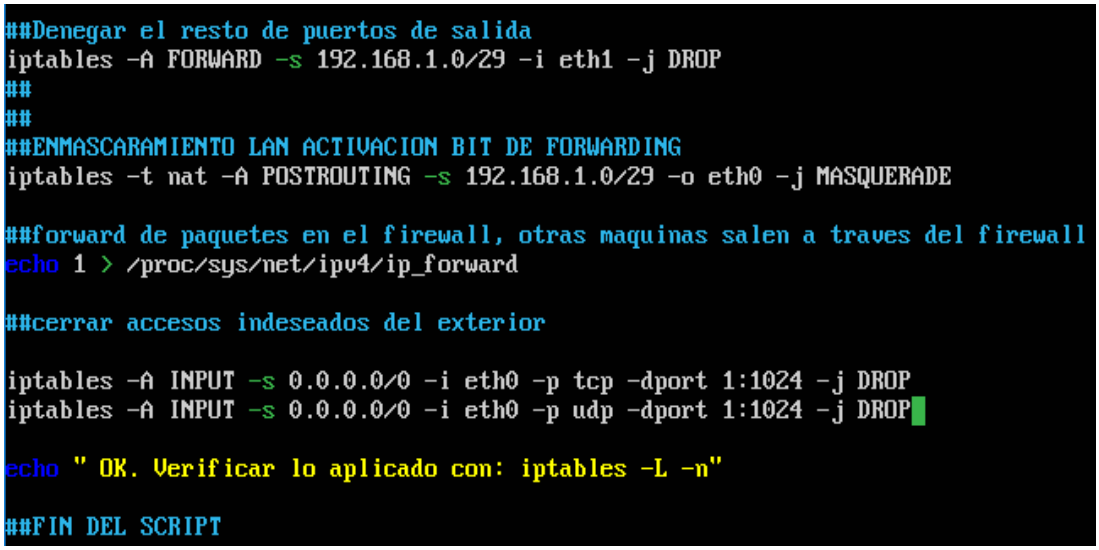
Figura 411. Archivo de configuración iptables-script.sh 5

```
#Acceso a puertos de aplicaciones
##
##
##
##Reglas de FORWARD acceso LAN  a internet.
##Puertos servidor web 8175
iptables -A FORWARD -s 192.168.1.0/29 -i eth1 -p tcp --dport 8175 -j ACCEPT
##Puertos seguros SSL
iptables -A FORWARD -s 192.168.1.0/29 -i eth1 -p udp --dport 443 -j ACCEPT
##Consulta de DNS
iptables -A FORWARD -s 192.168.1.0/29 -i eth1 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/29 -i eth1 -p udp --dport 53 -j ACCEPT
```

Finalmente, se deniega todo tipo de conexión de los demás puertos que no se están usando en el servidor, tanto para la red local como para las redes externas, esto con el fin de proteger la red y el servidor de posibles ataques informáticos como se explicó anteriormente.

También se debe activar el bit de forwarding, para permitir el enmascaramiento de la red haciendo uso de NAT, como se indica en la Figura 412.

Figura 412. Archivo de configuración iptables-script.sh 6



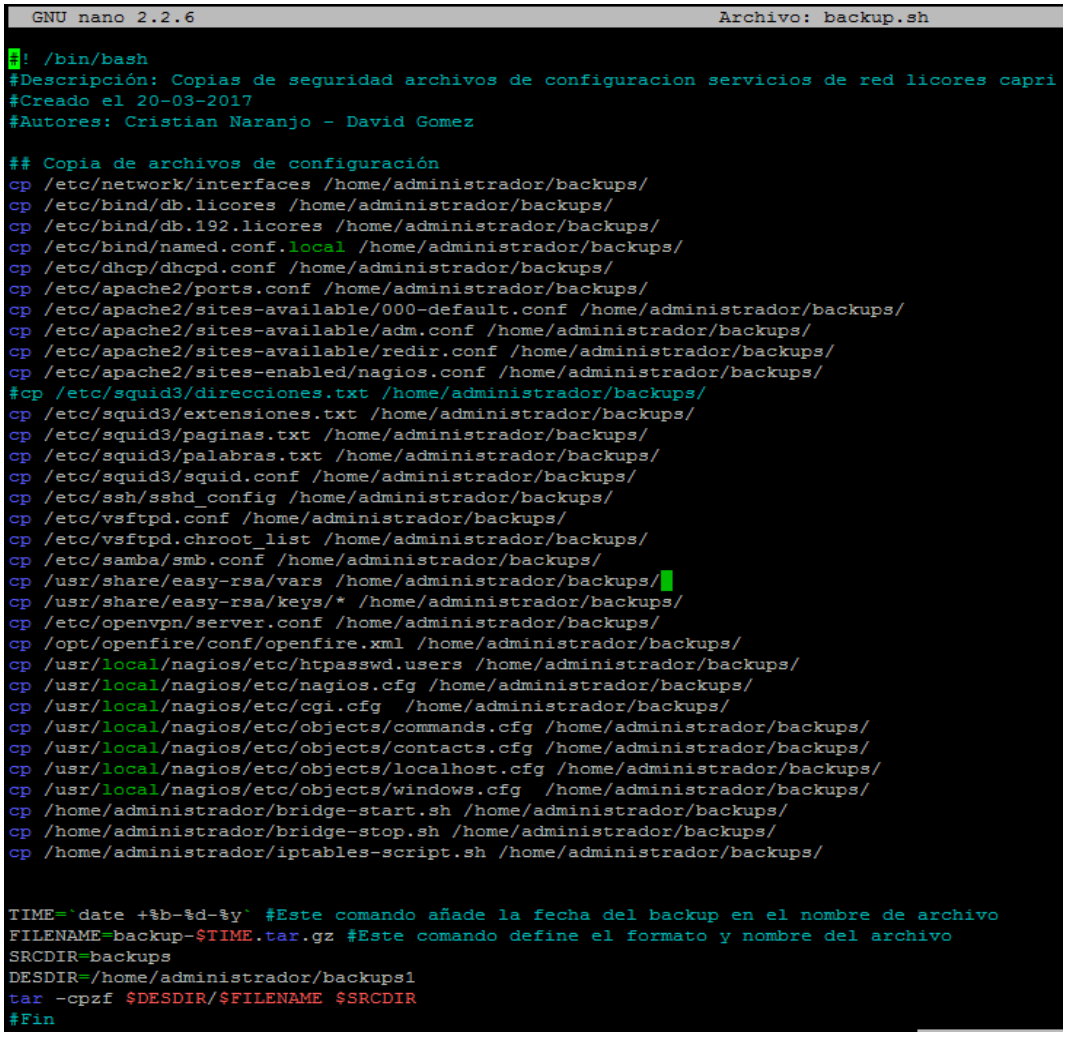
4.23 CONFIGURACIÓN DE COPIAS PERIÓDICAS AUTOMÁTICAS

Para la configuración periódica de todos los archivos de configuración del servidor se debe realizar un script en la carpeta ubicada en la ruta /home/administrador/, con el nombre de backup.sh como se ve en la Figura 413.

Figura 413. Creación archivo backup.sh

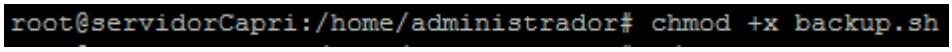
En el archivo con el comando cp se ubican la ruta de todos los archivos los cuales requieran hacer una copia de seguridad periódica automática, además de unas líneas que están descritas con comentarios para la creación de variables para que el archivo sea comprimido con la fecha en la cual la aplicación cron ejecuta el script. Como se describe en la Figura 414.

Figura 414. Edición del script para backups



Una vez guardado el anterior archivo, se procede a darles los permisos necesarios con el comando chmod para que el script pueda ser ejecutado, como se aprecia en la Figura 415.

Figura 415. Permisos de ejecución archivo backup.sh



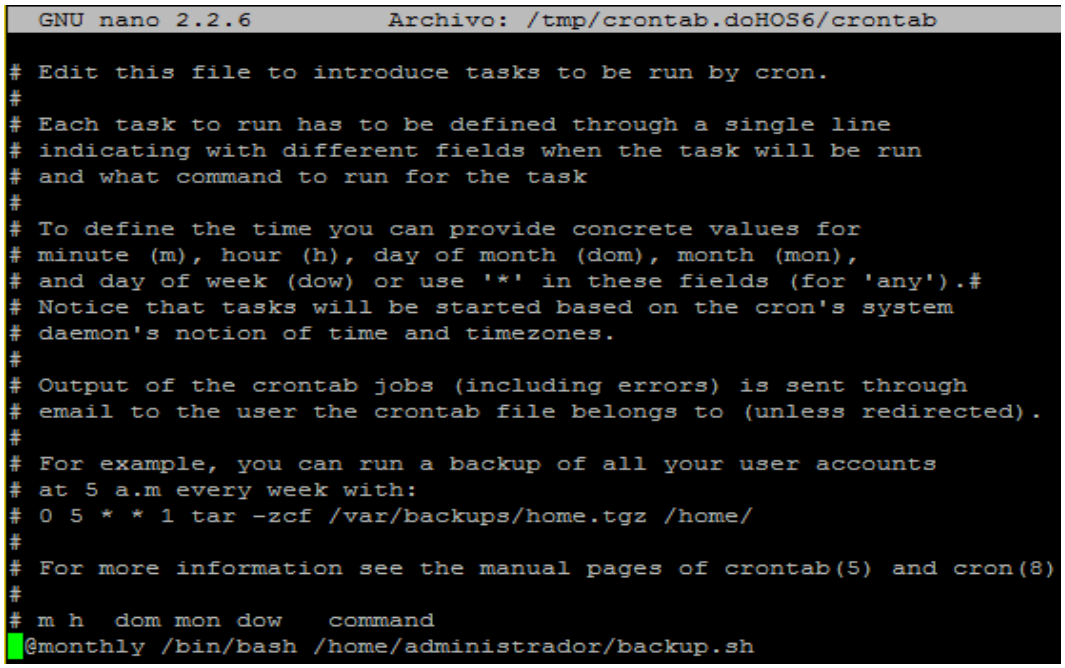
Una vez se otorgan los permisos de ejecución, se procede a abrir la aplicación crontab, la cual se encarga de ejecutar archivos de manera periódica, con el

comando crontab -e, la primera vez que se ejecuta este comando se escoge la opción de configurarlo con el editor nano, Ver Figura 416.

Figura 416. Acceso a la aplicación crontab

Una vez se abre el archivo de configuración de la aplicación crontab, se debe añadir el comando para que el script backup.sh ubicado en la ruta /home/administrador/, se ejecute automáticamente cada mes como se aprecia en la Figura 417.

Figura 417. Aplicación de configuración de crontab



Una vez configurado se debe guardar el archivo, y de ahora en adelante el servidor se encarga de hacer copias de todos los datos de configuración de las aplicaciones instaladas, comprimidos en un archivo dentro de la carpeta /home/administrador/backups1/ con la fecha en la cual se ejecuta el script. La descripción de un nombre del archivo creado por crontab se aprecia en la Figura 418, en el cual se ejecuta el comando tar –xvzf para su descomprensión.

Figura 418. Descomprensión de archivo buckup

```
root@servidorCapri:/home/administrador/backups1# tar -xvzf backup-mar-31-17.tar.gz
```

Cuando se descomprime se aprecia el contenido del archivo creado en el cual está la carpeta backups, y dentro de ella todos los archivos de configuración, como se aprecia en la Figura 419.

Figura 419. Contenido archivo creado por crontab

```
root@servidorCapri:/home/administrador/backups1# cd backups
root@servidorCapri:/home/administrador/backups1/backups# ls
000-default.conf  db.licores          nagios.conf       smb.conf
01.pem            dh2048.pem          named.conf.local  squid.conf
02.pem            dhcpd.conf          openfire.xml      sshd_config
03.pem            extensiones.txt     paginas.txt       usuariovpn2.crt
adm.conf          htpasswd.users      palabras.txt      usuariovpn2.csr
bridge-start.sh   index.txt           ports.conf        usuariovpn2.key
bridge-stop.sh    index.txt.attr      redir.conf        usuariovpn.crt
ca.crt            index.txt.attr.old  serial            usuariovpn.csr
ca.key            index.txt.old       serial.old        usuariovpn.key
cgi.cfg           interfaces          server.conf       vars
commands.cfg      iptables-script.sh  servidorvpn.crt   vsftpd.chroot_list
contacts.cfg      localhost.cfg       servidorvpn.csr   vsftpd.conf
db.192.licores    nagios.cfg          servidorvpn.key   windows.cfg
```

CONCLUSIONES

El óptimo funcionamiento de la red de la empresa, permite el desarrollo eficiente de los procesos de negocio, mejorando los servicios a los clientes.

La administración de los equipos de la red permite llevar un control permanente de sus recursos, los procesos, el estado de la conexión, ofreciendo un ambiente ideal para que los usuarios trabajen de manera correcta desde los puestos de trabajo.

Se aprende la responsabilidad de trabajar con recursos que requieren de gran cuidado, en los cuales se guardan información de muchos equipos y usuarios.

Este proyecto aporta al desarrollo de alternativas de solución ante distintas situaciones con la ayuda de tecnologías disponibles al alcance de todos.

Este proyecto otorga a la empresa la oportunidad de sacar un margen de utilidad, presentando herramientas informáticas que faciliten y mejoran la prestación de servicios a la organización.

La instalación del sistema operativo Linux Ubuntu server, permitió conocer de forma más detallada el funcionamiento de los entornos basados en consola, así como múltiples comandos necesarios para la administración de este sistema, adquiriendo experiencia sobre las necesidades en el área de sistemas y comunicaciones, con recursos disponibles al momento del desarrollo del trabajo, y la puesta en marcha del servidor.

La publicación de la página web ayuda a la empresa a la comercialización de sus productos, bienes y servicios, así como la expansión de su mercado, sin la necesidad de realizar grandes gastos y adquirir este servicio de manera fácil para que su marca sea conocida a nivel mundial.

Para el desarrollo de este trabajo se recolectó información necesaria sobre topologías de red, medios de transmisión, equipos de comunicación, entre otros, los cuales en la actualidad son de uso común en el campo de las redes y telecomunicaciones, facilitando el trabajo de cualquier empresa, en el ámbito de configuración de equipos tipo servidor Linux.

RECOMENDACIONES

Seguir trabajando en proyectos de este tipo para el beneficio de la empresa, añadiendo nuevos servicios, dispositivos y políticas que ayuden a un crecimiento exponencial general de la organización.

Presentar la documentación de este trabajo como soportes de vital importancia para la instalación de servidores en empresas que requieran agregar servidores tipo Linux Ubuntu Server.

Definir fechas periódicas para el mantenimiento técnico y administrativo de la red de la empresa, para el perfeccionamiento y crecimiento de la red.

Estar pendiente en nuevas versiones de las aplicaciones instaladas en el servidor, así como del hardware en funcionamiento para mejorar el rendimiento y escalabilidad de la red.

Incentivar a los estudiantes, a profundizar sobre nuevas herramientas tecnológicas, que puedan ser implementadas en cualquier tipo de organización social, innovando y mejorando la calidad de los sistemas y las telecomunicaciones

BIBLIOGRAFÍA

ICONTEC. Norma técnica colombiana NTC 1486: documentación presentación de tesis, trabajos de grado y otros trabajos de investigación. 2002.

Free Software Foundation Staff. What is free software and why is it so important for society? (en inglés). Consultado el 24 de agosto de 2015.

Windows Server Administration Fundamentals. Microsoft Official Academic Course. 111 River Street, Hoboken, NJ 07030: John Wiley & Sons. 2011. pp. 2-3. ISBN 978-0-470-90182-3.

REFERENCIAS DE INTERNET

CAMARA DE COMERCIO DE PASTO. Desarrollo de tics y comunicaciones http://www.ccpasto.org.co/index.php/desarrollo-de-tics-y-comunicaciones/

Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, Marzo 1997, http://www.rfc-editor.org/info/rfc2131

Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, noviembre 1987, http://www.rfc-editor.org/info/rfc1035.

Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, Enero 2006, http://www.rfc-editor.org/info/rfc4253.

Postel, J., "File Transfer Protocol specification", RFC 765, DOI 10.17487/RFC0765, Junio 1980, http://www.rfc-editor.org/info/rfc765.

“Application server”. http://jsonpedia.org. Publicado 2015-10-16. http://jsonpedia.org.

Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, DOI 10.17487/RFC3920, Octubre 2004, http://www.rfc-editor.org/info/rfc3920.

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", DOI 10.17487/RFC2616, Junio 1999, http://www.rfc-editor.org/info/rfc2616.

HESS KENETH. (2010). Ubuntu Server: The Linux Server Operating Systems Dark Horse. [En linea]. Disponible en: http://www.serverwatch.com/trends/article.php/3870141/Ubuntu-Server-The-Linux-Server-Operating-Systems-Dark-Horse.htm

Distribución de BIND. Disponible en internet https://www.isc.org/downloads/bind/

Distribución de ISC-DHCPD. Disponible en internet. https://www.isc.org/downloads/dhcp/

Distribución de servidor APACHE. Disponible en internet www.apache.org.

Distribución de SQUID. Disponible en internet. http://www.squid-cache.org/

Distribución de OPENVPN. Disponible en https://openvpn.net/.

Distribución de OPENFIRE y MEETINGS. Disponible en internet. http://www.igniterealtime.org/.

Distribución de SAMBA. Disponible en internet. https://www.samba.org.

Distribución de VSFTPD. Disponible en internet. https://security.appspot.com/vsftpd.html.

Distribución de TOMCAT. Disponible en internet http://tomcat.apache.org/.

Distribución de NAGIOS. Disponible en internet. https://www.nagios.org/.

Ubuntu Installation Guide. Copyright © 2004, 2005, 2006, 2007, 2008, 2009 the Debian Installer team Copyright © 2004, 2005, 2006, 2007, 2008, 2009, 2010 Canonical Ltd. https://help.ubuntu.com/14.04/installation-guide/i386/install.en.pdf

Baum-Netzwerktopologie, selbstgezeichnet, basierend auf Grafiken von Head. https://upload.wikimedia.org/wikipedia/commons/a/ad/Netzwerktopologie_Baum.PNG

Mesh network topology, own work. [23-02-17.] https://upload.wikimedia.org/wikipedia/commons/9/91/Netzwerktopologie_vermascht.png

Harald Mühlböck. LAN and WAN scheme. 11 May 2011, https://commons.wikimedia.org/wiki/File:Gateway_firewall.svg

Cableorganizer.com. Network & ethernet cables. http://www.cableorganizer.com/telecom-datacom/patch-cables-boots-plugs.html
Coatindustrial.com. Fibra óptica, alambre y cable, http://www.coatsindustrial.com/es/products-applications/yarn-applications/fibre-optics-wire-cable

Textoscientíficos.com, comparación modelo OSI, [23-02-2017], https://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi.